HITACHI
DATA SYSTEMS

# Hitachi TagmaStore®
# Adaptable Modular Storage and
# Workgroup Modular Storage

# NAS Manager User's Guide

MK-95DF757-03

**© 2006 Hitachi, Ltd., Hitachi Data Systems Corporation, ALL RIGHTS RESERVED**

***Notice:*** No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi Data Systems Corporation (hereinafter referred to as "Hitachi Data Systems").

Hitachi Data Systems reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. Hitachi Data Systems products and services can only be ordered under the terms and conditions of Hitachi Data Systems' applicable agreements. All of the features described in this document may not be currently available. Refer to the most recent product announcement or contact your local Hitachi Data Systems sales office for information on feature and product availability.

This document contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire document will be updated and distributed to all registered users.

## Trademarks

Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd. The Hitachi Data Systems design mark is a trademark and service mark of Hitachi, Ltd.

Hitachi TagmaStore is a registered trademark of Hitachi Data Systems Corporation.

Active Directory, Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

AIX is a registered trademark of International Business Machines Corporation.

Ethernet is a registered trademark of Xerox Corporation.

HP-UX is a registered trademark of the Hewlett-Packard Company.

IRIX and SGI are registered trademarks and XFS is a trademark of Silicon Graphics, Inc.

Linux is a registered trademark of Linus Torvalds.

Mozilla is a registered trademark of the Mozilla Corporation.

Netscape is a registered trademark of Netscape Communications Corporation.

NFS is a registered trademark and Java, Solaris, and Sun are trademarks of Sun Microsystems, Inc.

POSIX stands for Portable Operating System Interface for Computer Environment, which is a set of standard specifications published by the Institute of Electrical and Electronics Engineers, Inc.

RSA is a registered trademark or trademark of RSA Security Inc. in the United States and/or other countries.

Sun is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

Symantec AntiVirus Solution and VERITAS are trademarks of Symantec Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

All other brand or product names are or may be trademarks or service marks of and are used to identify products or services of their respective owners.

## Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Contact the Hitachi Data Systems Legal Department for any export compliance questions.

## Document Revision Level

| Revision | Date | Description |
|---|---|---|
| MK-95DF757-00 | December 2005 | Initial Release |
| MK-95DF757-01 | April 2006 | Revision 1, supersedes and replaces MK-95DF757-00 |
| MK-95DF757-02 | May 2006 | Revision 2, supersedes and replaces MK-95DF757-01 |
| MK-95DF757-03 | July 2006 | Revision 3, supersedes and replaces MK-95DF757-02 |

## Source Documents for this Revision

- *NAS Manager Modular User's Guide*, RSD-95DF757-R01, 8/22/05 (Hitachi SD-TI source document)
- *NAS Manager Modular User's Guide*, 3000-3-991-10(E), March 2006 (Hitachi SD-TI source document)
- Updates from Hitachi Data Systems technical personnel

## Changes in This Revision

- Added an example for the enas_sshkeylist command, section
- Added new information on Managing quotas in section 2.7.1.3.
- Added new notes on Using a File System from an NFS Client, section 2.8.1
- Added new note on NNC name in a CIFS environment, section 2.8.2

- Added new information on operating a NAS Modular system with a policy that creates at least one other NFS share for a directory, section 4.1.3
- Added new information on quota management functionality to section 4.12
- Added new prerequisites to observe before starting quota management in section 4.12.1
- Added new text on viewing group quota Information to section 4.12.3
- Changes in how the system administrator can use commands, in section 5.1
- Added a list of commands the SIGINT signal can be used to cancel in section 5.1.3 under Table 5.2
- Added a list of commands you specify the service IP address before executing in section 5.2.1 and 5.2.2
- Added enas_sshkeylist command information on viewing and deleting public key information in sections 5.3.1 and 5.3.3
- Added an example of enas_clstatus command to section 5.4.2
- Added an example of Cluster Status in the sudo enas_clstatus command display to section 5.4.3.1
- Added an example of Cluster Status in the sudo enas_clstatus command displayed to section 5.4.3.2
- Added to the procedure on how to forcibly stop a cluster in section 5.4.4
- Added an example of node status for command sudo enas_ndstatus in section 5.4.5
- Added an example of cluster status to the sudo enas_clstatus command in section 5.4.6.1
- Added examples to starting a node in section 5.4.6.2
- Added example on resource group status to the sudo enas_rgstatus command in section 5.4.7
- Added resource group status to the stopping resource group procedure in section 5.4.8.1
- Added cluster status  to the sudo enas_clstatus command in section 5.4.8.2
- Added the resource group status information to section 5.4.9
- Added cluster status to sudo enas_clstatus command in section 5.4.10
- Added resource group status information to section 5.4.11.1 and 5.4.11.2
- Added list of file systems information for sudo enas_fslist command in section 5.5.2
- Added new information for device file and list of file systems on file system creation in section 5.5.3
- Added new information about mount status to section 5.5.4
- Added new examples about the list of file systems for the sudo enas_fslist filesystem01 command to section 5.5.5.2

- Added list of file systems example for the sudo enas_fslist filesystem01 command in section 5.5.6.2, 5.5.7.2, 5.5.8.2, 5.5.9.2, 5.6.1.2, 5.6.1.3, 5.6.1.4, 5.6.1.5, 5.6.2.1, 5.6.2.2, 5.6.2.3, 5.6.2.4, and 6.2.33
- Add important notes about mount point directory attributes to section 5.6.2.2
- Updated text on using commands to view quota information in section 5.7.2.1, 5.7.3 and 5.7.3.1
- Added new text on seeting quota, grace period, and monitoring method for file systems to sections 5.7.3.4, 5.7.3.5, and 5.7.3.6
- Added new example of kernel interface table to the sudo enas_netstat –i command in section 5.9.1
- Added new example of sudo enas_ping host01 command to section 5.9.2
- Added new example to sudo enas_devfreelist command in section 6.2.27
- Added new values returned when the -l option is specified in the enas_fsctl command in section 6.2.19
- Added new conditions for setting user quotas to section 6.2.45
- Added new return value 65 to enas_rmfile command in section 6.2.51 and enas_umidget in section 6.2.56
- Added new options -1 and -2 to enas_sshkeydel command in section 6.2.51
- Added new step 2 to procedure on checking access suppression status in section 9.2.1.1
- Added new note on unknown status to section 9.3.4 under Table 9.5
- Revised step 1 and added step 2 for restoring file system in section 9.3.29
- Completed revised restoring a blocked file system procedure in section 9.3.29.3 and 9.3.29.4
- Updated Figure 1.2, Figure 1.3, Figure 2.23, Figure 2.24, Figure 3.5
- Added new sections 1.2.5.1, 1.2.5.2, 1.2.5.3, 2.6, 2.6.1, 2.6.2, 5.6.1.1, 5.6.1.6, 5.6.1.7, 5.7.1, 5.7.2, 5.7.4 - 5.7.4.9, 5.10 - 5.10.2, 6.2.15, 6.2.29 - 6.2.32, 6.2.57 - 6.2.59, 8.1.1 - 8.1.2, 8.1.4.1, 9.3.29.2
- Updated the Managed NNCs in Table 3.1
- Updated Information in the **Contents of List of Services Window** in Table 4.9
- Updated service information displayed in the **CIFS Service Maintenance** window, in Table 4.19
- Updated the /ect/host/ information in Editable System Files in Table 4.36
- Updated server status information in the List of Scanner Servers, Table 4.41
- Updated the mount quota and default options in Table 4.50
- Updated the quota setting found in the Mount Window at File System Mounting in Table 4.51
- Added new information for soft limit and grace period item notifications in Table 4.62

- Added new information displayed when executing the enas_fsctl command in Table 6.18
- Updated the procedure to migrate the file system when changing the method of user mapping in section 2.5.3.
- Made minor revisions to numerous commands, appendices, and the glossary.

# Preface

This document describes and provides instructions for setting up and using the NAS Manager feature of the Hitachi Adaptable Modular Storage (AMS) and Workgroup Modular Storage (WMS) storage systems.

This document assumes the following:

- The user is familiar with the operating system and web browser software on the system hosting the NAS Manager.
- The user is familiar with the Hitachi TagmaStore® AMS/WMS systems and has read and understands the appropriate Storage Navigator User's Guide listed in "Referenced Documents" on the next page.
- The user is familiar with network-attached storage (NAS).

***Notes:***

- In this document the term "Adaptable Modular Storage (AMS)" refers to all models of the TagmaStore AMS system, unless otherwise noted.
- In this document the term "Workgroup Modular Storage (WMS)" refers to all models of the TagmaStore WMS system, unless otherwise noted.
- The NAS Manager screens shown in this document were captured on a Windows® system with the Internet Explorer web browser. They may display differently on other operating systems and browsers.Screen shots from a TagmaStore AMS 500 are used for examples of GUI windows.
- This product includes remote-boot technology licensed from Rembo Technology SaRL, Switzerland.

***Notice:*** The use of NAS Manager and all other Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

## Software Version

This document revision applies to NAS Manager version 4.2 and higher.

## Release Notes

The Release Notes for this product (located on the installation CD) contain requirements and/or restrictions that may not be fully described in this document. The Release Notes may also contain updates and/or corrections to this document. Make sure to read the Release Notes before installation and use of the product.

## Convention for Storage Capacity Values

Storage capacity values for hard disk drives (HDDs) on the AMS/WMS are calculated based on the following values:

1 KB = 1,000 bytes
1 MB = $1,000^2$ bytes
1 GB = $1,000^3$ bytes
1 TB = $1,000^4$ bytes

Storage capacity values for logical units (LUs) on the AMS/WMS are calculated based on the following values:

1 KB = 1,024 bytes
1 MB = $1,024^2$ bytes
1 GB = $1,024^3$ bytes
1 TB = $1,024^4$ bytes

## Referenced Documents

- **Hitachi TagmaStore Adaptable Modular Storage and Workgroup Modular Storage:**
  - *Command Control Interface (CCI) User and Reference Guide* (MK-95DF701)
  - *NAS Backup Restore User's Guide* (MK-95DF759)
  - *NAS Error Codes* (MK-95DF760)
  - *NAS Sync Image User's Guide* (MK-95DF758)
  - *TrueCopy™ Synchronous Remote Replication Software User's Guide* (MK-95DF710)
  - *ShadowImage™ In-System Replication Software User's Guide* (MK-95DF709)
  - *SNMP Agent Support Function User's Guide* (MK-95DF705)
  - *Storage Navigator Modular Command Line Interface (CLI) User's Guide* (MK-95DF712)
  - *Storage Navigator Modular for Web User's Guide* (MK-95DF719)
  - *Storage Navigator Modular Graphical User Interface (GUI) User's Guide* (MK-95DF711)
  - *Hitachi TagmaStore AMS 1000 (Adaptable Modular Storage) Series User and Reference Guide,* (MK-95DF780)
  - *Hitachi TagmaStore AMS 500 (Adaptable Modular Storage) Series User and Reference Guide, (*MK-95DF714)
  - *Hitachi TagmaStore AMS 200 (Adaptable Modular Storage) Series User and Reference Guide, (*MK-95DF713)
  - *Hitachi TagmaStore WMS 100 (Workgroup Modular Storage) Series User and Reference Guide,* (MK-95DF738)

## Comments

Please send us your comments on this document. Make sure to include the document title, number, and revision. Please refer to specific section(s) and paragraph(s) whenever possible.

- **E-mail:** doc.comments@hds.com
- **Fax:** 858-695-1186
- **Mail:**
  Technical Writing, M/S 35-10
  Hitachi Data Systems
  10277 Scripps Ranch Blvd.
  San Diego, CA 92131

***Thank you!*** All comments become the property of Hitachi Data Systems Corporation.

# Contents


**Chapter 1 Introducing NAS Manager....31**

1.1 Introducing NAS Features and Functions.... 31
1.2 Reviewing System Administration Capabilities.... 36
1.2.1 Managing File Systems.... 36
1.2.2 Sharing Files and File Systems using NFS and CIFS Protocols.... 41
1.2.3 Managing User Access to File Systems.... 43
*1.2.4* Methods of Managing File System Users.... 43
1.2.5 Using Quota Management.... 44
1.2.6 Managing Clusters, Nodes, and Resource Groups.... 48
1.2.7 Managing Error Information.... 55
1.2.8 Viewing System Status Using SNMP.... 57
1.2.9 Controlling Service Setup and Service Startup.... 57
1.2.10 Specifying System Settings.... 58
1.2.11 Specifying an Administrator.... 58
1.2.12 Enabling Program Installation.... 59
1.2.13 Protecting the NAS Modular system against Viruses (optional product).... 60
1.2.14 Saving NAS System LU Data.... 61
1.3 Reviewing End-User Capabilities of NAS Manager.... 61

**Chapter 2 System Configuration and Environment Settings....63**

2.1 NAS Modular System Configuration.... 63
2.1.1 Hardware Configuration in a NAS Modular System.... 63
2.1.2 Software Configuration in a NAS Modular System.... 66
2.2 Network Configuration in a NAS Modular System.... 68
2.2.1 Configuring a Network When Using CIFS.... 70
2.3 Reviewing a Trunking Configuration in a NAS Modular System.... 75
2.3.1 Trunking Definition.... 75
2.3.2 Using Trunking in a NAS Modular System.... 82
2.4 Using a Virtual LAN (VLAN) Configuration in a NAS Modular system.... 84
2.4.1 Setting up a VLAN.... 86
2.4.2 Using a VLAN and Trunking in a NAS Modular system.... 87
2.5 Considerations Before Using User Mapping.... 87
2.5.1 Domains that allow Access to a NAS Modular System.... 88
2.5.2 Method of User Mapping.... 90
2.5.3 Changing the Method of User Mapping.... 90
2.5.4 Determining the range of user IDs and group IDs by using RIDs (Examples).. 93
2.6 Considerations before setting quotas.... 96
2.6.1 Setting quotas for each file system.... 97
2.6.2 Setting quotas for each directory.... 97
2.7 Verifying Environment Settings in a NAS Modular system.... 99
2.7.1 Operating with more than 10,000 Users or Groups.... 101
2.8 Reviewing a Client's Operating Environment.... 105
2.8.1 Notes on Using a File System from an NFS Client.... 105
2.8.2 Notes on Using a File System from a CIFS Client.... 110
2.8.3 Configuring the LDAP Server.... 117
2.8.4 Notes on using ADAM.... 127

**Chapter 3 Performing Account Administrator Operations ..... 133**

3.1 Overview of Operations ..... 134
3.2 Logging in and Logging Out ..... 135
3.2.1 Logging In ..... 135
3.2.2 Logging Out ..... 136
3.3 Window Transitions ..... 137
3.4 Basic GUI Operations ..... 139
3.4.1 Window Layout ..... 139
3.4.2 Navigating the GUI ..... 143
3.5 Managing System Administrators ..... 144
3.5.1 Viewing a List of System Administrators ..... 144
3.5.2 Registering System Administrators ..... 145
3.5.3 Deleting System Administrators ..... 147
3.5.4 Editing User Information for System Administrators ..... 147
3.5.5 Changing the System Administrator Password ..... 148
3.6 Editing the Account Administrator's Personal Information ..... 149
3.6.1 Viewing the Account Administrator's User Information ..... 149
3.6.2 Editing the Account Administrator's User Information ..... 150
3.6.3 Changing the Account Administrator's Password ..... 151

**Chapter 4 Performing System Administrator Operations ..... 155**

4.1 Overview of Operations ..... 156
4.1.1 Preparing to Run the System ..... 156
4.1.2 Completing Post-Operation Tasks ..... 157
4.1.3 Reviewing Critical Operations Notes ..... 159
4.2 Logging In and Logging Out ..... 162
4.2.1 Logging In ..... 162
4.2.2 Logging Out ..... 164
4.2.3 Notes on Login and Logout ..... 164
4.3 Window Transitions ..... 164
4.3.1 Window Transitions for Each Function ..... 167
4.4 Information Required Before Using the GUI ..... 178
4.4.1 Window Layout and Method of Operation ..... 178
4.4.2 GUI Features ..... 181
4.5 Managing Clusters ..... 182
4.5.1 Defining a Cluster Configuration ..... 182
4.5.2 Changing a Cluster Configuration ..... 184
4.5.3 Viewing the Status of a Cluster and Nodes ..... 186
4.5.4 Stopping and Starting a Cluster ..... 187
4.5.5 Stopping and Starting a Node ..... 188
4.5.6 Performing a Forced Stop for a Cluster or Node ..... 189
4.5.7 Viewing Resource Group Status ..... 190
4.5.8 Stopping and Starting a Resource Group ..... 193
4.5.9 Performing a Forced Stop for a Resource Group ..... 193
4.5.10 Disabling and Restarting Resource Group Monitoring ..... 194
4.5.11 Changing the Execution Node of a Resource Group ..... 195
4.5.12 Rebooting the NAS OS ..... 195
4.5.13 Changing NNC Names ..... 197
4.6 Managing Services ..... 199

4.6.1 Viewing Service Information ..... 200
4.6.2 Changing the NFS Service Configuration ..... 202
4.6.3 Before Changing the CIFS Service Configuration ..... 203
4.6.4 Maintaining the CIFS Service ..... 224
4.6.5 Changing the SSH Service Configuration (Registering a Public Key) ..... 234
4.6.6 Changing the FTP Service Configuration ..... 238
4.6.7 Starting, Stopping, or Restarting a Service ..... 245
4.7 System Setup ..... 246
4.7.1 Setting Data LAN Ports ..... 249
4.7.2 Setting Up Trunking ..... 254
4.7.3 Viewing Trunking Information ..... 254
4.7.4 Setting Interface and Network Information ..... 264
4.7.5 Setting DNS, NIS, and LDAP Server Information ..... 272
4.7.6 Managing Routing Information ..... 275
4.7.7 Synchronizing Times of Client Machines ..... 279
4.7.8 Setting System Log Transfer Destinations ..... 281
4.7.9 Setting the Log File Size ..... 286
4.7.10 Setting the Period for Saving the Core File ..... 289
4.7.11 Editing System Files Directly ..... 291
4.7.12 Tuning the System's Performance ..... 294
4.7.13 Setting SNMP Information ..... 296
4.7.14 Selecting the User Interface Mode ..... 300
4.8 Using Anti Virus Agent ..... 302
4.8.1 Completing Prerequisites for Linking to Scan Servers ..... 303
4.8.2 Viewing Scan Server Status ..... 305
4.8.3 Registering a Scan Server ..... 308
4.8.4 Changing the Registered Contents of a Scan Server ..... 309
4.8.5 Deleting a Registered Scan Server ..... 310
4.8.6 Setting the Scan Conditions ..... 311
4.8.7 Starting and Stopping the Virus Scan Function ..... 316
4.9 Managing User Information ..... 316
4.9.1 Viewing User Information ..... 317
4.9.2 Managing Group Information ..... 328
4.10 Managing File Systems ..... 333
4.10.2 Allocating a Device File ..... 334
4.10.3 Planning File System Capacity ..... 335
4.10.4 Viewing File System Information ..... 336
4.10.5 Creating a File System ..... 342
4.10.6 Mounting a File System ..... 349
4.10.7 Unmounting a File System ..... 352
4.10.8 Expanding File System Capacity ..... 354
4.10.9 Deleting a File System ..... 355
4.11 Managing File Shares ..... 356
4.11.1 Viewing NFS Share Information ..... 357
4.11.2 Creating an NFS Share ..... 359
4.11.3 Selecting a File System for Creating an NFS Share ..... 364
4.11.4 Editing Information About an NFS Share ..... 366
4.11.5 Deleting an NFS Share ..... 369
4.11.6 When Creating an NFS Share Fails ..... 370
4.11.7 Viewing CIFS Share Information ..... 372

4.11.8 Creating a CIFS Share ..... 374
4.11.9 Selecting a File System for Creating a CIFS Share ..... 381
4.11.10 Setting User and Group Access Permissions ..... 383
4.11.11 Editing Information About a CIFS Share ..... 386
4.11.12 Deleting a CIFS Share ..... 391
4.11.13 When a Creating a CIFS Share Fails ..... 391
4.12 Managing Quotas ..... 393
4.12.1 Before Managing Quotas ..... 397
4.12.2 Viewing User Quota Information ..... 398
4.12.3 Viewing Group Quota Information ..... 401
4.12.4 Setting Quotas ..... 403
4.12.5 Setting Default Quotas ..... 405
4.12.6 Setting a Grace Period ..... 408
4.12.7 Setting Quota Monitoring Times ..... 409
4.13 Managing Error Information ..... 411
4.13.1 Viewing System Messages ..... 413
4.13.2 Downloading System Messages ..... 415
4.13.3 Deleting System Messages ..... 415
4.13.4 Viewing System Logs ..... 416
4.13.5 Downloading a System Log ..... 417
4.13.6 Deleting a System Log ..... 417
4.13.7 Viewing Other Log File Types ..... 418
4.13.8 Downloading Other Log File Types ..... 421
4.13.9 Deleting Other Log File Types ..... 421
4.13.10 Downloading Log Files in a Batch Operation ..... 422
4.13.11 Deleting Log Files in a Batch Operation ..... 427
4.14 Managing Core Files ..... 428
4.14.1 Viewing a List of Core Files ..... 428
4.14.2 Downloading a Core File ..... 429
4.14.3 Deleting a Core File ..... 430
4.15 Managing Programs ..... 431
4.15.1 Viewing Program Information ..... 431
4.15.2 Installing and Uninstalling Programs ..... 432
4.16 Modifying a System Administrator's Personal Information ..... 434
4.16.1 Viewing a System Administrator's Personal Information ..... 435
4.16.2 Editing a System Administrator's Personal Information ..... 435
4.16.3 Changing the System Administrator's Password ..... 436
4.17 Saving NAS System LUs ..... 437
4.17.1 When to Save NAS System LUs ..... 437
4.17.2 Saving NAS OS LUs ..... 438
4.17.3 Saving NAS Cluster Management LUs ..... 443

**Chapter 5 Performing System Administrator Operations Using Commands ..... 451**

5.1 Using Commands ..... 451
5.1.1 Operations that can be performed using commands ..... 451
5.1.2 Flow of operations using commands ..... 455
5.1.3 Notes on operations (required reading before using commands) ..... 456
5.2 Command execution ..... 457
5.2.1 Executing commands by logging in to the NAS Unit ..... 458
5.2.2 Executing commands from a remote host ..... 458

5.3 Register a public key using commands ..... 459
5.3.1 Viewing public key information ..... 459
5.3.2 Registering a public key ..... 459
5.3.3 Deleting a public key ..... 460
5.4 Managing Clusters using Commands ..... 461
5.4.1 Before using Commands to Manage a Cluster ..... 461
5.4.2 Viewing the status of a cluster ..... 461
5.4.3 Stopping and Starting a Cluster ..... 462
5.4.4 Performing a Forced Stop for a Cluster ..... 465
5.4.5 Viewing the Status of Node(s) ..... 467
5.4.6 Stopping and starting a node ..... 467
5.4.7 Viewing the status of resource group(s) ..... 469
5.4.8 Stopping and Starting a Resource Group ..... 470
5.4.9 Performing a Forced Stop for a Resource Group ..... 472
5.4.10 Changing the Execution Node of a Resource Group ..... 473
5.4.11 Disabling and restarting resource group monitoring ..... 474
5.5 File System Management using Commands ..... 475
5.5.1 Before managing a file system ..... 476
5.5.2 Viewing File System Information ..... 476
5.5.3 Creating a File System ..... 477
5.5.4 Mounting a File System ..... 478
5.5.5 Unmounting a File System ..... 479
5.5.6 Deleting a file system ..... 480
5.5.7 Managing the Warning Notifications related to File System Usage ..... 482
5.5.8 Managing Automatic failover if a File System becomes Blocked ..... 484
5.5.9 Managing the Settings for Recording the File Creation Time ..... 487
5.6 File Share Management using Commands ..... 489
5.6.1 Managing NFS shares ..... 490
5.6.2 Managing CIFS shares ..... 500
5.6.3 Managing ACL ..... 505
5.7 Quota management using commands ..... 508
5.7.1 Note on managing quotas ..... 508
5.7.2 Managing quotas set for file systems ..... 509
5.7.3 Setting a user quota for a file system ..... 509
5.7.4 Managing subtree quotas ..... 515
5.8 Managing user mapping information using commands ..... 524
5.9 Checking the network settings and connectivity using commands ..... 524
5.9.1 Checking the network settings ..... 524
5.9.2 Checking the connection to a specified host ..... 525
5.9.3 Checking the path that leads to a specified host ..... 526
5.10 Managing the FC port using commands ..... 527
5.10.1 Before changing the settings of the FC port ..... 527
5.10.2 Changing the data transfer rate of the FC port ..... 527

**Chapter 6 Performing NAS Management Tasks Using Commands ..... 531**

6.1 Reviewing Command Functions ..... 531
6.2 enas_cifscreate (Create a CIFS Share) ..... 533
6.2.1 enas_cifsdelete (Delete a CIFS Share) ..... 539
6.2.2 enas_cifsedit (Edit CIFS Share Information) ..... 540
6.2.3 enas_cifslist (List CIFS Share Information) ..... 549

6.2.4 enas_clstart (Start a cluster) ..... 554
6.2.5 enas_clstatus (Display cluster status) ..... 556
6.2.6 enas_clstop (stop a cluster) ..... 561
6.2.7 enas_devfreelist (List available device files information) ..... 563
6.2.8 enas_dircreate (Create a Subdirectory) ..... 566
6.2.9 enas_dircreate (Create a directory) ..... 568
6.2.10 enas_diredit (Change Directory Attributes) ..... 571
6.2.11 enas_dirgetacl (Display ACL information) ..... 574
6.2.12 enas_dirlist (List Directory Attributes) ..... 578
6.2.13 enas_dirsetacl (Set ACLs) ..... 581
6.2.14 enas_eraselog (Delete Logs) ..... 585
6.2.15 enas_fcparm (Display and change the settings of the FC port) ..... 586
6.2.16 enas_fsautofo (Manage auto failover functionality when a file system is blocked) ..... 588
6.2.17 enas_fscreate (Create a File System) ..... 591
6.2.18 enas_fsdelete (Delete a File System) ..... 595
6.2.19 enas_fsctl (Manage an active file system) ..... 597
6.2.20 enas_fslist (List File System Information) ..... 608
6.2.21 enas_fsfullmsg (Manage warning notification functionality) ..... 613
6.2.22 enas_fsmount (Mount a File System) ..... 617
6.2.23 enas_fsumount (Unmount a File System) ..... 620
6.2.24 enas_ndstart (Start a node) ..... 622
6.2.25 enas_ndstatus (Display node status) ..... 624
6.2.26 enas_ndstop (Stop a node) ..... 627
6.2.27 enas_netstat (Displays the network setting information) ..... 629
6.2.28 enas_nfs_locks_clear (Delete file lock information for an NFS client host) ..... 632
6.2.29 enas_nfs_mount_del (Delete mount information for an NFS client host) ... 634
6.2.30 enas_nfs_mount_list (List mount information for an NFS client host) ..... 636
6.2.31 enas_nfs_opt_list (List the NFS environment settings of the NAS OS) ..... 637
6.2.32 enas_nfs_opt_set (Set an NFS environment for the NAS OS) ..... 638
6.2.33 enas_nfscreate (Create an NFS share) ..... 639
6.2.34 enas_nfsdelete (Delete NFS shares) ..... 645
6.2.35 enas_nfsedit (Edit NFS share information) ..... 647
6.2.36 enas_nfslist (List NFS share information) ..... 652
6.2.37 enas_ping (Display the connection to a specified host) ..... 655
6.2.38 enas_netstat (Check the Network Settings) ..... 657
6.2.39 enas_nfscreate (Create an NFS Share) ..... 660
6.2.40 enas_nfsdelete (Delete NFS Shares) ..... 665
6.2.41 enas_nfsedit (Edit NFS Share Information) ..... 666
6.2.42 enas_nfslist (List NFS Share Information) ..... 669
6.2.43 enas_ping (Display the connection to a specified host ..... 672
6.2.44 enas_quotaget (Display the quota information set for a file system) ..... 674
6.2.45 enas_quotaset (Set quotas for a file system) ..... 682
6.2.46 enas_rgmon (Disable and restart resource group monitoring) ..... 689
6.2.47 enas_rgmove (Change the execution node of a resource group) ..... 691
6.2.48 enas_rgstart (Start a resource group) ..... 693
6.2.49 enas_rgstatus (Display resource group status) ..... 695
6.2.50 enas_rgstop (Stop a resource group) ..... 699
6.2.51 enas_rmfile (Delete a specified file) ..... 701

6.2.52 enas_sshkeyadd (Register a public key) ..... 703
6.2.53 enas_sshkeydel (Delete a public key) ..... 706
6.2.54 enas_sshkeylist (List public key information) ..... 708
6.2.55 enas_traceroute (Check path leading to specified IP address) ..... 710
6.2.56 enas_umidget (Check IDs and names mapped using RIDs) ..... 712
6.2.57 stquota (Display the quota information set for a directory)..... 715
6.2.58 stquotalist (List the user or group quota information set for a directory)..... 721
6.2.59 stquotaset (Set quotas for directories) ..... 724

**Chapter 7 Performing End User Operations.....731**

7.1 Overview of Operations..... 731
7.2 Logging In and Logging Out ..... 731
7.2.1 Logging In..... 732
7.2.2 Logging Out..... 733
7.3 Window Transitions ..... 733
7.4 Basic GUI Operations..... 734
7.4.1 Window Layout ..... 735
7.4.2 Reviewing Program Usage Notes ..... 736
7.5 Viewing a List of NFS File Shares..... 737
7.5.1 Viewing a List of CIFS File Shares..... 738
7.6 Viewing Quota Information set for file systems (end user) ..... 738
7.6.1 Viewing User Quota Information (end user)..... 739
7.6.2 Viewing Group Quota Information (end user)..... 741
7.7 Changing Your Password..... 743
7.8 Editing Your User Comment..... 744

**Chapter 8 Performing Maintenance Tasks.....749**

8.1 Maintaining the Hardware..... 749
8.1.1 Tasks for replacing hardware periodically ..... 749
8.1.2 Tasks for adding or removing disks ..... 751
8.1.3 Adding a Disk to Add a New File System..... 751
8.1.4 Deleting a File System to Remove Disks ..... 752
8.1.5 Expanding File System Capacity (When not using a volume manager)..... 753
8.1.6 Removing a Disk to Reduce File System Capacity ..... 753
8.2 Software Maintenance ..... 754
8.2.1 Installing NAS Manager ..... 754
8.2.2 Installing an optional program ..... 755
8.2.3 Installing a NAS OS Patch Version..... 755

**Chapter 9 Troubleshooting .....757**

9.1 General Troubleshooting Procedures..... 757
9.1.1 Detecting Errors ..... 758
9.1.2 Troubleshooting ..... 759
9.2 Identifying the Error ..... 760
9.2.1 Verifying the Source of Error without using a NAS Modular System ..... 760
9.2.2 Checking Error Messages in the Processing Results Window..... 764
9.2.3 Checking System Messages..... 764
9.2.4 Checking Error Information in the Browse Cluster Status Window ..... 766

9.2.5 Checking Error Statuses in the List of File Systems Window ..... 770
9.2.6 Checking Error Information by using SNMP Notification ..... 771
9.2.7 Checking for a Web Server Error ..... 771
9.2.8 Checking Error Information Sent by E-mail ..... 772
9.2.9 Checking user mapping information ..... 772
9.2.10 Checking for a possible server connection problem ..... 773
9.3 Collecting data and contacting the maintenance personnel ..... 774
9.3.1 Downloading error information ..... 774
9.3.2 Checking and Re-Running Erroneous GUI Operations ..... 775
9.3.3 Checking System Messages ..... 775
9.3.4 Viewing Error Data in the Browse Cluster Status Window ..... 775
9.3.5 Recovery Procedure 1 ..... 779
9.3.6 Recovery Procedure 2 ..... 779
9.3.7 Recovery Procedure 3 ..... 779
9.3.8 Recovery Procedure 4 ..... 780
9.3.9 Recovery Procedure 5 ..... 780
9.3.10 Recovery Procedure 6 ..... 780
9.3.11 Recovery Procedure 7 ..... 780
9.3.12 Recovery Procedure 8 ..... 781
9.3.13 Recovery Procedure 9 ..... 781
9.3.14 Recovery Procedure 10 ..... 781
9.3.15 Recovery Procedure 11 ..... 781
9.3.16 Recovery Procedure 12 ..... 781
9.3.17 Recovery Procedure 13 ..... 782
9.3.18 Recovery Procedure 14 ..... 782
9.3.19 Recovery Procedure 15 ..... 782
9.3.20 Recovery Procedure 16 ..... 782
9.3.21 Recovery Procedure 17 ..... 782
9.3.22 Recovery Procedure 18 ..... 783
9.3.23 Recovery Procedure 19 ..... 783
9.3.24 Recovery Procedure 20 ..... 784
9.3.25 Recovery Procedure 21 ..... 784
9.3.26 Recovery Procedure 22 ..... 784
9.3.27 Manual Failover and Failback ..... 784
9.3.28 Replacing NAS Manager ..... 785
9.3.29 Recovering from File System Errors ..... 785
9.3.30 Checking Error Information in the List of File Systems Window ..... 791
9.3.31 Checking Error Information (List of Interfaces Window) ..... 796
9.3.32 Checking Error Information on Trunking ..... 797
9.3.33 Checking Error Information on Data LAN Port ..... 799
9.4 Collecting Data and Contacting Your HDS Representative ..... 799
9.5 Calling the Hitachi Data Systems Support Center ..... 800

**Appendix A List of Reserved Words ..... 801**

**Appendix B List of MIB Objects ..... 803**

B.1 MIB Objects for Responding to SNMP Get Requests ..... 804
B.2 SNMP Traps ..... 827
B.3 Obtaining a Definition File for Hitachi MIB Objects ..... 832

**Appendix C Tasks that Require Saving NAS System LUs ..... 833**

C.1 Account Administrator Tasks ..... 833
C.2 System Administrator Tasks ..... 833
C.3 End User Tasks ..... 844
C.4 Maintenance Tasks ..... 844

**Appendix D Output of Network Information ..... 847**

D.1 Output content of network information ..... 847
D.2 Output content of the enas_routelist.log file ..... 848

**Appendix E Checking Network Communication ..... 861**

E.1 Checking Network Communication ..... 861

**Acronyms and Abbreviations ..... 873**

**Glossary ..... 875**

# List of Figures


Figure 1.1 Overview of a NAS Modular System ..... 32
Figure 1.2 Position of NAS Manager in a NAS Modular System ..... 35
Figure 1.3 When warnings related to File Systems are Issued ..... 39
Figure 1.4 General Process during File Access ..... 41
Figure 1.5 Overview of Quota Management ..... 44
Figure 1.6 Example of quota management ..... 46
Figure 1.7 Example of Quota Management ..... 47
Figure 1.8 Cluster Configuration in a NAS Modular system ..... 49
Figure 1.9 General Process for Client Services (normal operation) ..... 51
Figure 1.10 General Process for Client Services (at failover) ..... 52
Figure 1.11 Scanning for Viruses on a NAS Modular System..... 60

Figure 2.1 Overview of Hardware Configuration in a NAS Modular System ..... 64
Figure 2.2 Overview of Software Configuration in a NAS Modular System ..... 66
Figure 2.3 Overview of Network Configuration in a NAS Modular system ..... 69
Figure 2.4 Network with CIFS Client and NAS Unit in Single Work Group ..... 71
Figure 2.5 Network with CIFS Client and NAS Unit in Multiple Work Groups ..... 71
Figure 2.6 Network with CIFS Client and NAS Unit in Single NT Domain ..... 72
Figure 2.7 Network with NAS Unit and Primary Domain Controller in Same Subnet ..... 73
Figure 2.8 Network without NAS Unit and Primary Domain Controller in Same Subnet .... 73
Figure 2.9 Network with NAS Unit and Primary Domain Controller in Same Subnet ..... 74
Figure 2.10 Network with gbe1 and gbe4 in a CIFS Service..... 75
Figure 2.11 Network Configuration that Does Not Use Trunking..... 76
Figure 2.12 Network Configuration with Link Aggregation (with No Error) ..... 77
Figure 2.13 Network Configuration with Link Aggregation (with an Error))..... 78
Figure 2.14 Network Configuration with Link Alternation (with No Error) ..... 79
Figure 2.15 Network Configuration with Link Alternation (with an Error) ..... 80
Figure 2.16 Network Configuration with Cascaded Trunking (with No Error)..... 81
Figure 2.17 Recommended Trunking Configuration 1..... 83
Figure 2.18 Recommended Trunking Configuration 2..... 84
Figure 2.19 Usual LAN Network Configuration ..... 84
Figure 2.20 Network Configuration when a VLAN is Used..... 85
Figure 2.21 Domains that allow access to CIFS shares in a NAS Modular system ..... 89
Figure 2.22 Example of assigning user IDs and group IDs by using RIDs..... 93
Figure 2.23 Estimating Total Number of Required User IDs and Group IDs..... 95
Figure 2.24 Example of Setting User IDs and Group IDs ..... 96
Figure 2.25 Example of setting quotas for a file system ..... 97
Figure 2.26 Example of setting subtree quotas..... 98
Figure 2.27 System Requirements with more than 10,000 Users or Groups..... 103

Figure 3.1 Login (Account Administrator) Window ..... 135
Figure 3.2 Main Menu (Account Administrator) Window ..... 137
Figure 3.3 Window Transitions for Account Administrator ..... 138
Figure 3.4 GUI Window Layout (Account Administrator)..... 142
Figure 3.5 List of Administrators Window..... 144
Figure 3.6 Change Password (system administrator setup) Window ..... 148
Figure 3.7 Personal Info. Setup (Account Administrator Setup) Window..... 149
Figure 3.8 Change Password (Account Administrator Setup) Window ..... 151

Figure 4.1 NAS Manager Setup Procedure ..... 156
Figure 4.2 Login Window ..... 163
Figure 4.3 Main Menu Window ..... 165
Figure 4.4 Window Transitions for Cluster Management ..... 167
Figure 4.5 Window Transitions for System Setup (continued on next page) ..... 168
Figure 4.4 Window Transitions for System Setup (continued) ..... 169
Figure 4.6 Window Transitions for User Management ..... 170
Figure 4.7 Window Transitions for File System Management *Notes:* ..... 171
Figure 4.8 Window Transitions for File Share Management ..... 172
Figure 4.9 Window Transitions for Error Information Management ..... 174
Figure 4.10 Window Transitions for Error Information Management ..... 175
Figure 4.11 Window Transitions for Service Management ..... 176
Figure 4.12 Window Transitions for Editing System Administrator Information ..... 177
Figure 4.13 Window Transitions for Saving the NAS System LUs ..... 177
Figure 4.14 Window Transitions for Virus Countermeasures ..... 178
Figure 4.15 GUI Window Layout ..... 179
Figure 4.16 Define Cluster Configuration Window ..... 182
Figure 4.17 Modify Cluster Configuration Window ..... 184
Figure 4.18 Browse Cluster Status (Cluster / Node Status) Window ..... 186
Figure 4.19 Browse Cluster Status (Resource Group Status) Window ..... 190
Figure 4.20 Browse Cluster Status (Cluster / Node Status) Window ..... 196
Figure 4.21 Modify NNC Name Window ..... 198
Figure 4.22 List of Services Window ..... 200
Figure 4.23 NFS Service Management Window ..... 202
Figure 4.24 CIFS service and default setup in the CIFS Service Management window ..... 207
Figure 4.25 User Mapping Setup in CIFS Service Mgmt Window (user mapping uses RIDs) ..... 212
Figure 4.26 Mapping Setup in CIFS Service Mgmt Window (when user mapping uses LDAP) ..... 214
Figure 4.27 Select Authentication Mode Window ..... 218
Figure 4.28 Local Authentication Window ..... 220
Figure 4.29 NT Server Authentication Window ..... 221
Figure 4.30 NT Domain Authentication Window ..... 222
Figure 4.31 Active Directory Authentication Window ..... 223
Figure 4.32 CIFS Service Maintenance window ..... 225
Figure 4.33 CIFS Service Maintenance window (when user mapping uses RIDs) ..... 230
Figure 4.34 CIFS Service Maintenance window (when user mapping uses LDAP) ..... 231
Figure 4.35 CIFS Service Maintenance Window ..... 233
Figure 4.36 Public Key List Window ..... 235
Figure 4.37 Add Public Key Window ..... 236
Figure 4.38 FTP Service Management Window ..... 238
Figure 4.39 List of Mounted File Systems Window ..... 243
Figure 4.40 Select FTP Users Window ..... 244
Figure 4.41 System Setup Menu Window ..... 246
Figure 4.42 Setting Interface, Network, and Routing Information for gbe4 ..... 248
Figure 4.43 List of Data Ports window ..... 251
Figure 4.44 Negotiation Mode Setup Window ..... 253
Figure 4.45 List of Trunking Configurations Window ..... 255
Figure 4.46 Link Aggregation Setup Window ..... 258

Figure 4.47 Link Alternation Setup Window ..... 260
Figure 4.48 Edit Cascaded Trunking Window ..... 262
Figure 4.49 List of Interfaces Window ..... 265
Figure 4.50 Add Interface Window ..... 268
Figure 4.51 Edit Interface Window ..... 270
Figure 4.52 DNS, NIS, LDAP Setup Window ..... 272
Figure 4.53 List of Routings Window ..... 275
Figure 4.54 Add Routing Window ..... 277
Figure 4.55 Time Setup Window ..... 281
Figure 4.56 Syslog Setup Window ..... 282
Figure 4.57 Add Syslog Setup Window ..... 283
Figure 4.58 Edit Syslog Setup Window ..... 284
Figure 4.59 Log File Capacity Setup Window ..... 286
Figure 4.60 Edit File Capacity Window ..... 287
Figure 4.61 Core File Auto. Deletion Setup Window ..... 290
Figure 4.62 Edit System File Window ..... 292
Figure 4.63 Performance Tuning Window ..... 294
Figure 4.64 List of SNMPs Window ..... 296
Figure 4.65 Add SNMP Window ..... 297
Figure 4.66 Edit SNMP Window ..... 299
Figure 4.67 Select User Interface window ..... 301
Figure 4.68 List of Scanner Servers Window ..... 306
Figure 4.69 Add Scanner Server Window ..... 308
Figure 4.70 Edit Scanner Server Window ..... 309
Figure 4.71 Scan Conditions Window ..... 311
Figure 4.72 List of Users / Groups Window ..... 317
Figure 4.73 Add User Window ..... 318
Figure 4.74 Edit User Window ..... 320
Figure 4.75 Change Password (User Setup) Window ..... 321
Figure 4.76 Batch Operation Window ..... 323
Figure 4.77 List of Users / Groups Window ..... 328
Figure 4.78 Add Group Window ..... 329
Figure 4.79 Edit Group Window ..... 332
Figure 4.80 Assigning Device FilesUsed for File System (TagmaStore AMS 500) ..... 334
Figure 4.81 File System Capacity when LVM is Used ..... 335
Figure 4.82 List of File Systems Window ..... 337
Figure 4.83 Creating a File System Error Details Window ..... 340
Figure 4.84 Create New File System Window ..... 343
Figure 4.85 Creating a File Share after Creating a File System ..... 348
Figure 4.86 Edit Mount Window ..... 350
Figure 4.87 Edit Mount Window (at unmounting) ..... 353
Figure 4.88 Expand File System Window ..... 354
Figure 4.89 List of File Shares Window ..... 357
Figure 4.90 Create NFS File Share Window ..... 359
Figure 4.91 List of Mounted File Systems Window ..... 365
Figure 4.92 Edit NFS File Share Window ..... 366
Figure 4.93 Creating an NFS File Share Error Details Window ..... 371
Figure 4.94 List of File Shares (List of CIFS File Shares) Window ..... 372
Figure 4.95 Create CIFS File Share Window ..... 374
Figure 4.96 Write Disallowed Users / Groups Setup Window ..... 383

Figure 4.97 Write Allowed Users / Groups Setup Window ..... 384
Figure 4.98 Edit CIFS File Share Window ..... 386
Figure 4.99 Creating CIFS File Share Error Details Window ..... 392
Figure 4.100 List of Quota Information (User) Window ..... 398
Figure 4.101 List of Quota Information (Group) Window ..... 401
Figure 4.102 Quota Setup Window ..... 403
Figure 4.103 Default Quota Setup Window ..... 406
Figure 4.104 Grace Period Setup Window ..... 408
Figure 4.105 Monitoring Setup Window ..... 410
Figure 4.106 List of RAS Information (List of Messages) Window ..... 413
Figure 4.107 List of RAS Information (List of System Logs) Window ..... 416
Figure 4.108 List of RAS Information (List of Other Log Files) Window ..... 418
Figure 4.109 List of RAS Information (Batch-Download) Window ..... 422
Figure 4.110 List of RAS Information (Batch-download Window) ..... 427
Figure 4.111 List of RAS Information (List of Core Files) Window ..... 428
Figure 4.112 List of Programs Window ..... 431
Figure 4.113 Install Window ..... 433
Figure 4.114 Personal Info. Setup Window ..... 435
Figure 4.115 Change Password Window ..... 436
Figure 4.116 Save System LU Window ..... 438
Figure 4.117 Save NAS OS LU Window ..... 439
Figure 4.118 Schedule Settings for NAS OS LU Window ..... 442
Figure 4.119 Save NAS Cluster Management LU Window ..... 444
Figure 4.120 Schedule Settings for NAS Cluster Management LU Window ..... 447

Figure 5.1 Overall flow of operations using commands ..... 455

Figure 7.1 Login (End User) Window ..... 732
Figure 7.2 Window Transitions for End Users ..... 734
Figure 7.3 GUI Window Layout ..... 735
Figure 7.4 List of File Shares (List of NFS File Shares, end user) Window ..... 737
Figure 7.5 List of File Shares (List of CIFS File Shares, end user) Window ..... 738
Figure 7.6 Display Quota (User Quota Info.) Window ..... 739
Figure 7.7 Display Quota (Group Quota Info.) Window ..... 741
Figure 7.8 Password Setup Window ..... 743
Figure 7.9 User Info. Setup Window ..... 745
Figure 7.10 User Info Setup Window ..... 746

Figure 9.1 General Troubleshooting Procedure ..... 758

Figure B.1 Structure for Standard MIB Objects ..... 803
Figure B.2 Responding to SNMP Get Requests - Tables Referenced (Stnd MIB Objects) ... 804

Figure E.1 Configuration When NAS Modular System and Client in Same Network ..... 864
Figure E.2 Configuration When NAS Modular System and Client in Different Networks ... 865

# List of Tables


Table 1.1 Features of NAS Modular Systems ..... 33
Table 1.2 Times at which the warnings related to file system usage are issued ..... 39
Table 1.3 System Settings defined in NAS Manager ..... 58
Table 1.4 Programs and Settings Managed from the NAS Manager ..... 59

Table 2.1 Required Servers and Other Devices ..... 65
Table 2.2 Usable Combinations of Web Browsers and Operating Systems ..... 67
Table 2.3 Web Browser Font Settings ..... 68
Table 2.4 Web Browser Cache Settings ..... 68
Table 2.5 NAS Manager Server Configuration ..... 99
Table 2.6 Verification Tasks before Restarting CIFS Service ..... 113
Table 2.7 Configuration Tasks for Configuring the LDAP Server using OpenLDAP ..... 117
Table 2.8 Configuration Tasks for Configuring the LDAP Server using ADAM ..... 119
Table 2.9 Configuration Tasks for LDAP Server using Sun Java System Directory Server ..... 124
Table 2.10 Configuration Tasks for LDAP Server using Sun Java System Directory Server ..... 127

Table 3.1 Add Administrator Window Contents ..... 145
Table 3.2 Change Password (Account Administrator Setup) Window Information ..... 151

Table 4.1 Post-Operation Tasks ..... 157
Table 4.2 Available NAS Manager Functions (Main Menu window) ..... 165
Table 4.3 Information Specified in the Define Cluster Configuration Window ..... 183
Table 4.4 Information Changed in the Modify Cluster Configuration Window ..... 185
Table 4.5 Contents of the Browse Cluster Status (Cluster / Node Status) Window ..... 186
Table 4.6 Contents of the Browse Cluster Status (Resource Group Status) Window ..... 190
Table 4.7 Information Specified in the Modify NNC Name Window ..... 199
Table 4.8 Services and Management Tasks ..... 199
Table 4.9 Contents of List of Services Window ..... 200
Table 4.10 Contents of CIFS Service Management Window ..... 207
Table 4.11 Info Specified in CIFS Service and Default Setup Service Mgmt Window ..... 208
Table 4.12 User Mapping Setup in CIFS Service Mgmt Window (user mapping uses RIDs) ..... 212
Table 4.13 Mapping Setup in CIFS Service Mgmt window (when user mapping uses LDAP) ..... 214
Table 4.14 User Mapping Info ID Assignment in CIFS Service Maintenance window ..... 216
Table 4.15 User Mapping Setup in CIFS Service Mgmt window (when mapping is not used) ..... 217
Table 4.16 Information Specified in NT Server Authentication Window ..... 221
Table 4.17 Information Specified in NT Domain Authentication Window ..... 222
Table 4.18 Information Specified in Active Directory Authentication Window ..... 223
Table 4.19 Information displayed in the CIFS Service Maintenance window ..... 225
Table 4.20 User Mapping in CIFS Service Maintenance window (when mapping uses RIDs) ..... 230
Table 4.21 User Mapping in CIFS Service Maintenance window (when mapping uses LDAP) ..... 232
Table 4.22 Information Specified in Add Public Key Window ..... 236

Table 4.23 Contents of FTP Service Management Window ..... 239
Table 4.24 Add Interface and Add Routing Windows Information ..... 248
Table 4.25 Checking Negotiation Modes ..... 249
Table 4.26 Information Displayed in the List of Data Ports Window ..... 252
Table 4.27 Information to be specified in the Negotiation Mode Setup window ..... 253
Table 4.28 Information Displayed in the List of Trunking Configurations Window ..... 255
Table 4.29 Information to be Specified in the Link Aggregation Setup Window ..... 258
Table 4.30 Information to be Specified in the Link Alternation Setup Window ..... 260
Table 4.31 Information to be Specified in the Edit Cascaded Trunking Window ..... 263
Table 4.32 Information Displayed in List Of Interfaces Window ..... 265
Table 4.33 Contents of List of Routings Window ..... 275
Table 4.34 Information Specified in Add Routing Window ..... 278
Table 4.35 Log File Types and Descriptions ..... 287
Table 4.36 Editable System Files in Edit System File Window ..... 292
Table 4.37 Information Specified in Performance Tuning Window ..... 295
Table 4.38 Information Specified in the Add SNMP Window ..... 298
Table 4.39 Information Specified in Edit SNMP Window ..... 300
Table 4.40 Information specified in the Select User Interface window ..... 302
Table 4.41 Contents of List of Scanner Servers Window ..... 306
Table 4.42 Information Specified in Scan Conditions Window ..... 312
Table 4.43 Information Specified in Add User Window ..... 319
Table 4.44 Information Specified in Edit User Window ..... 320
Table 4.45 Information Specified for Batch Registration or Deletion of User Data ..... 323
Table 4.46 Batch Registration Error Messages, Causes, and Corrective Actions ..... 326
Table 4.47 Information Specified in Add Group Window ..... 331
Table 4.48 Contents of List of File Systems Window ..... 337
Table 4.49 Creating File System Error Details Window (Displayed Information) ..... 341
Table 4.50 Create New File System Window (Information Specified) ..... 344
Table 4.51 Edit Mount Window at File System Mounting ..... 351
Table 4.52 List of File Shares Window ..... 357
Table 4.53 Create NFS File Share Window ..... 360
Table 4.54 Edit NFS File Share Window ..... 367
Table 4.55 Creating an NFS File Share Error Details Window ..... 371
Table 4.56 CIFS Shares Data Displayed in List of File Shares Window ..... 373
Table 4.57 Create CIFS File Share Window ..... 375
Table 4.58 Write Disallowed and Write Allowed Users / Groups Setup Window ..... 385
Table 4.59 Edit CIFS File Share Window ..... 387
Table 4.60 Creating CIFS File Share Error Details Window (Information Displayed) ..... 392
Table 4.61 Information set for the quota management functionality ..... 393
Table 4.62 Information reported if an exceeded soft limit or grace period is detected .. 395
Table 4.63 User Quota Settings ..... 396
Table 4.64 List of Quota Information (User) Window ..... 398
Table 4.65 List of Quota Information (Group) Window ..... 402
Table 4.66 Quota Setup Window ..... 404
Table 4.67 Information specified in the Monitoring Setup window ..... 410
Table 4.68 Error Information that can be Displayed, Downloaded, and Deleted ..... 411
Table 4.69 List of RAS Information (List of Messages) Window ..... 413
Table 4.70 Log File Types in File Type Drop-Down List ..... 419
Table 4.71 List of Log Groups ..... 422
Table 4.72 Contents of List of RAS Information (List of Core Files) Window ..... 429

Table 4.73 Contents of List of Programs Window ..... 432
Table 4.74 Information Specified in Change Password Window ..... 437
Table 4.75 Contents of Save NAS OS LU Window ..... 440
Table 4.76 Contents of Schedule Settings for NAS OS LU Window ..... 443
Table 4.77 Contents of Save NAS Cluster Management LU Window ..... 445
Table 4.78 Info Specified in Schedule Settings for NAS Cluster Management LU Window ..... 448

Table 5.1 Operations Performed Using Commands and Document References ..... 451
Table 5.2 List of signals to be blocked with a command ..... 456
Table 5.3 Relationship Between Set ACL and Access Control Contents in CIFS Clients ..... 505
Table 5.4 Relationship Between Set and Access Permissions Contents for CIFS Clients ..... 506

Table 6.1 List of Commands ..... 531
Table 6.2 enas_cifscreate Arguments and Options ..... 535
Table 6.3 enas_cifsedit Arguments and Options ..... 540
Table 6.4 Information Displayed when enas_cifslist ..... 549
Table 6.5 Information displayed when executing the enas_clstatus command ..... 556
Table 6.6 Information Displayed when enas_devfreelist Command is Used ..... 563
Table 6.7 enas_dircreate Arguments and Options ..... 566
Table 6.8 Directory Modes Specifiable in the -m option of the enas_dircreate Command ..... 568
Table 6.9 enas_diredit Arguments and Options ..... 571
Table 6.10 ACL settings displayed when executing the enas_dirgetacl command ..... 574
Table 6.11 Information Displayed when enas_dirlist Command is Used ..... 578
Table 6.12 enas_dirlist Arguments and Options ..... 579
Table 6.13 Information specified as ACL entries in the enas_dirsetacl command ..... 582
Table 6.14 Information displayed when executing the enas_fcparm command ..... 586
Table 6.15 Information displayed when executing the enas_fsautofo command ..... 589
Table 6.16 enas_fscreate Arguments and Options ..... 591
Table 6.17 File System Division Sizes specified in -d Option ..... 592
Table 6.18 Information displayed when executing the enas_fsctl command ..... 603
Table 6.19 Information Displayed enas_fslist is Used ..... 608
Table 6.20 enas_fslist Arguments and Options ..... 611
Table 6.21 Information displayed when executing the enas_fsfullmsg command ..... 615
Table 6.22 enas_fsmount Arguments and Options ..... 617
Table 6.23 Information displayed when executing the enas_ndstatus command ..... 624
Table 6.24 Information displayed when executing the enas_nfs_mount_list command ..... 636
Table 6.25 Information displayed when executing the enas_nfs_opt_list command ..... 637
Table 6.26 Information displayed when executing the enas_nfslist command ..... 652
Table 6.27 enas_netstat Arguments and Options ..... 658
Table 6.28 enas_nfscreate Arguments and Options ..... 660
Table 6.29 enas_nfsdelete Arguments and Options ..... 665
Table 6.30 enas_nfsedit Arguments and Options ..... 666
Table 6.31 Information Displayed when Executing the enas_nfslist Command ..... 669
Table 6.32 enas_nfslist Arguments and Options ..... 669
Table 6.33 enas_ping Arguments and Options ..... 672

Table 6.34 Display When Executing enas_quotaget Command (quota info user or group) ..... 676
Table 6.35 Display When Executing enas_quotaget Command (default quota) ..... 678
Table 6.36 Display When Executing enas_quotaget Command (grace period) ..... 678
Table 6.37 Info Dsplayed When Executing enas_quotaget Command (monitoring method) ..... 678
Table 6.38 enas_quotaset Arguments and Options ..... 683
Table 6.39 Information displayed when executing the enas_rgstatus command ..... 695
Table 6.40 Information displayed when executing the enas_sshkeylist command ..... 708
Table 6.41 enas_traceroute Arguments and Options ..... 710
Table 6.42 Info Displayed When Executing stquota Command (quota of directory, user, or group) ..... 717
Table 6.43 Info Displayed When Executing stquota Command (default quota) ..... 718
Table 6.44 Information Displayed When Executing stquota Command (grace period) ..... 718
Table 6.45 Information displayed when executing the stquotalist command ..... 722

Table 7.1 NAS Manager Components for End Users (Menu Area) ..... 735
Table 7.2 Contents of Display Quota (User Quota Info.) Window ..... 739
Table 7.3 Contents of Display Quota (Group Quota Info.) Window ..... 741

Table 9.1 Cluster Statuses and Causes for Display ..... 766
Table 9.2 Node Statuses and Causes for Display ..... 766
Table 9.3 Resource Group Statuses and Causes for Display ..... 767
Table 9.4 Resource Group Error Information and Reasons for Display ..... 767
Table 9.5 Error Recovery Procedures for Cluster Statuses ..... 776
Table 9.6 Error Recovery Procedures for Node Statuses ..... 776
Table 9.7 Error Recovery Procedures for Resource Group Statuses ..... 777
Table 9.8 Error Recovery Procedures for Resource Group Errors ..... 778

Table A.1 List of Reserved Words in NAS Modular systems ..... 801

Table B.1 MIB Objects for Responding to SNMP Get Requests (standard MIB objects) ..... 804
Table B.2 MIB Objects for Responding to SNMP Get Requests (Hitachi MIB objects) ..... 805
Table B.3 System(1) Group ..... 805
Table B.4 Interfaces(2) Group ..... 807
Table B.5 at(3) Group ..... 808
Table B.6 ip(4) Group ..... 808
Table B.7 icmp(5) Group ..... 810
Table B.8 tcp(6) Group ..... 811
Table B.9 udp(7) Group ..... 812
Table B.10 >snmp(11) Group ..... 812
Table B.11 ucdavis(2021) Group ..... 814
Table B.12 snmpFrameworkMIB(10) Group ..... 817
Table B.13 snmpMPDMIB(11) Group ..... 818
Table B.14 snmpTargetMIB(12) Group ..... 818
Table B.15 snmpNotificationMIB(13) Group ..... 819
Table B.16 snmpUsmMIB(15) Group ..... 820
Table B.17 snmpVacmMIB(16) Group ..... 820

Table B.18 >enasExMibQuotaTable(2) Group ..... 821
Table B.19 >enasExMibNfs(4) Group ..... 822
Table B.20 >enasExMibCifs(5) Group ..... 826
Table B.21 >enasExMibNetwork(6) Group ..... 826
Table B.22 >enasExMibPerformManager(7) Group ..... 827
Table B.23 Specific Traps for NAS Modular system ..... 827
Table B.24 Groups of MIB Objects Used in SNMP Traps and Tables to be Referenced ..... 828
Table B.25 enasExMibQuotaTrapFS(3) Group ..... 828
Table B.26 enasExMibEvent(8) Group ..... 831
Table B.27 Severity Level for SNMP Trap Event ..... 832

Table C.1 Account Administrator Tasks ..... 833
Table C.2 System Administrator Tasks requiring NAS System LUs to be Saved ..... 833
Table C.3 Sys Admin Ops Requiring NAS System LUs to be Saved (when SN Modular is used) ..... 843
Table C.4 End-User Tasks ..... 844
Table C.5 Maintenance Tasks ..... 845

Table D.1 Interface Names Output to enas_routelist.log and log_ifconfig Difference ... 847
Table D.2 Information That Is Output to the enas_routelist.log File ..... 848
Table D.3 Information That Is Output to the log_ifconfig File ..... 851
Table D.4 Connection Statuses That Are Output to the log_interfaces_check File ..... 852
Table D.5 Output Showing Connection Statuses Between a NAS Unit and DNS Server ... 853
Table D.6 Output Showing Connection Statuses Between NAS Unit and NIS Server ..... 853
Table D.7 Output Showing Connection Statuses Between NAS Unit and NTP Server ..... 854
Table D.8 Output Statuses Between NAS Unit and LDAP Server for User Auth ..... 855
Table D.9 Output Statuses Between NAS Unit and Auth Server for CIFS Clients ..... 856
Table D.10 Output Statuses Between NAS Unit and LDAP Server for User Mapping ..... 857

# Chapter 1 Introducing NAS Manager

This chapter describes the features and functions of NAS Manager:

- Introducing NAS Features and Functions (see section 1.1)
- Reviewing the System Administration Capabilities (see section 1.2)
- Reviewing the End-user Capabilities (see section 1.3)

## 1.1 Introducing NAS Features and Functions

***Note:*** If you want to use the Hitachi Data Systems NAS Initial Configuration Wizard, you must launch it before you launch the NAS Manager. The Wizard will not launch if you do not execute in this order. Once you launch the Wizard, it must be allowed to fully complete. If the Wizard has not completed successfully, you need to use the NAS Manager GUI to check for the SSH public key with comment "---DEFAULTSETUPKEY---", which could be a security hole, and then delete it manually.

A NAS environment created using NAS Units connected with a TagmaStore AMS/WMS series disk array is called a *NAS Modular system*. NAS Manager is a program for efficiently setting up, operating, and managing the NAS Modular system.

Figure 1.1 illustrates an overview of a NAS Modular system:

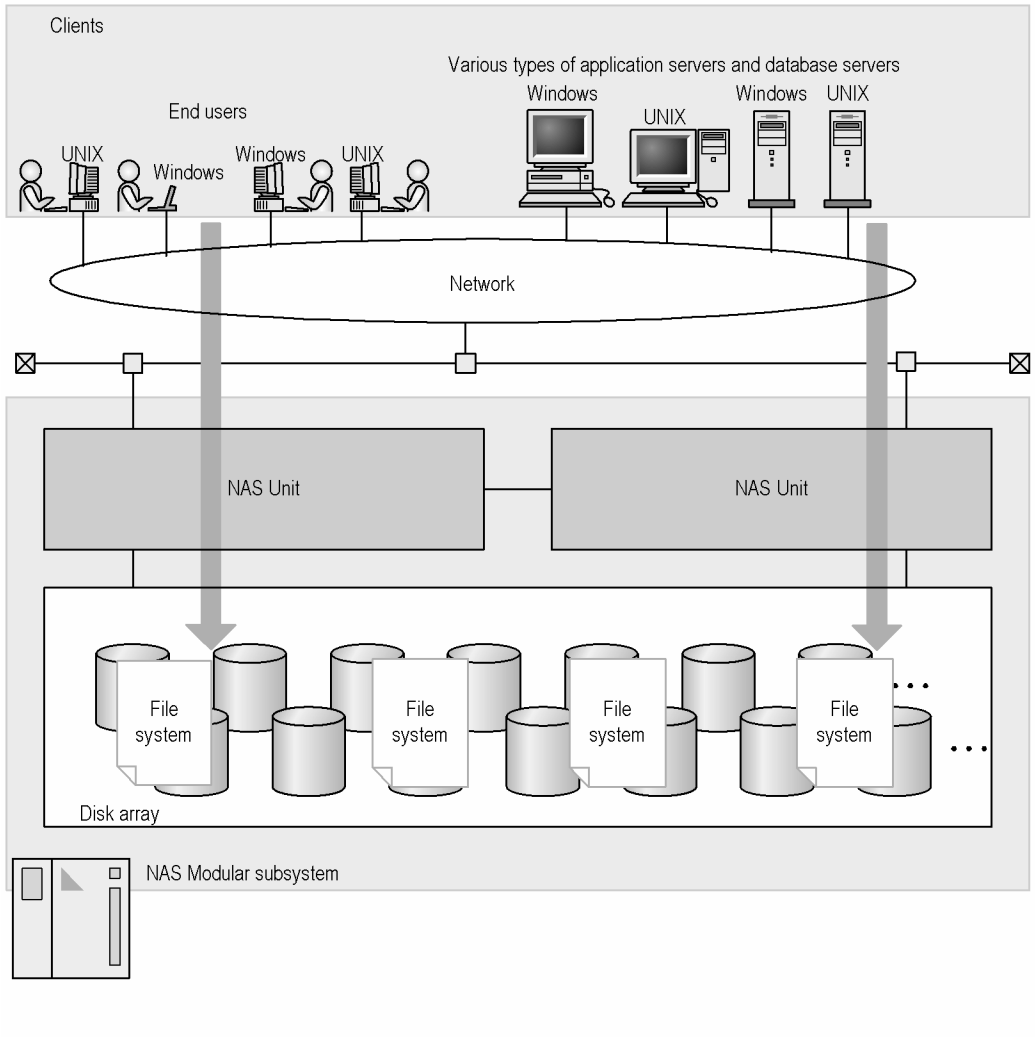



**Figure 1.1 Overview of a NAS Modular System**

Table 1.1 lists the features of NAS Modular systems.

**Table 1.1 Features of NAS Modular Systems**

| Feature | Description |
|---|---|
| Open data-sharing environment that utilizes legacy systems | The disk system enables integrated data management utilizing the enterprise's LAN environment already in place. Data within a disk system can be shared across heterogeneous platforms. |
| High-performance NAS environment | The NAS Units are built into the disk system, so overhead is lower than with a separate NAS server and disk system. |
| High availability | In a NAS Modular system, NAS Units make up a cluster system to reliably deliver services such as NFS and CIFS file shares provided by NAS function. If an error occurs in one NAS Unit, services can be relocated to the other NAS Unit in the cluster, ensuring service stability.<br>Services are quickly switched within a cluster through the shared cache of the TagmaStore® AMS/WMS Series. Used in conjunction with the failover function, the NAS Modular system enables online maintenance of hardware, software, and the services provided by the NAS Modular system. |
| Scalability | In a NAS Modular system, a cluster is configured as two NAS Units. You can increase the number of NAS Units to a maximum of eight. This assures scalability of the NAS environment. |
| Safety assuredness | In a NAS Modular system, data resources on disk systems can be protected from viruses by linking to a network scan server that scans for viruses. |
| High reliability (optional) | In a NAS Modular system, you can protect critical organization data resources that are shared on a disk system against loss or corruption.<br>By using NAS Backup Restore and NetBackup from the TagmaStore USP, you can obtain high-speed snapshots and online backup.<br>You can also create differential-data snapshots by using NAS Sync Image.<br>By using NAS Backup Restore, CCI, and ShadowImage, you can use the remote copy function to duplicate, into a different cabinet, data in a file system that is shared in a NAS Modular system. |
| Efficient deployment of a NAS Modular system | A system administrator can use the NAS Manager GUI or use commands to easily carry out the tasks involved in deploying a NAS Modular system: including cluster configuration, network setup, system setup, user setup, and file system creation. |
| NAS Modular system operation, management, and error monitoring | A system administrator can use the NAS Manager GUI or commands to check file system usage, extend a file system, and perform error monitoring from any client *//Reviewers: Is "client" the same as "machine"?//* in the network.<br>End users can use the NAS Manager to check file system usage. |
| Linking NAS Manager with SNMP Manager | NAS Manager can be linked with SNMP Manager for obtaining information on NFS, CIFS, networks, and error messages as well as for monitoring disk usage. |
| Virus-scanning function | If a NAS Anti-Virus Agent license has been set up, NAS Anti-Virus Agent can be linked with a network scan server for virus-scanning. This allows you to scan for viruses, set scan conditions and reporting scan results. |
| Backup and restore function | NAS Manager supports standard backup and restore, compliant with the NDMP protocol. This allows a system administrator to perform online backups. |

| Feature | Description |
|---|---|
| Differential-data snapshot function (optional) | Allows you to create differential-data snapshots of file systems in a disk system. A snapshot is useful when an end user has incorrectly modified data in a file system shared over a NAS Modular system.<br>Once the system administrator has created a differential-data snapshot, the end user is able to directly reconstitute required data. |
| Linkage with the HiCommand series of programs | Linking NAS Manager with the HiCommand Device Manager enables the NAS Manager to be launched from the Device Manager GUI without logging on to NAS Manager. In addition, by linking with Tuning Manager, you can view data such as usage information about the file systems managed by NAS Manager and NAS OS performance information. |

In a NAS Modular system, the NAS environment is set up by installing the NAS OS and the requisite programs for NAS operation on a NAS OS LU in a disk system, and by using such programs from a NAS Unit. The NAS OS includes the NAS function and the following functions required for NAS Manager operation:

- CIFS® server
- NFS® server
- FTP server
- LVM
- XFS™
- RAID driver
- Web server
- NTP client
- SNMP agent
- DNS client
- NIS client
- LDAP client
- Failover
- Installer

Running under the NAS OS, the NAS Manager program supports NAS Modular system setup, operating status monitoring, modification of system settings, error monitoring, and data backup and restoration. You can access NAS Manager from any machine. The position of NAS Manager in a NAS Modular system is shown in Figure 1.2.

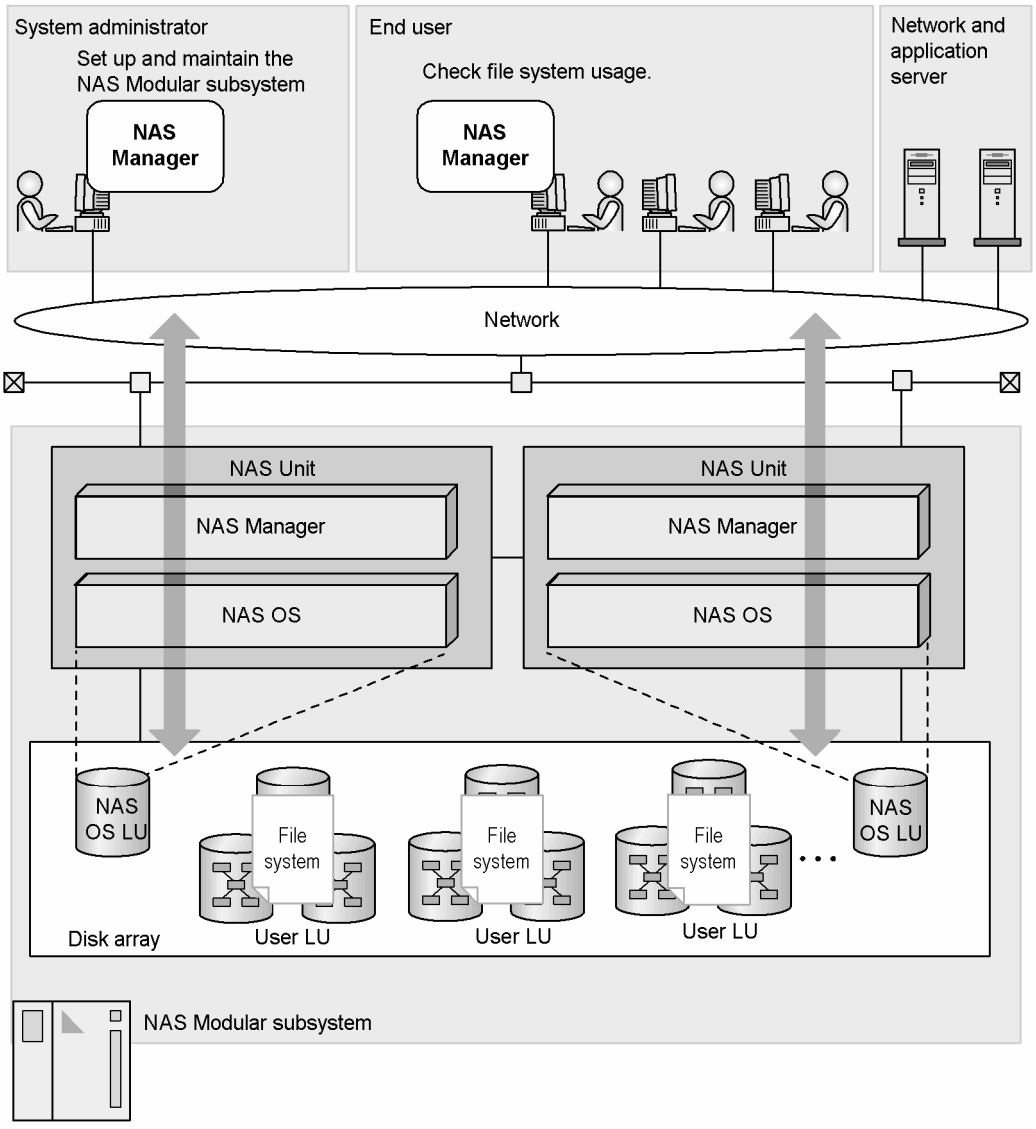



**Figure 1.2 Position of NAS Manager in a NAS Modular System**

NAS OS and NAS Manager are contained in a NAS OS LU assigned for each NAS Unit. The file system is created on a user LU:

- End users using a file system can use the NAS Manager to check the status of their file system usage.
- A system administrator can use the NAS Manager to perform NAS Modular system setup and management tasks, including creating file systems and monitoring for errors.

## 1.2 Reviewing System Administration Capabilities

A system administrator manages a NAS Modular system from the NAS Manager. This section describes the basic operations for using the NAS Manager GUI, and the system administration capabilities that are provided in NAS Manager.

### 1.2.1 Managing File Systems

Based on XFS™, a NAS Modular system builds a hierarchical file system that assures fast file access and high reliability. The files that clients create when accessing a file system are stored as data within the disk array.

For file system management, NAS Manager also provides the following functionalities:

- Create and manage a file system
- Issue warnings about file system usage
- Perform failover automatically when a file system is blocked

#### 1.2.1.1 Creating and managing a file system

As a system administrator, you can use NAS Manager to create and manage a file system as follows:

- Create a file system
- Extend a file system
- Mount and unmount a file system

In NAS Manager, you can create a file system by configuring one or more device files on the disk array as a logical volume. To configure a logical volume, you use a logical volume manager (LVM). Creating a logical volume allows the file system to be managed transparently, so that users are unaware of the device file structure. You can also create a file system containing a single device file, without a logical volume. If you use a LVM, you can extend the file system capacity by adding another device file to a previously created file system.

To improve compatibility between the NAS Modular system and CIFS client environments, you can also set a file system to record the creation time for a file separately from the last access time (`atime`), last change time (`ctime`), and last modification time (`mtime`).

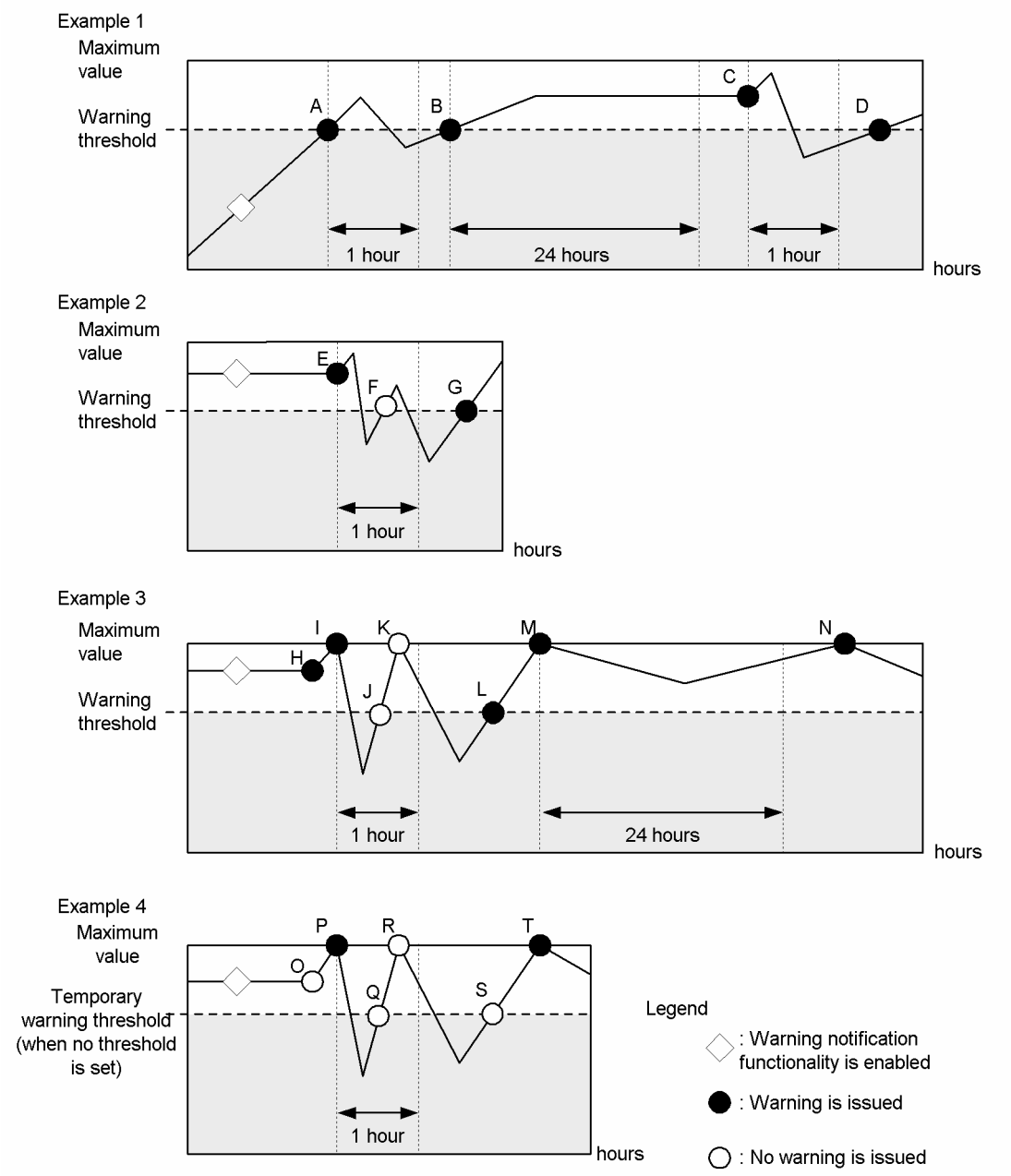
Note, however, that NFS clients cannot reference the creation time for the file even when recording of the file creation time is enabled.

#### 1.2.1.2 Issuing warnings related to file system usage

NAS Manager provides functionality that uses an SNMP trap to issue warnings about file system usage if the file system usage exceeds a predefined value (warning threshold) or reaches a maximum value.

When the system is first installed, NAS Manager is not set to issue warnings related to file system usage. A system administrator can use NAS Manager to enable or disable warning notification. The system administrator can also view the warning notification settings and change the warning threshold.

When warning notification is enabled, and the file system usage exceeds the warning threshold or reaches the maximum value, messages KAQG90002-W to KAQG90005-W are issued to the SNMP server by an SNMP trap. Once a warning has been issued by an SNMP trap, the times at which the warning is issued change depending on the file system usage. The following figure shows the times at which the warnings are issued.


Example 1
Maximum value
Warning threshold
A
B
C
D
1 hour
24 hours
1 hour
hours
Example 2
Maximum value
Warning threshold
E
F
G
1 hour
hours
Example 3
Maximum value
Warning threshold
H
I
J
K
L
M
N
1 hour
24 hours
hours
Example 4
Maximum value
Temporary warning threshold (when no threshold is set)
O
P
Q
R
S
T
1 hour
hours
Legend
: Warning notification functionality is enabled
: Warning is issued
: No warning is issued

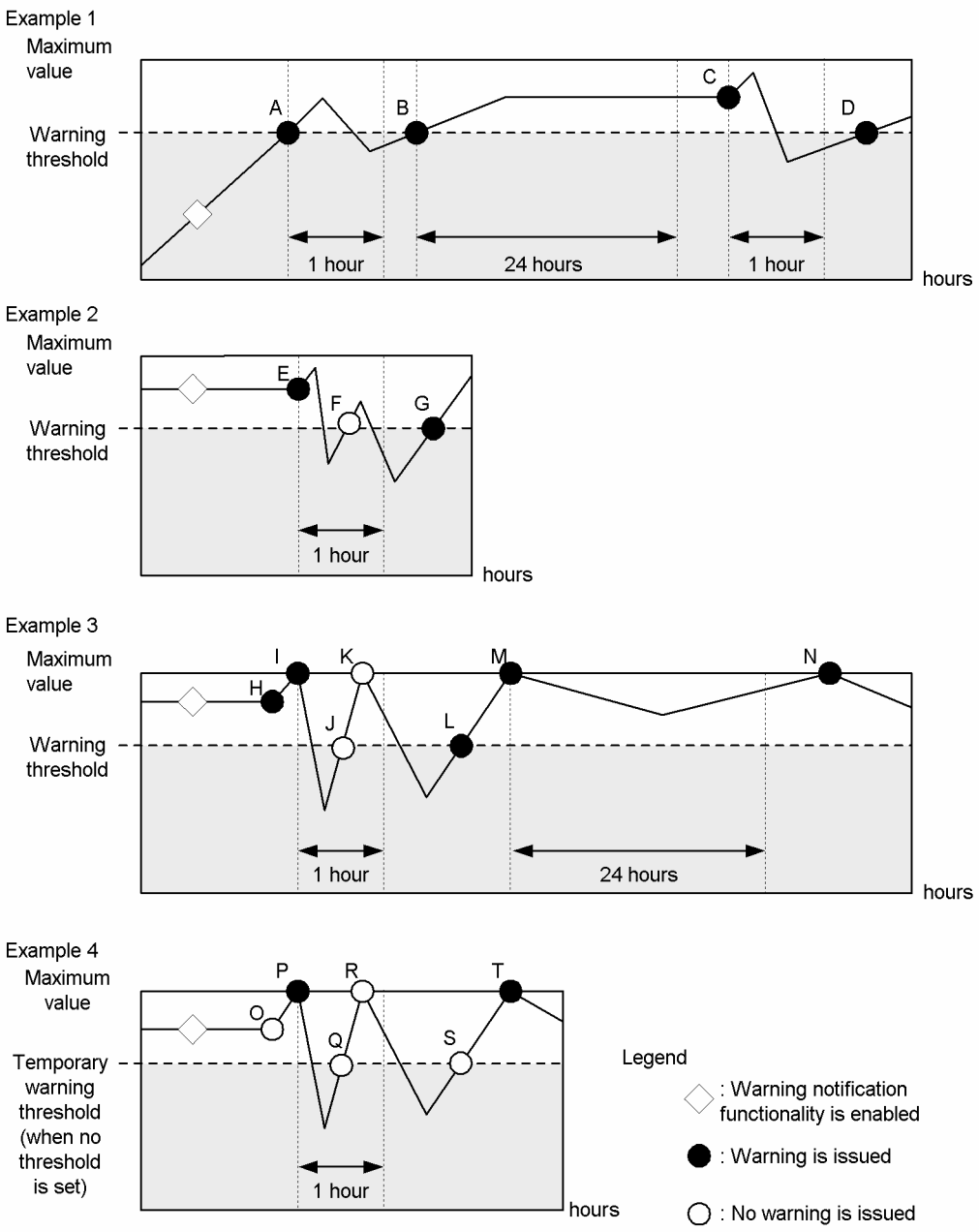



**Figure 1.3 When warnings related to File Systems are Issued**

The following table lists and describes the times at which the warnings related to file system usage are issued.

**Table 1.2 Times at which the warnings related to file system usage are issued**

| State | Times at which the warnings related to file system usage are issued | Symbols in the figure |
|---|---|---|
| File system usage exceeds the warning threshold | When file system usage exceeds the warning threshold for the first time after the warning notification has been enabled | A |
| | When file system usage exceeds the warning threshold at the time the warning notification has been enabled, and then the file system is used | E, H |

| State | Times at which the warnings related to file system usage are issued | Symbols in the figure |
|---|---|---|
| | When both of the following conditions are satisfied:<br>▪ At least one hour has passed since the warning was issued for the last time the warning threshold was exceeded. #1<br>▪ File system usage exceeded the warning threshold. | B, D, G, L |
| | When both of the following conditions are satisfied:<br>▪ The warning threshold has been exceeded for at least 24 hours since the warning was issued for the last time the warning threshold was exceeded.<br>▪ The file system was used. | C |
| File system usage reaches the maximum value | When file system usage reaches the maximum value for the first time after warning notification has been enabled | I, P |
| | When both of the following conditions are satisfied:<br>▪ At least one hour has passed since the warning was issued for the last time the file system usage reached the maximum value. #1<br>▪ The file system usage once was below the warning threshold and then reaches the maximum value again. #2 | M, T |
| | When both of the following conditions are satisfied:<br>▪ The warning threshold has been exceeded for at least 24 hours since the warning was issued for the last time the file system usage reached the maximum value.<br>▪ The file system usage reaches the maximum value again. | N |

***Note:*** Regardless of the situation, the warning notification state is reset to the first state if any of the following operations are performed:

- Warning notification is disabled and then enabled again.
- The warning threshold is changed.
- The file system is unmounted and then mounted again.

#1:

Once a warning has been issued, the same warning is not issued until one hour passes (F, J, K, and R in the figure).

#2:

If the warning threshold is 0, a dummy warning threshold is set to judge whether file system usage has been below the warning threshold after reaching the maximum value. An SNMP trap is not issued even when file system usage exceeds the dummy warning threshold (O, Q, and S in the figure).

### 1.2.1.3 Performing failover automatically when a file system is blocked

The system administrator can use NAS Manager to enable or disable automatic failover functionality when a file system is blocked.

When automatic failover is enabled:

A failover occurs automatically if a file system is blocked. The other node in the cluster continues to provide services for the other file systems. Note that the blocked file system must be deleted.

When automatic failover is disabled:

A failover does not occur if a file system is blocked. The node currently being used continues to provide services for the other file systems.

### 1.2.2 Sharing Files and File Systems using NFS and CIFS Protocols

In NAS Manager, files and file systems can be shared using the NFS and CIFS protocols. This allows users on heterogeneous operating systems such as UNIX® and Windows® to access the file systems on a disk array over their networks.

Figure 1.4 illustrates the general process when clients access data in a file system.

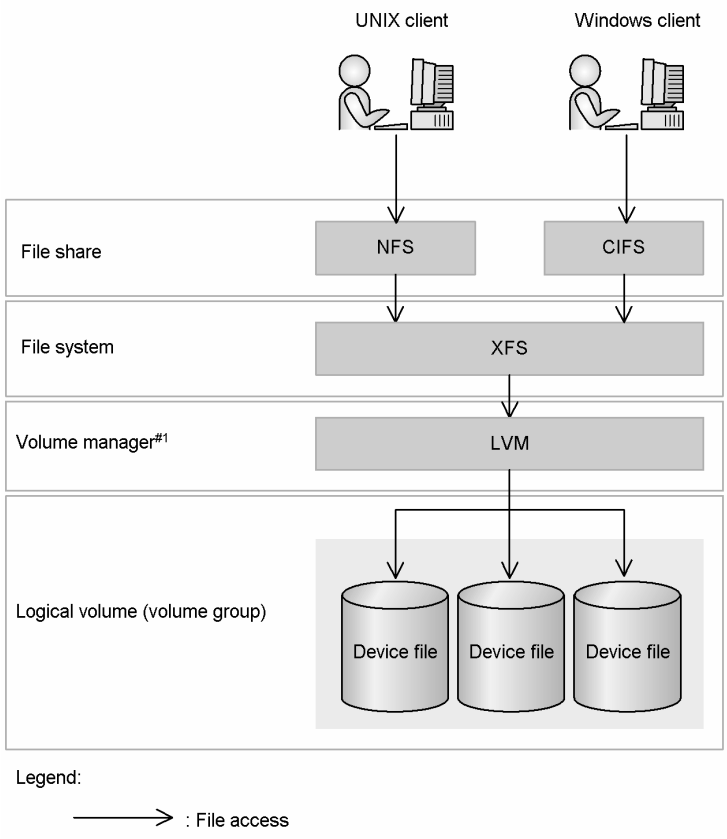



**Figure 1.4 General Process during File Access**

You can use the NAS Manager to create NFS and CIFS shares. The following information can be set for an NFS share:

- Write permission
- Anonymous mapping
- Check of access permissions of the sending port
- Subtree check
- Check of access permissions when a lock is requested

The following information can be set for a CIFS share:

- Share name and comment
- Write permission
- Permission to browse read-only shares
- Users and groups granted read-only access or read/write access
- ACL settings

For details on using the NAS Manager to manage the shares of file systems and files, see section 4.11.

### 1.2.3 Managing User Access to File Systems

In a NAS Modular system, users on heterogeneous operating systems such as UNIX® and Windows® can access, over the network, the file systems on a disk array. Using NAS Manager, a system administrator can manage user information and group information of users accessing the file systems.

Within a file system, users and groups are managed by ID numbers. A system administrator registers user information to assign a name to each ID number. User information is also required when a quota or ACL is set.

### 1.2.4 Methods of Managing File System Users

In a NAS Modular system, users can access the file systems in a disk array from different operating systems, such as UNIX and Windows, over the network. Because users and groups are managed using IDs in a file system, a system administrator must manage user information, such as user IDs and group IDs. User information is also required when a quota or ACL is set.

In a NAS Modular system, the system administrator can use the following methods to manage user information, such as user IDs and group IDs. The system administrator must choose the appropriate method after considering how the NAS Modular system will be operated.

Using NAS Manager to manage user information (recommended)

In this method, information for a maximum of 2,000 items of information about users can be managed. The system administrator registers group information from the **Add Group** window and registers user information from the Add User window. The system administrator can also use the **Batch Operation** window to register and remove information about multiple users by using a CSV-format file.

Using the NIS server or the LDAP server (or both) to manage user information (recommended)

Besides NAS Manager, the NIS server and LDAP server can manage 50,000 items of information about users. In this method, the NIS server and LDAP server are used to manage the information for a maximum total of 50,000 users and 50,000 groups. The system administrator registers user information by setting server information from the **DNS, NIS, LDAP Setup** window.

Using Active Directory or the NT domain to manage user information

Active Directory or NT domain can manage 24,000 items of information about users who use the CIFS service. To use this method, user mapping must be used, or the users corresponding to the managed user information must be managed by NAS Manager, an NIS server, or an LDAP server (used for user authentication). When using user mapping, the system administrator must specify the necessary settings in the **CIFS Service Management** window.

In this method, the information for a maximum of 24,000 users who use the CIFS service can be managed. User mapping can also be used for management of user information. The system administrator sets the information necessary for user mapping from the **CIFS Service Management** window.

### 1.2.5 Using Quota Management

The *quota management* function restrict disk usage (block usage) and file-and-directory usage (i-node usage) to prevent specific users or groups from using too much disk capacity. Figure 1.5 illustrates how quota management works.

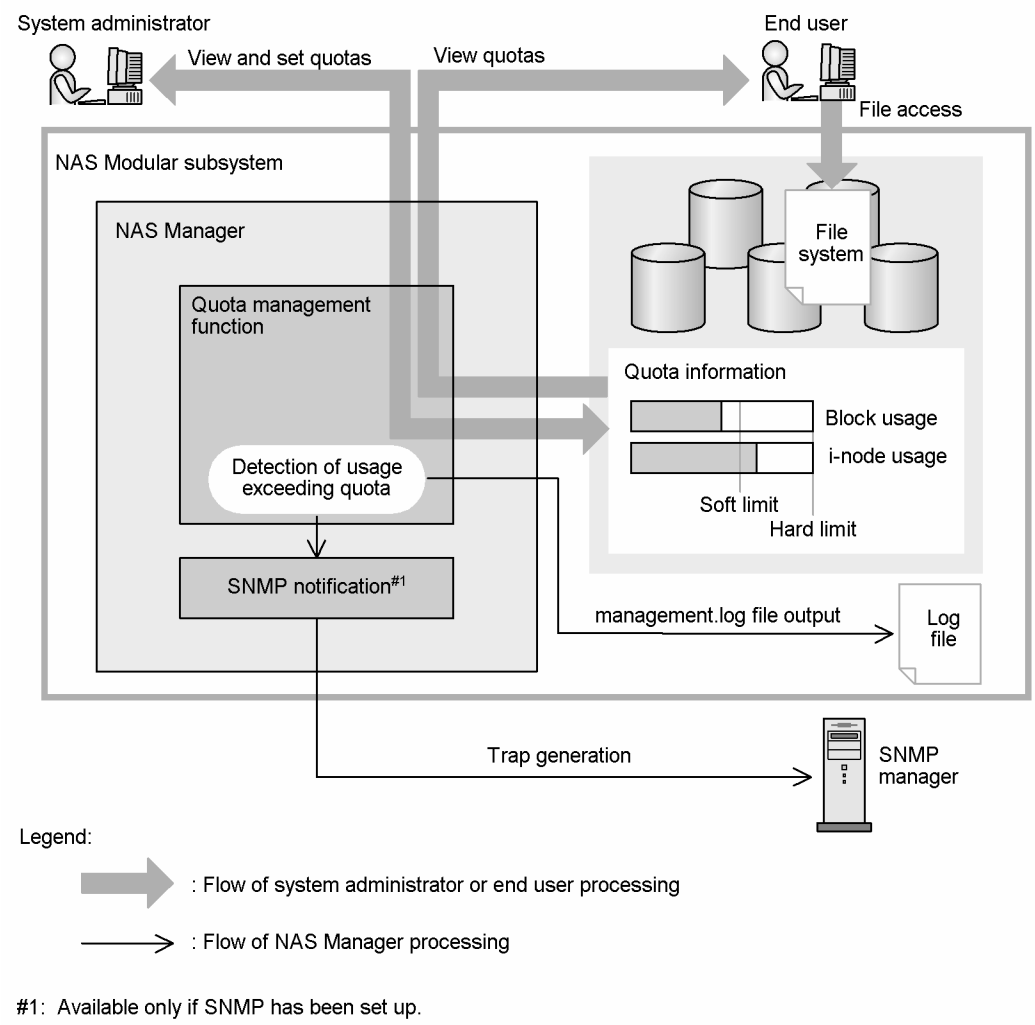



**Figure 1.5 Overview of Quota Management**

A system administrator can set a quota for a specific user, group, or directory from NAS Manager to restrict the block usage and i-node usage in a file system or directory. The system administrator can also set a *default quota* for users, for whom a quota has not been specifically set, to restrict their block and i-node usage. After the default quota is set, if a user for whom a quota has not been set starts using the file system, the default quota is used to restrict the block usage and i-node usage for that user.

The NAS Modular system also provides quota management for each file system or each directory. In the NAS Modular system, quotas set on a directory basis are called *subtree quotas*.

### 1.2.5.1 Managing quotas for each file system

When managing quotas for each file system, you set user or group quotas by using the GUI or commands from NAS Manager.

When a quota has been set for each file system, NAS Manager monitors the block usage and i-node usage of individual users. If users or groups are detected who have exceeded the *soft limit* (the value used for alert), or who have exceeded the *grace period* (the time period in which users can continue to create or update files after their usage of disk space exceeds the soft limit), a notification will be generated via the `management.log` file or an SNMP trap.

A notification using an SNMP trap can be generated in two modes: *individual notification mode* and *summary notification mode*. In individual notification mode, quota information for an individual user or group is reported. In summary notification mode, only the number of users and groups who have exceeded the soft limit or grace period is reported. A system administrator can also use commands to view the file system usage of only those users and groups who have exceeded the soft limit or grace period.

### 1.2.5.2 Managing subtree quotas

A subtree quota is set for each directory immediately under the mount point directory.

When subtree quotas have been set, the maximum block usage and i-node usage can be managed for each directory. Subtree quotas can also be used to manage the maximum block usage and i-node usage for a user or group (for each directory).

When multiple file shares have been created in one file system, by setting subtree quotas for the shared directory created immediately under the mount point directory, you can flexibly manage the capacity of each file share.

### 1.2.5.3 Typical example of quota management

The following figure shows a typical example of quota management.

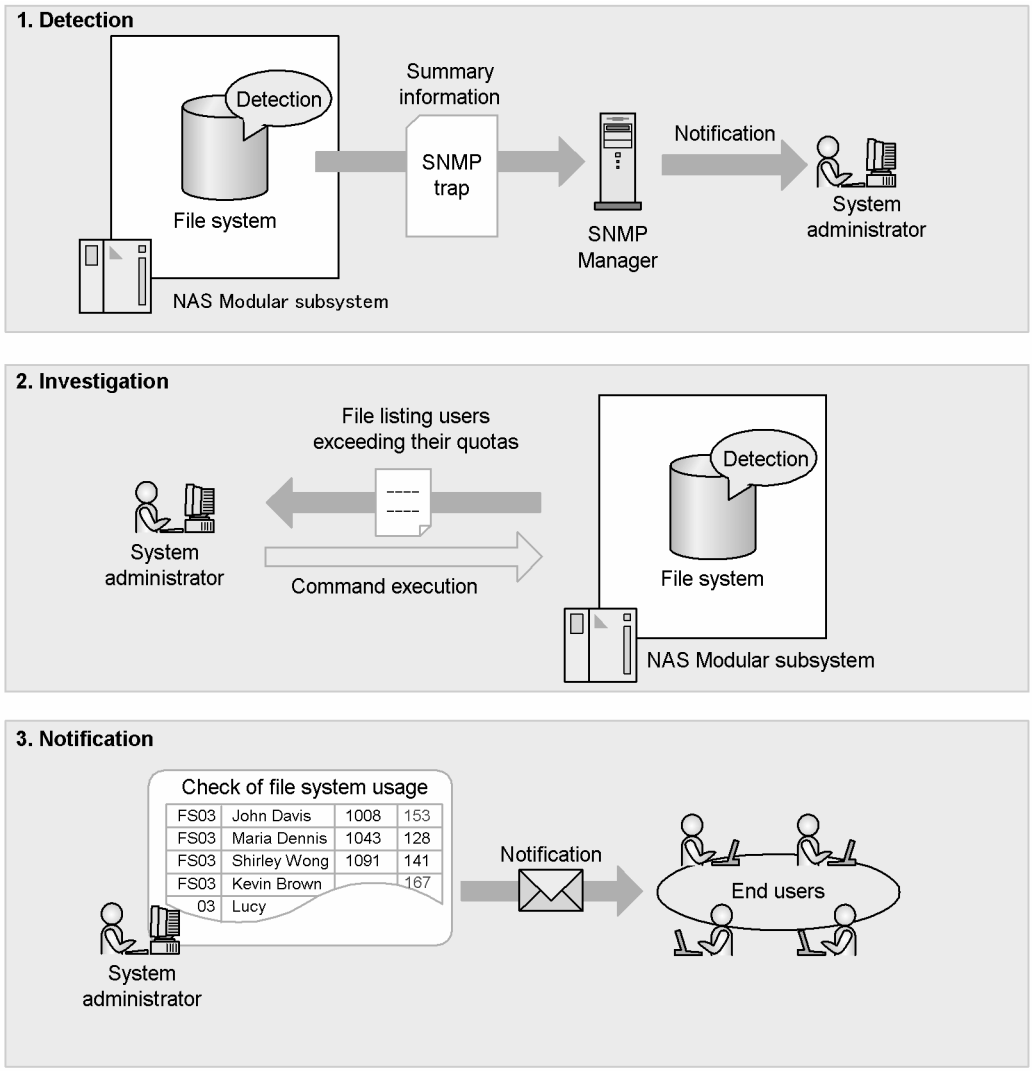



**Figure 1.6 Example of quota management**

On receipt of a summary notification via an SNMP trap from the SNMP manager, the system administrator uses commands to obtain a list of users who have exceeded their quotas. After editing the list with spreadsheet software or a text editor, the system administrator checks the file system usage of the end users. If necessary, the system administrator notifies the end users about their file system usage often changing the quota settings or asking users to delete unnecessary data.

The combination of summary notification and command operation gives the system administrator a comparatively easy way to manage file system usage individually for many users and groups.

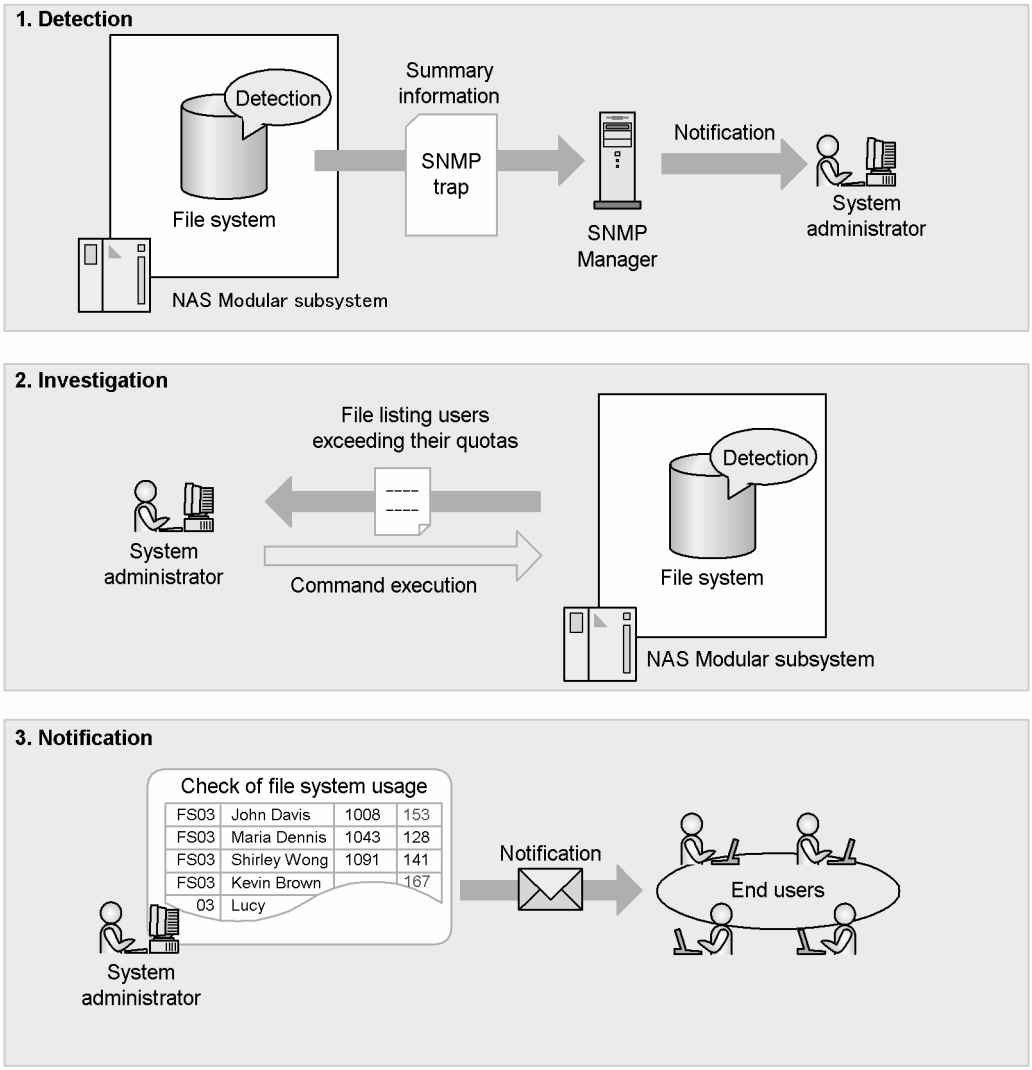



**Figure 1.7 Example of Quota Management**

On receipt of a summary notification via an SNMP trap from the SNMP manager, the system administrator uses commands to obtain a list of users who have exceeded their quotas. After editing the list with spreadsheet software or a text editor, the system administrator checks the file system usage of the end users. If necessary, the system administrator notifies the end users about their file system usage.

The combination of summary notification and command operation gives the system administrator a comparatively easy way to manage file system usage individually for many users and groups.

To manage quotas for users or groups that do not use an NIS server or user mapping, a system administrator must register the user information or group information in a NAS Modular system. For details on registering user and group information, see section 4.9.

For file-system users who do not have a quota, a default quota can be set to prevent the users from using too much disk space. After the default quota is set, it will be applied to a user who does not have a set quota and who starts using the file system.

For details on using the NAS Manager to manage quotas, see section 4.12_Managing Clusters, Nodes, and Resource Groups

In a NAS Modular system, a cluster is configured with two NAS Units to enhance the system reliability. If an error occurs in one NAS Unit, services continue on the other NAS Unit in the cluster. NFS and CIFS file-sharing services provided by the NAS Modular system remain active without any downtime. In a NAS Modular system, switching services from one NAS Unit to the other in the cluster if an error occurs is called *failover*.

When returning a NAS Modular system to normal operation after it has been temporarily restricted due to a failover, or when performing maintenance of the NAS Modular system, a system administrator must check or control the status of the failover function by using the NAS Manager.

To manage a cluster, nodes, and resource groups, a NAS Modular system allows you to:

- Manage cluster configuration information,
- Perform failover of resource groups when an error occurs, and
- Control failover function.

### 1.2.5.4 Managing Cluster Configuration Information

In a NAS Modular system, each NAS Unit in a cluster is called a *node*. Information about NFS share settings, CIFS share settings, the service IP address, and the file system mounted on a node is managed together as a *resource group*. In normal operation, a single resource group runs on a single node. The following figure illustrates cluster configuration in a NAS Modular system.

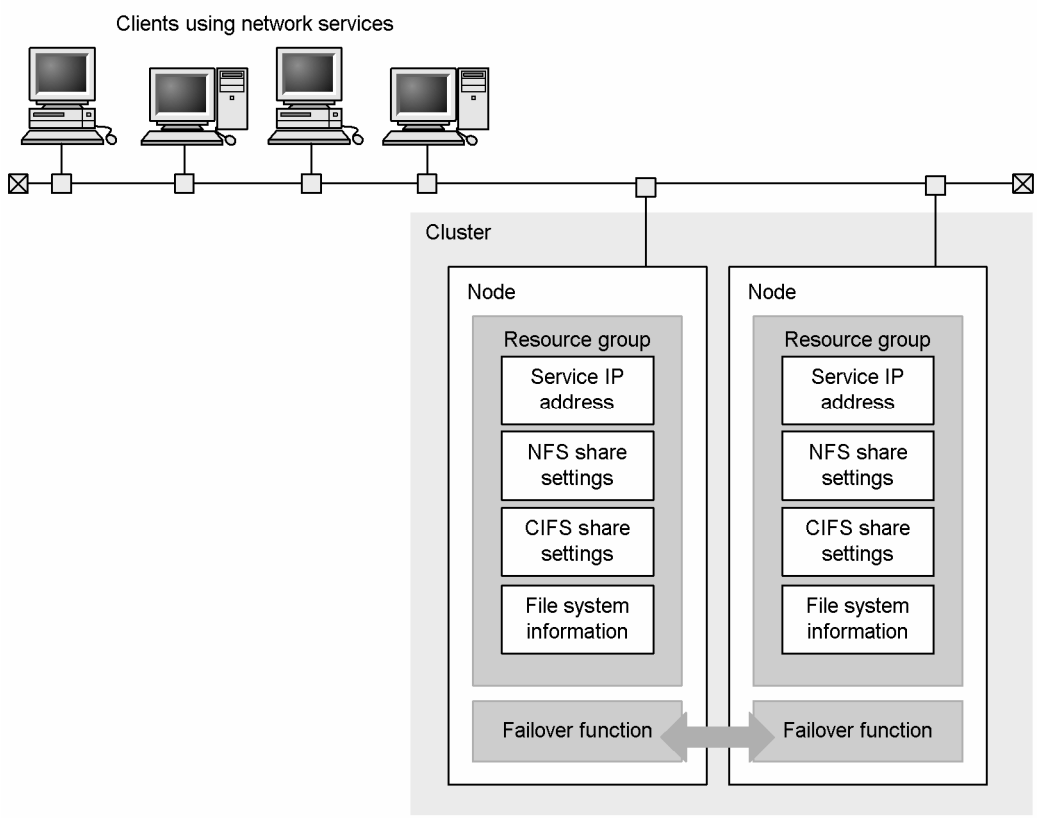



**Figure 1.8 Cluster Configuration in a NAS Modular system**

The NAS Modular system manages the cluster configuration information and resource group information set by a system administrator from the NAS Manager. This information is automatically synchronized across the nodes. Therefore, if a system administrator changes the cluster configuration settings on one node, there is no need to change anything on the other node in the cluster. For details on setting cluster information, see section 4.5.1.

### 1.2.5.5 Performing Failover when an Error Occurs

The relocation of a resource group to the other node in the cluster is known as *failover*. The migration of a failed-over resource group back to the original node is called *failback*.

The NAS Modular system monitors the system for possible errors. If an error requiring failover occurs, the error information is reported to the failover function, and failover starts automatically. A system administrator can use the NAS Manager to verify that a failover has occurred.

Failover in a NAS Modular system allows active services to continue without interruption during error recovery, hardware replacement, or other maintenance.

The following two figures show the general process for client services at normal operation, and the general process for client services after failover.

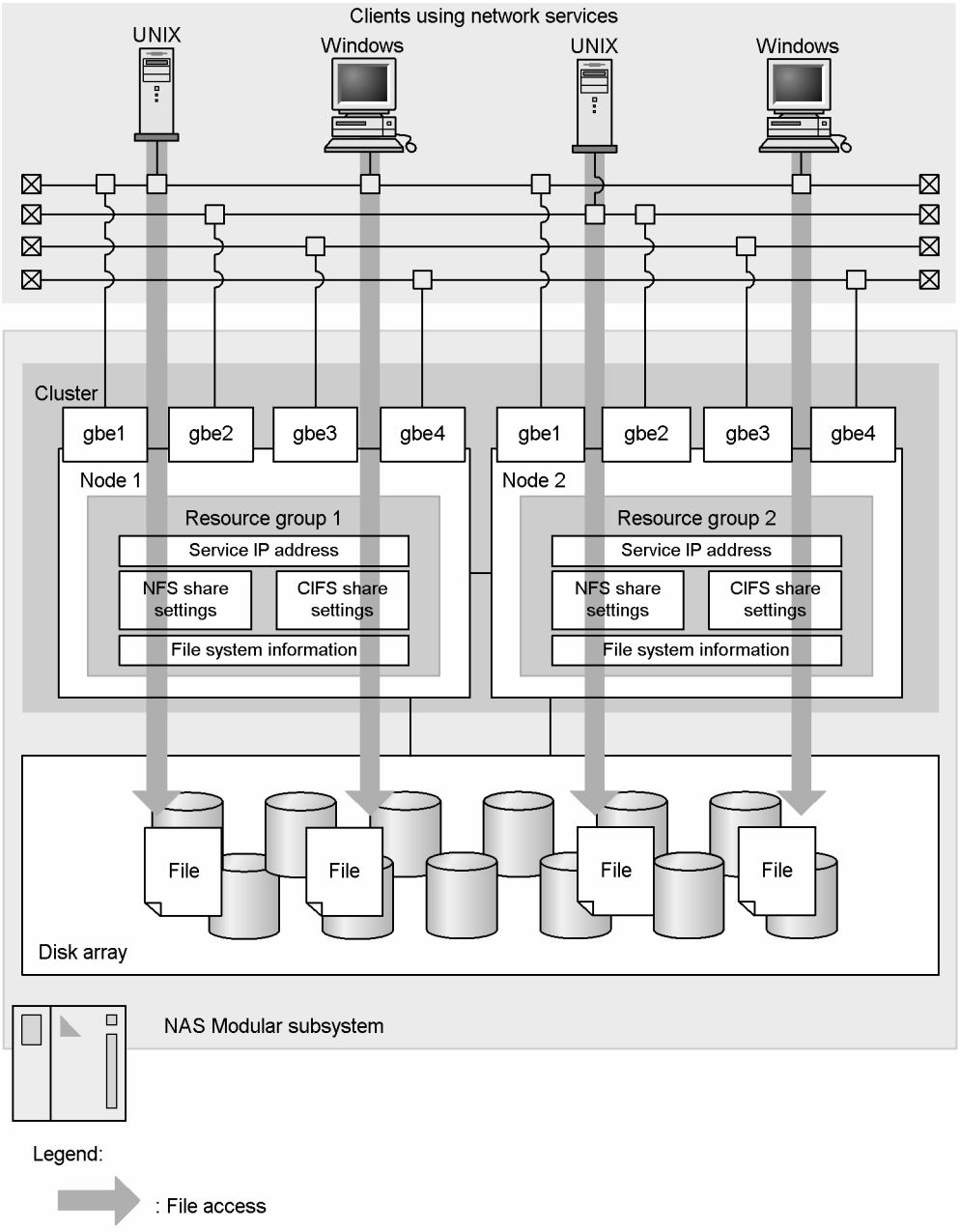



**Figure 1.9 General Process for Client Services (normal operation)**

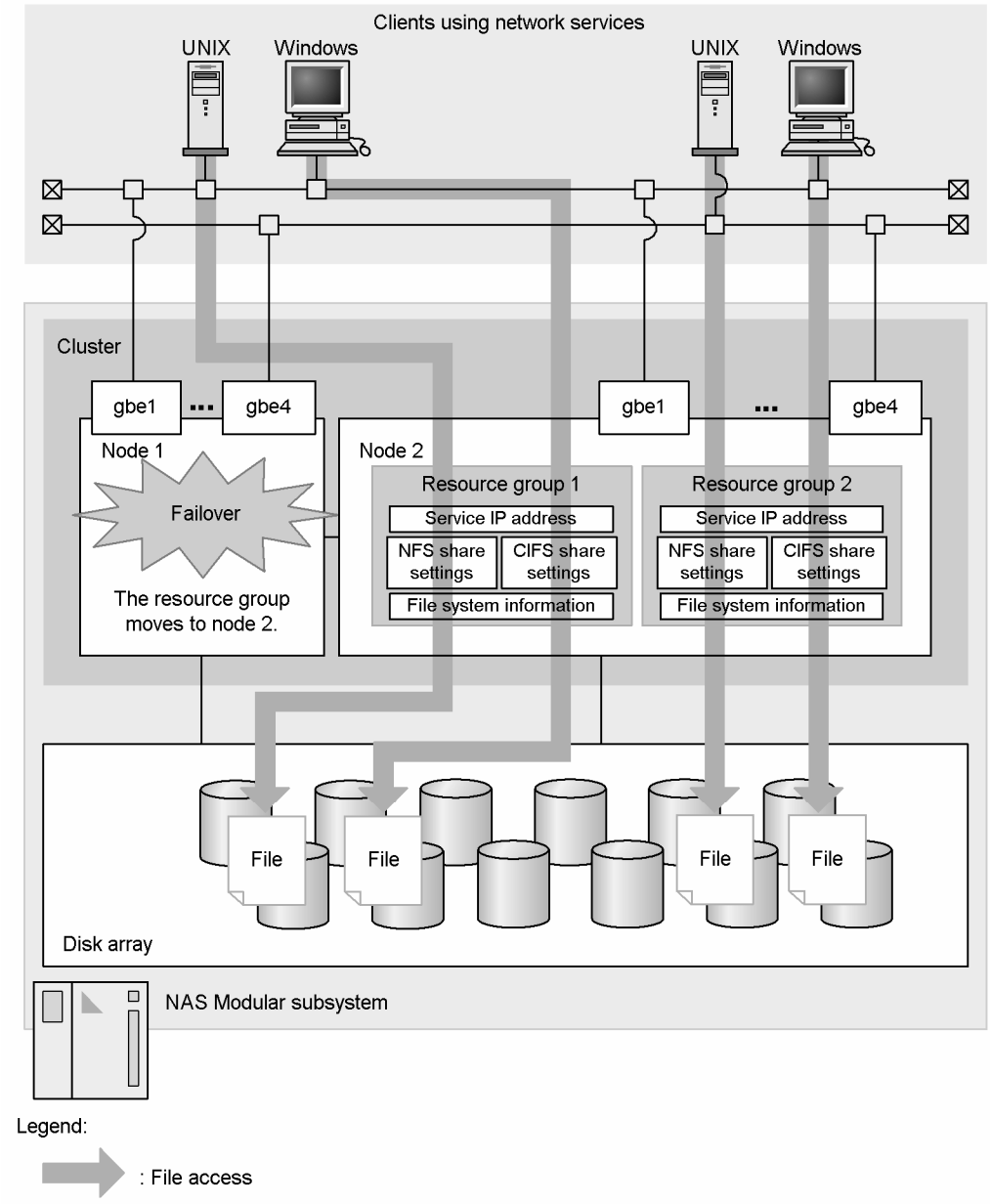



**Figure 1.10 General Process for Client Services (at failover)**

In a NAS Modular system, the IP address that the client uses to connect a service of a resource group is called a *service IP address*. A service IP address is associated with the fixed IP address of each NIC in the node. When a resource group is relocated to the other node in the cluster, the system associates the service IP addresses of the resource group with the corresponding fixed IP addresses of NICs in the destination node. For example, the service IP address previously associated with the fixed IP address of the NIC (eth1) in the original node is associated with the fixed IP address of the NIC (eth1) in the destination node.

In a NAS Modular system, a different file system is mounted at each node to provide services. A client accesses files by using a service IP address to connect to the desired service. By planning and carrying out network configuration and mounting file systems, a system administrator can distribute file accesses to both nodes and balance the loads between the nodes.

If an error occurs, a failover occurs and the resource group moves to the other node. Since the service IP address is transferred to the other node, the client can continue accessing the files using the same environment.

Normal operation restarts automatically when a failed-over resource group is failed back to the original node after error recovery. A system administrator can fail back a resource group by changing the node on which the resource group is running. As a system administrator, if you need to carry out failback, you should follow the instructions of your HDS representative. For details on manual failback, see section 4.5.11.

### 1.2.5.6 Controlling Failover Function

In a NAS Modular system, you can control failover so that active services can continue while a cluster node is stopped for maintenance. The NAS Modular system also provides means for error recovery of the failover function itself without disrupting services. You can use the NAS Manager to monitor resource groups, and check whether an error occurred in the failover function.

To control the failover function, you can complete the following tasks:

- **Stop and start clusters and nodes**

  You can stop and start a cluster or node to carry out system maintenance or error recovery. When stopping or starting a cluster or node, the failover function on that cluster or node also stops or starts:

  - Stopping a cluster disables failover on each node in the cluster, and stops all resource groups running on the cluster nodes. The services provided by the resource group also stop.

    For details on stopping and starting a cluster, see section 4.5.4.

  - Stopping a node moves the resource group running on that node to the other node in the cluster, and disables failover on the original node.

    For details on stopping and starting a node, see section 4.5.5.

- **Stop and start a resource group**

  You can start and stop services provided by a selected resource group. For details, see section 4.5.8.

- **Perform a forced stop for a cluster, node, or resource group**

  In the event of an error during start/stop processing, if the start/stop processing cannot finish, you can perform a forced stop to shut down the failed cluster, node, or resource group. In a forced stop, all errors are ignored and processing is forced to terminate. For details on performing a forced stop for a cluster or node, see section 4.5.6. For details on performing a forced stop for a resource group, see section 4.5.9.

- **Disable and restart resource group monitoring**

  If you manually stop and change the settings of a service running in a resource group during normal operation, or if you attempt to manually stop and re-install the active service, the NAS Modular system will assume that an error occurred and activate failover automatically. To avoid automatic failover when performing a maintenance task on a service in a resource group, you must temporarily disable monitoring of the resource group. After finishing the maintenance task, you can restart resource group monitoring. For details, see section 4.5.10.

- **Change the execution node of a resource group**

  Manual failover or failback is required when you need to switch the node on which a resource group is running. For example, you may need to change the active node in order to manually fail back a resource group after an error triggers failover, or to carry out maintenance without disrupting services. For details on changing the node on which a resource group is running, see section 4.5.11.

### 1.2.6 Managing Error Information

A NAS Modular system is designed to continually run and be available. It is therefore vital to centrally control and promptly respond to errors wherever they occur: in the drivers installed on the NAS Units, in the NAS OS, or in applications running on the NAS OS.

To manage error information in a NAS Modular system, NAS Manager provides function to:

- Monitor errors throughout the whole NAS Modular system,
- Report detected errors to a system administrator, and
- Manage error information.

#### 1.2.6.1 Monitoring Errors Across the NAS Modular System

NAS Manager can monitor all errors occurring in the drivers installed on the NAS Units, in the NAS OS, and in applications running on the NAS OS. If a failover is triggered by a NAS OS error, NAS Manager on the alternate NAS Unit takes over error monitoring. On receipt of an error report from a monitoring target, NAS Manager logs the event in the following log files:

- **System messages file**

  A log of important messages produced by the NAS Modular system. From the message ID, a system administrator can determine where the error occurred and identify its cause.

- **System log**

  A system log for the NAS OS. Important messages for the NAS OS are written in this log. A system administrator can use this log to obtain detailed information about errors of the NAS OS, and about errors for which causes could not be determined from the system messages.

#### 1.2.6.2 Reporting Errors

In NAS Manager, errors written to a system log or system messages file can be reported in two ways:

- By display in the NAS Manager
- By SNMP notification

When you use the NAS Manager to request a display of the contents of a system log or a system messages file, NAS Manager uses the GUI to display this information. When you request a display of a list of core files, NAS Manager uses the GUI to list the files.

NAS Manager can also report system messages to the SNMP manager if the SNMP notification function has been set up. Errors are reported automatically by SNMP notification, enabling even faster response.

For details about the SNMP settings, see section 4.7.13.

#### 1.2.6.3 Managing Error Information

You can use the NAS Manager to display, download, and delete error information in system messages and system log files.

NAS Manager also allows you to acquire and manage the log files output by applications running on the NAS OS. You can also use the NAS Manager to display, download, and delete these log files.

Since there are log files other than system messages and system log files, NAS Manager allows you to download a specific group of log files that are necessary to discover the cause of an error. This group is called a *log group* and is categorized based on the location of the error.

In addition, you can view a list of core files found by NAS Manager. You can then manage the listed core files (when the NAS OS dump files are output, the dump files are displayed in addition to the core files), downloading and deleting them as required.

For details on using the NAS Manager to manage system messages, system logs and other log files, and core files, see section 4.13.

For some types of error information, it is possible to specify system settings for the number of files to be kept and the file sizes.

### 1.2.7 Viewing System Status Using SNMP

When SNMP is set up in NAS Manager, an SNMP agent running on a NAS Unit can acquire the system status on receipt of a *get* request from a SNMP manager outside the NAS Modular system, and send that information to the SNMP manager.

For the *get* request that acquires quota information, a system administrator can set a threshold for the number of responses from the NAS OS. The number of responses here means the number of users or groups whose quota information the NAS OS returns to the SNMP manager. If the total number of users or groups for which quotas for the file system have been set exceeds the threshold, a warning is issued to the SNMP manager and the NAS OS does not respond to any more requests for quota information for users or groups. In this way you can alleviate degradation of access performance in the whole NAS Modular system in an environment where file system users and groups will be likely to increase or where the SNMP manager and network are often under heavy loads.

For details on SNMP setup, see section 4.7.13.

For details on the MIB objects that can be used in NAS Manager when responding to SNMP *get* requests, see Appendix A.

### 1.2.8 Controlling Service Setup and Service Startup

A NAS Modular system allows you to manage NFS file sharing and CIFS file sharing services.

As a system administrator, you can use the NAS Manager to verify that services are working properly, change service configurations according to operational requirements, and start, stop, and restart services:

- **Managing the NFS service**

  The NFS service allows efficient access from NFS clients to file systems. A system administrator can perform NFS reconfiguration and startup control from the NAS Manager.

- **Managing the CIFS service**

  The CIFS service (cifs_service) enables Windows® clients to access CIFS-based shared file systems. You can use the NAS Manager to change the cifs_service configuration definitions and control service activation.

- **Managing the SSH service**

  The SSH service (ssh_service) registers a public key generated in SSH clients to allow SSH access to the NAS OS. You can use the NAS Manager to change the configuration definitions of ssh_service.

- **Managing the FTP service**

  The FTP service (ftp_service) enables FTP clients to access the file systems. A system administrator can use the NAS Manager to change the ftp_service configuration definitions and control service activation.

For details on using the NAS Manager to manage services, see section 4.6.

### 1.2.9 Specifying System Settings

NAS Manager provides a GUI for specifying the system settings needed for running the NAS Modular system. As a system administrator, you can use the NAS Manager GUI to specify system settings, as listed in Table 1.3.

**Table 1.3 System Settings defined in NAS Manager**

| Setting | Use |
|---|---|
| Data LAN Port | Specify the negotiation settings for data LAN ports. |
| Trunking | Create a group of ports and specify the trunking settings for the group. You can set: *link aggregation*, *link alternation*, and *cascaded*. |
| Interface and Network | Set and change service IP addresses and fixed IP addresses, and set and change whether or not to use a VLAN. |
| NIS server, DNS server and LDAP | Set and change information about the NIS or DNS server. |
| Routing information | View, add, and delete routing information. |
| Time | Synchronize the NAS Modular system time with the time of the NTP Server. |
| System file editing | Edit the `/etc/hosts`, `/etc/samba/lmhosts` and `/etc/snmp/snmpd.conf`. |
| Log file | Set the number of log generations to keep and the log file size. |
| Core file storage period | Set the core file storage period. Core files are automatically deleted when the specified storage period has elapsed. |
| Tuning of performance | Tune system performance. |
| SNMP | Set the MIB objects used for SNMP. |
| User interface | Select GUI or commands. |

For details on using the NAS Manager to set the above network information and system information, see section 4.7.

### 1.2.10 Specifying an Administrator

The administrators for NAS Manager include a single *account administrator* and 16 *system administrators*:

- **Account administrator**

  An account administrator can use the NAS Manager to register or delete system administrators, and to manage system administrators by changing their user information, such as their passwords. Account administrators can also change their user information and password.

- **System administrators**

  A system administrator can use the NAS Manager to log in to a NAS Unit assigned by the account administrator, set up the NAS Modular system (for example, define the cluster configuration, configure file systems, and register end users), and operate and maintain the NAS Modular system. System administrators can use the NAS Manager to change their own user information and password.

For details on how the account administrator can use the NAS Manager to manage system administrators or edit the account administrator's own user information, see sections 3.5 and 3.6. For details on how system administrators edit their own user information, see section 4.16.

### 1.2.11 Enabling Program Installation

In NAS Manager, a system administrator can use the NAS Manager to install distributed revisions or upgrades over the installed program files on NAS OS LUs.

- Perform an overwrite installation when a program for an existing program is provided or when the version of an existing program is updated
- Install optional modules purchased at a later date, and uninstall unneeded optional modules

The following table lists the programs and program settings that a system administrator can manage from the NAS Manager. Version-down installation is not supported.

**Table 1.4 Programs and Settings Managed from the NAS Manager**

| Program Name | Install | Uninstall |
|---|---|---|
| NAS Data Control (required) | Cannot be performed See ***Note*** | Cannot be performed |
| NAS File Sharing (required) | Cannot be performed See ***Note*** | Cannot be performed |
| NAS Manager (required) | Can be performed | Cannot be performed |
| NAS Anti Virus Agent module | Can be performed | Can be performed |
| NAS Backup Restore module | Can be performed | Can be performed |
| NAS Sync Image module | Can be performed | Can be performed |

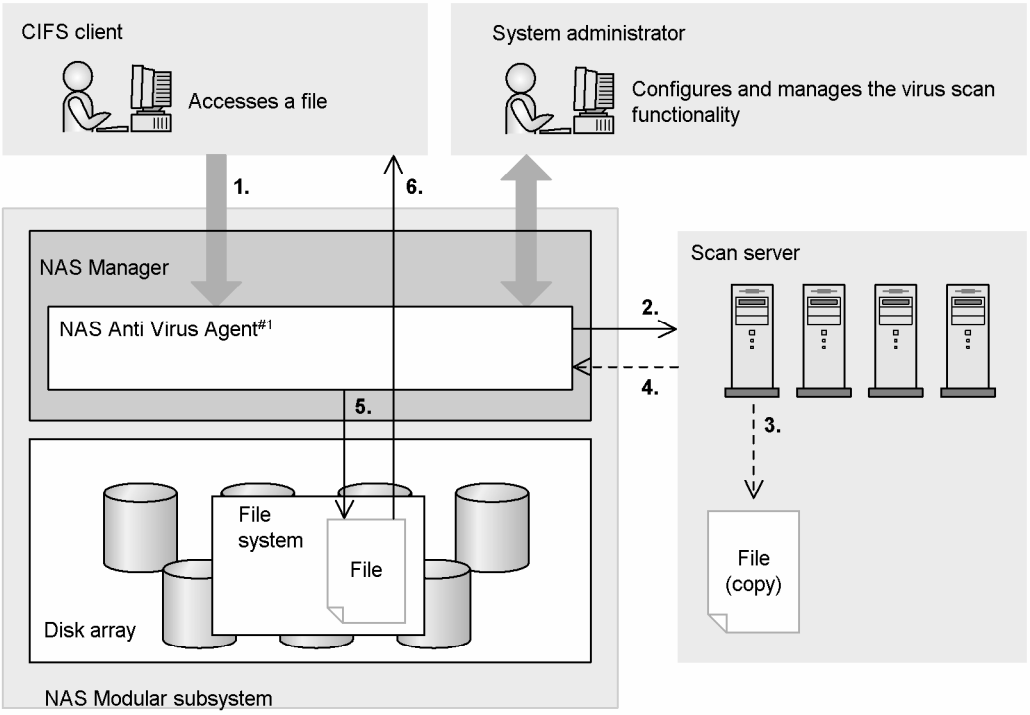
***Note:*** You may be able to install a patch version of this program. For information on whether the patch version can be installed using the GUI, see the documentation for the patch version obtained from the developer.

For more information on using the NAS Manager to manage programs, see section 4.15.

### 1.2.12 Protecting the NAS Modular system against Viruses (optional product)

If a NAS Anti Virus Agent license has been set up in a NAS Modular system, a network scan server can scan for viruses as needed whenever a CIFS client opens or closes a file in a disk array. Use the NAS Manager to manage the virus scan function, to configure virus scan operations, scan conditions, and scan results reports. For more information on the license setup in NAS Anti-Virus Agent, see the description of license keys in the manual the *Storage Navigator Modular User's Guide*.

Figure 1.11 shows an example of scanning for viruses on a NAS Modular system.




1. A file read or write is requested.
2. A copy of the file is provided to the scan server, and a virus scan is requested.
3. A virus scan is performed on a copy of the file. If the file is infected, perform recovery of the infected file.
4. The results of the virus scan are provided.
5. If recovery of a virus-infected file is successful, the recovered file is written over the file stored on the disk.
6. A response is made to the file read or write request. If recovery of a virus-infected file failed, the file is processed as set by the system administrator.

Legend:

- System administrator and CIFS client process flow
- NAS Manager process flow
- Scan server process flow

#1: Available for use when a NAS Anti Virus Agent license has been configured.

**Figure 1.11 Scanning for Viruses on a NAS Modular System**

Virus information and information about clients that worked with infected files is output to the system log (syslog). You can also generate reports using an SNMP trap. For details on accessing system logs, see section 4.7.8. For the settings required in order to use SNMP trap reports, see section 4.7.13.

### 1.2.13 Saving NAS System LU Data

To be prepared for errors, use the NAS Manager to save NAS system LUs (NAS OS LUs and the NAS Cluster Management LU). A NAS OS LU stores programs such as the NAS OS and NAS Manager. One LU is assigned to each NAS Unit.

The NAS Cluster Management LU stores NAS Modular system settings information, such as cluster configuration information and file system information. All NAS Units share the NAS Cluster Management LU. The NAS system LUs can be stored manually or automatically at specified intervals.

These NAS system LUs must be saved manually whenever a system administrator modifies the NAS Modular system configuration. If the latest status of a NAS system LU is not saved, the NAS Modular system may not be recoverable in the event of a failure. When an error occurs in the NAS system LU, contact your HDS representative, then restore the NAS system LU from the saved data.

## 1.3 Reviewing End-User Capabilities of NAS Manager

NAS Manager provides a GUI that enables end users to set up and change their password for CIFS user authentication. End users can also use the GUI to view the information about file shares and the quota for a file system created by system administrators. Users registered with user mapping cannot use the NAS Manager for end users.

For details on how to use the NAS Manager for end users, see Chapter 7.

# Chapter 2 System Configuration and Environment Settings

This chapter describes the NAS Modular system configuration and environment settings that are performed before or during NAS Manager operations:

- NAS Modular system configuration (see section 2.1)
- Network Configuration in a NAS Modular system (see section 2.2)
- Trunking Configuration in a NAS Modular system (see section 2.3)
- Using a Virtual LAN (VLAN) Configuration in a NAS Modular system (see section 2.4)
- Preparing for User Mapping (see section 2.5)
- Considerations before setting quotas (see section 2.6)
- Verifying Environment Settings in a NAS Modular system (see section 2.7)
- Reviewing a Client's Operating Environment (see section 2.8)

## 2.1 NAS Modular System Configuration

This section provides an overview of the hardware and software configurations in NAS Modular systems.

### 2.1.1 Hardware Configuration in a NAS Modular System

Figure 2.1 provides an overview of the hardware configuration in a NAS Modular system.

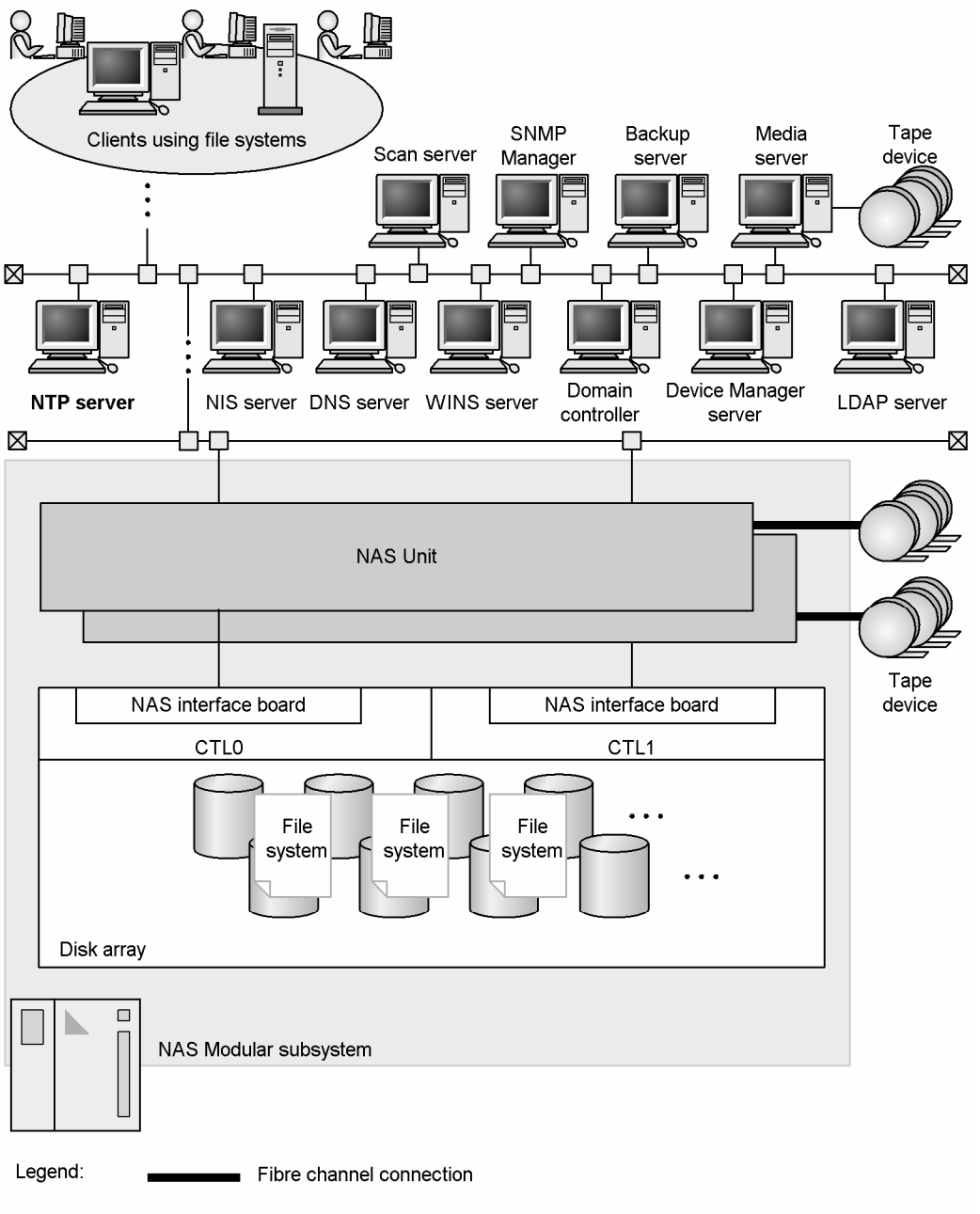



**Figure 2.1 Overview of Hardware Configuration in a NAS Modular System**

A NAS Modular system managed by NAS Manager uses a NAS Modular subsystem, to which a disk array of the TagmaStore AMS/WMS series and NAS Units are connected. The *NAS Unit* device is required to use the NAS Modular subsystem as a NAS server. Each NAS Unit is equipped with a Gigabit Ethernet adapter and a CPU. Two NAS Units form a single cluster.

A NAS Modular system requires servers and devices in addition to a disk array and NAS Unit. Table 2.1 lists the servers and other devices that are required to use a NAS Modular system.

**Table 2.1 Required Servers and Other Devices**

| Required Item | Description |
|---|---|
| NTP server | Required for time synchronization between the NAS Modular system and the client machines accessing the file systems. This server is required to use a NAS Modular system. |
| SNMP manager | Required when a NAS Modular system references NAS OS system information and reporting errors by using SNMP. |
| Backup server | Required when the NAS Modular system uses the NAS Backup Restore program. For more information, see the *NAS Backup Restore User's Guide.* |
| Media server | Used to manage tape devices. For details on the prerequisites for the media server, see the manual *NAS Backup Restore Modular User's Guide*.<br>If you use a tape device to connect to the NAS Unit via Fibre Channel, you do not have to set up the media server. In this case, the NDMP server implemented in NAS Backup Restore manages the tape device. |
| Tape device | Used to back up data in a file system or to restore data to a file system. For details on the standards for backup media that can be used on a tape device connected to a media server, see the vendor documentation. |
| NIS server | Required when a NAS Modular system uses the NIS to find information about users and hosts. |
| DNS server | Required when a NAS Modular system uses the DNS to find a host name. |
| WINS server | Required when a CIFS client using a NAS Modular system resolves a host name using WINS. |
| Domain controller | Required when a NAS Modular system uses the Active Directory authentication, or the NT domain authentication to authenticate users. |
| Device Manager server | Required when a NAS Modular system links with Device Manager. |
| Scan server | Required when a NAS Modular system uses the NAS Anti Virus Agent for virus-scanning. The scan server must be connected to the NAS Units with a 1000 Base LAN cable. |
| LDAP server | Required for either of the following purposes. The LDAP server can be used for only one of these purposes, not both.<br>-User authentication<br>User information is managed on the LDAP server.<br>-User mapping<br>Information about automatically-assigned user IDs and group IDs is stored in the LDAP server database. |

### 2.1.2 Software Configuration in a NAS Modular System

Figure 2.2 provides an overview of the software configuration in a NAS Modular system.

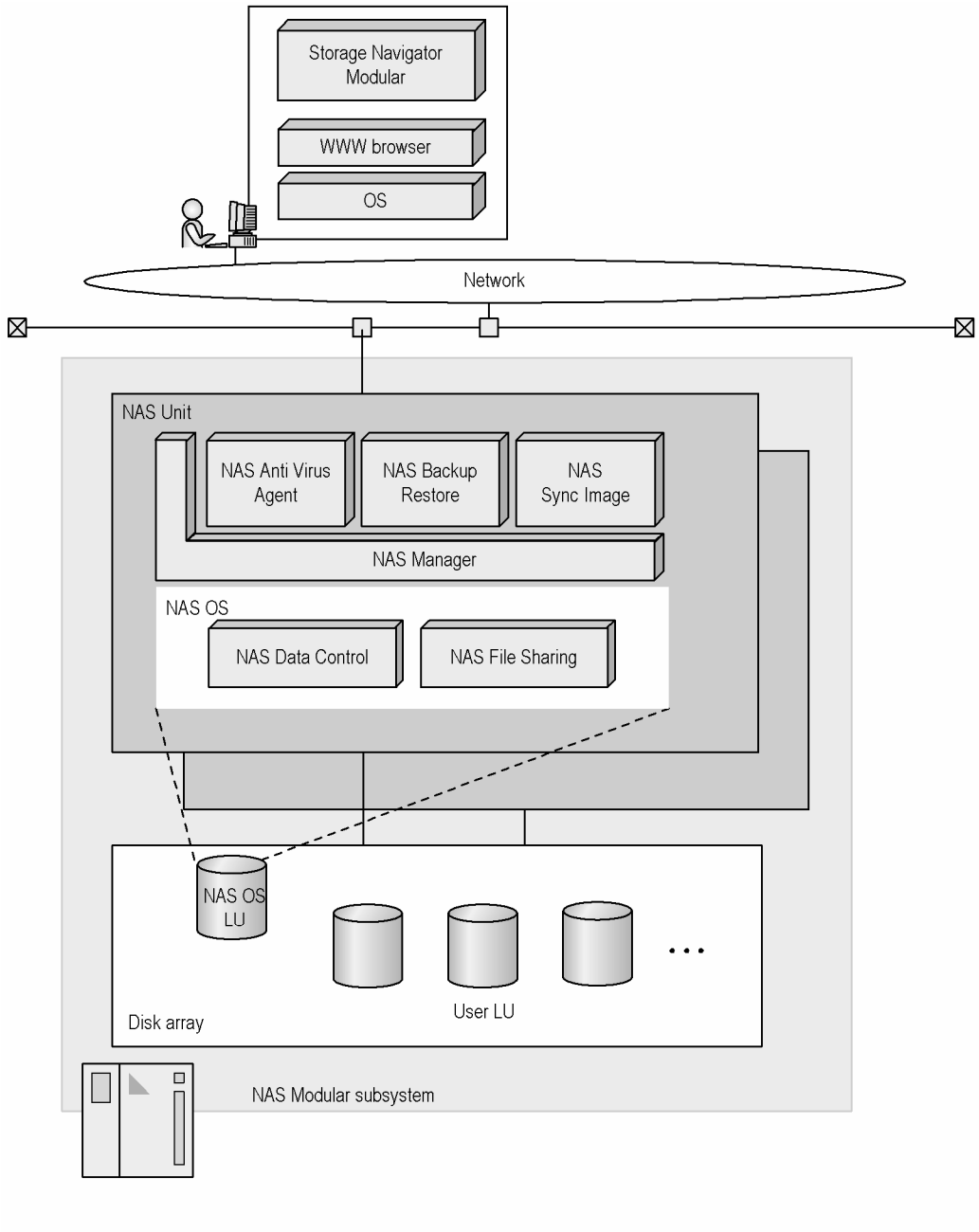



**Figure 2.2 Overview of Software Configuration in a NAS Modular System**

### About the NAS Operating System (OS)

The operating system provides the NAS function. The NAS OS runs on NAS Units, and it consists of the following standard programs:

- NAS Data Control (required program)
- NAS File Sharing (required program)

Programs that run on the NAS OS are described below. A system administrator must set up licenses for using these programs. For details on license setup, see the description of license keys in the *Storage Navigator Modular User's Guide*.

- NAS Manager (required)

  This program allows you to set up, operate and control a NAS Modular system.

- NAS Anti Virus Agent (optional)

  Allows you to scan for viruses on NAS Modular systems and includes registering a scan server, configuring scanning conditions and starting and stopping virus scanning.

- NAS Backup Restore (optional)

  This program provides backup/restore functionality and remote copy functionality for protecting file systems managed by the NAS Modular system. For more information, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

- NAS Sync Image (optional)

  Allows you to create differential-data snapshots for protecting file systems managed by NAS Modular systems. For more information, see the *Hitachi AMS/WMS NAS Sync Image User's Guide*.

### Using a Web Browser

System administrators and end users require a Web browser to access the NAS Manager GUI.

The Web browser displays the NAS Manager GUI. Since NAS Manager uses cookies, the Web browser must have cookies enabled. In addition, the color depth of the monitor displaying the Web browser must support 65,000 colors (**High Color (16 bit)**) or better, and the screen resolution must be set to 800 x 600 pixels or higher.

The following table lists the usable combinations of Web browsers and operating systems:

**Table 2.2 Usable Combinations of Web Browsers and Operating Systems**

| Web Browser | | Operating Systems |
|---|---|---|
| **Product Name** | **Version** | |
| Internet Explorer | 6 | Windows® 2000 Professional SP2 to SP4<br>Windows® XP Professional Edition SP2<br>Windows Server 2003 SP1 |
| Netscape® | 7.0 | Solaris™ 8 |
| Mozilla® | 1.4 and 1.7 | Solaris™ 9 |

The following table lists the recommended font settings for the Web browsers that are recommended in a NAS Modular system when you display the NAS Manager:

**Table 2.3 Web Browser Font Settings**

| Web Browser | Font Settings |
|---|---|
| Internet Explorer | Language script: Latin based<br>Web page font: Times New Roman<br>Plain text font: Courier New<br>Text size: Smallest |
| Netscape® or Mozilla® | Fonts for: Western<br>Proportional : Serif<br>Size (pixels) : 12<br>Serif : adobe-times-iso8859-1<br>Sans-serif : adobe-helvetica-iso8859-1<br>Cursive : -courier-iso8859-1<br>Fantasy : -courier-iso8859-1<br>Monospace : adobe-courier-iso8859-1<br>Size (pixels) : 12 |

If the browser user sets the text (or the font) to sizes other than those indicated above, the NAS Manager may not display properly.

The following table shows the cache settings used for displaying the NAS Manager:

**Table 2.4 Web Browser Cache Settings**

| Web Browser | Cache Settings |
|---|---|
| Internet Explorer | Check for newer versions of stored pages: Every visit to the page. |
| Netscape® or Mozilla® | Compare the page in the cache to the page on the network: Every time I view the page. |

If the cache settings are different from the ones listed above, the Web page may not be displayed properly.

**Storage Navigator Modular**

This program is used to perform operations such as restarting the NAS OS and setting up licenses.

## 2.2 Network Configuration in a NAS Modular System

A NAS Unit has the following three types of ports:

- Maintenance LAN port (mtp1)
- Management LAN port (mng1)

- User LAN ports (gbe1 to gbe4)

In a NAS Manager system, the maintenance LAN port (mng1) is used to perform communication between NAS Units in a cluster or between a NAS Unit and a disk array. Ports gbe1 to gbe4 are user LAN ports. By assigning these ports to clients that use a file system, the load on the system can be distributed.

Figure 2.3 shows an overview of the network configuration in a NAS Modular system.

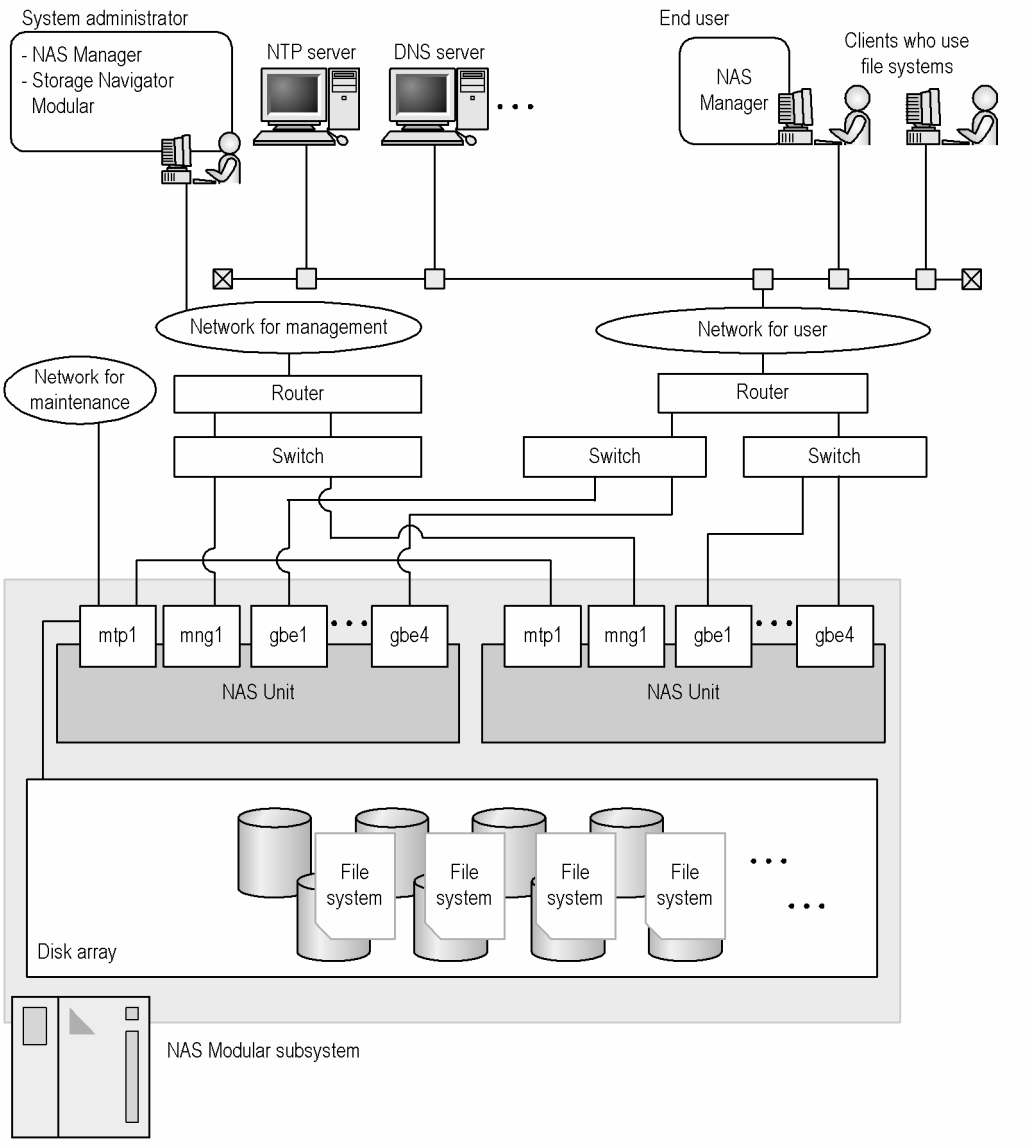



**Figure 2.3 Overview of Network Configuration in a NAS Modular system**

### Computers used by system administrators

System administrators can use any computer to use the NAS Manager GUI or commands.

The computers used by system administrators must be connected to the management LAN port (mng1); otherwise, NAS Manager might not operate properly.

If system administrators are required to access the file system, you must prepare a machine other than the ones being used for operating the NAS Manager GUI or commands, in order to connect to the network segments different from the management LAN.

**Computers used by end users**

End users can use any computer to access the NAS Manager GUI or file systems. The computers used by end users must be connected to a different network segment from the management LAN port.

**IP addresses assigned to interfaces**

The fixed IP address and service IP address that are assigned to each interface must use different network segments among the interfaces (gbe1 to gbe4) in the same NAS Unit.

**Routing setup**

Routing information must be set in NAS Manager to enable communication between NAS Units and client machines.

### 2.2.1 Configuring a Network When Using CIFS

In a NAS Modular system, the CIFS service can be used by using the NetBIOS name of the NAS Unit or the service IP address.

In the network configuration example described below, it is assumed that all the machine names in the network are resolved by using WINS, DNS, or the lmhosts service when, in the NAS Modular system, using the NETBIOS name of the NAS Unit to use the CIFS service. All the NAS Units in the cluster must be joined to the same work group, NT domain, or Active Directory® domain.

To specify the NetBIOS name of the NAS Unit from the CIFS client, specify the NNC of the NAS Unit you want to specify.

#### 2.2.1.1 Connecting the CIFS Client and NAS Unit to the Same Subnet

If the CIFS client and the NAS Unit are connected to the same subnet, we recommend that you use the WINS server on the CIFS client side to resolve machine names.

If a domain controller does not exist in the same subnet, it might take some time to obtain a list of computers when a failover occurs.

Figure 2.4 illustrates a network where the CIFS client and NAS Unit belong to a single work group.

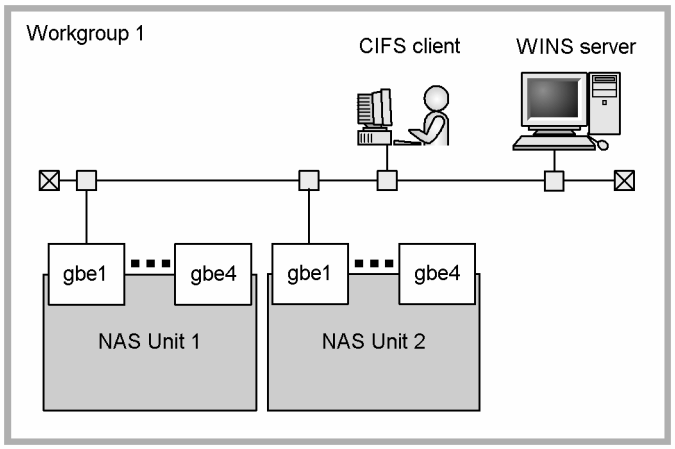



**Figure 2.4 Network with CIFS Client and NAS Unit in Single Work Group**

Figure 2.5 illustrates a network where the CIFS client and NAS Unit belong to multiple work groups.

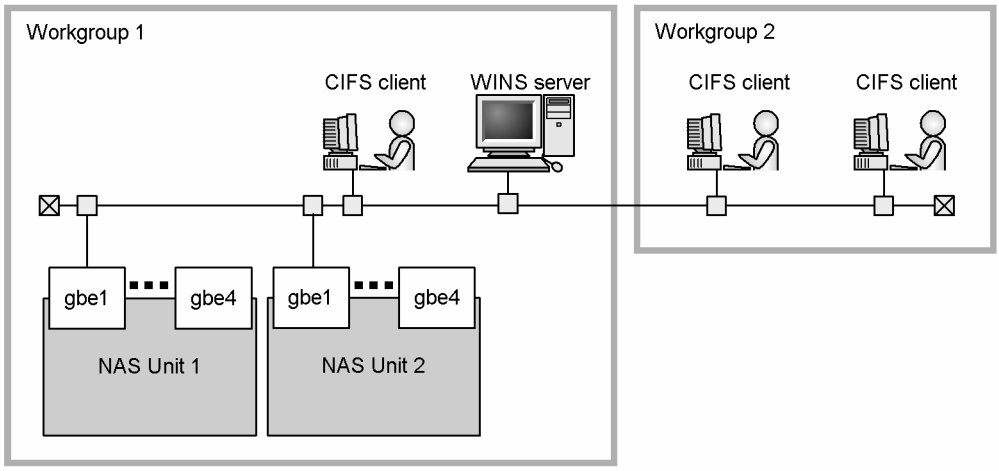



**Figure 2.5 Network with CIFS Client and NAS Unit in Multiple Work Groups**

Figure 2.6 illustrates a network where the CIFS client and NAS Unit belong to a single NT domain.

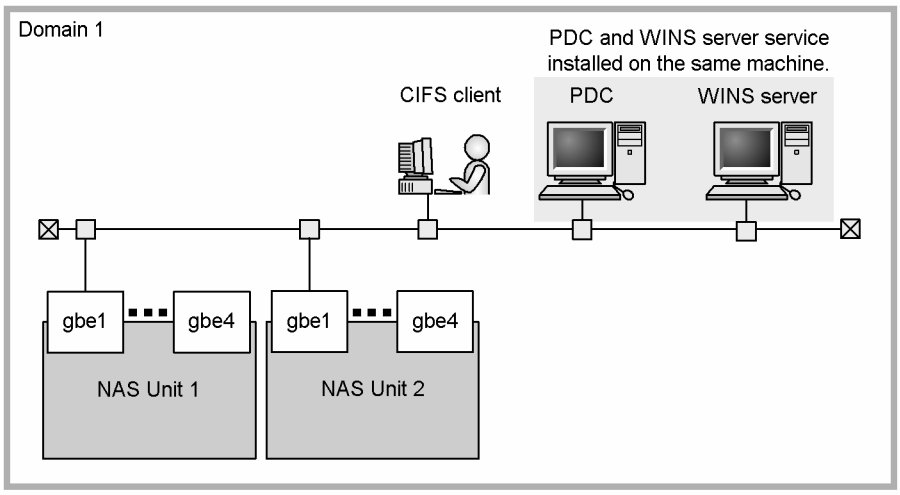



**Figure 2.6 Network with CIFS Client and NAS Unit in Single NT Domain**

### 2.2.1.2 Connecting the CIFS Client and NAS Unit to Different Subnets

When the CIFS client and the NAS Unit are connected to different subnets, note the following points:

- The NT domain configuration or the Active Directory® configuration is required.
- A domain controller is required for the subnet to which the NAS Unit is connected.
- When a WINS server is used as a name server to CIFS clients, we recommend that all the CIFS clients in the network be set as WINS clients.
- When a WINS server is not used, the lmhosts file must be modified as follows:
  - In an NT domain configuration:

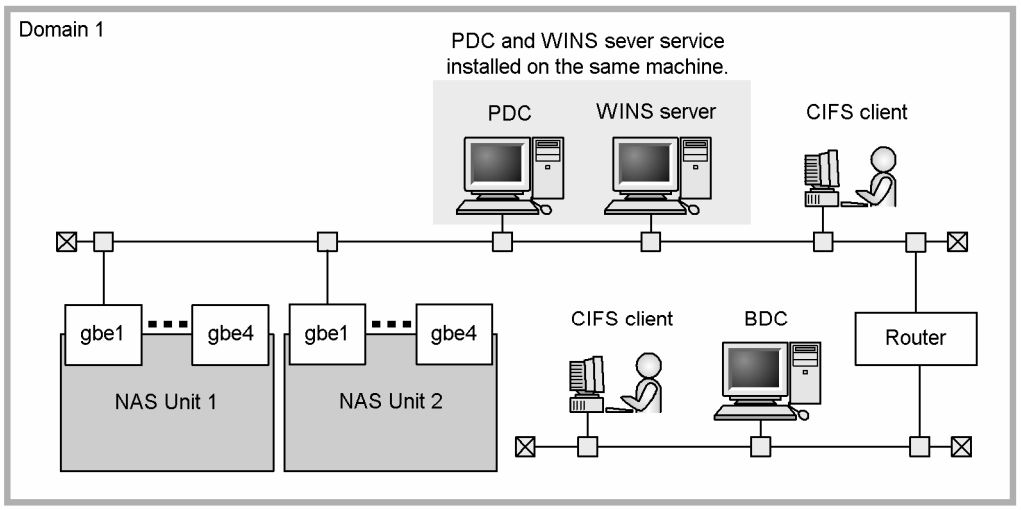
    Add the following description to the lmhosts file in the backup domain controller. When you use the subnet not connecting with the domain controller, add the following description to the lmhosts file provided for each CIFS client.

    *IP-address-of-the-primary-domain-controller domain-name*#1B
  - In an Active Directory® domain configuration:

    Add the following description to the lmhosts file in the domain controller that exists in the same subnet as the CIFS client. In the subnet where the domain controller is not connected, add the following description to the lmhosts file provided for each CIFS client.

    *IP-address-of-the-domain-controller-that-exists-in-the-same-subnet-as-NAS Unit domain-name*#1B

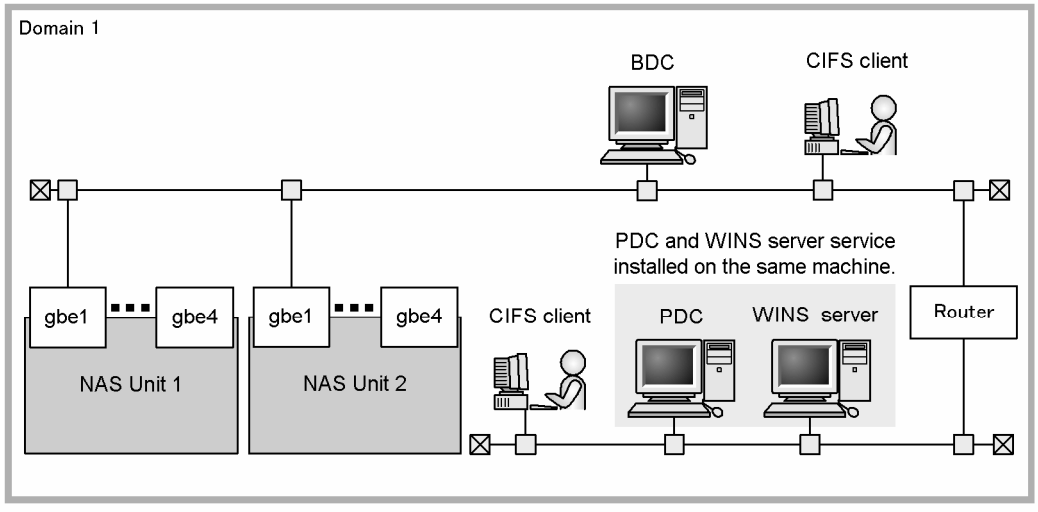
In an NT domain configuration, Figure 2.7 illustrates a network where the NAS Unit and the primary domain controller exist in the same subnet.




Legend:
PDC : Primary domain controller
BDC : Backup domain controller

**Figure 2.7 Network with NAS Unit and Primary Domain Controller in Same Subnet**

In an NT domain configuration, the following figure illustrates a network where the NAS Unit and the primary domain controller do not exist in the same subnet.




Legend :
PDC : Primary domain controller
BDC : Backup domain controller

**Figure 2.8 Network without NAS Unit and Primary Domain Controller in Same Subnet**

In an Active Directory® domain configuration, Figure 2.9 illustrates a network where the NAS Unit and the primary domain controller exist in the same subnet.

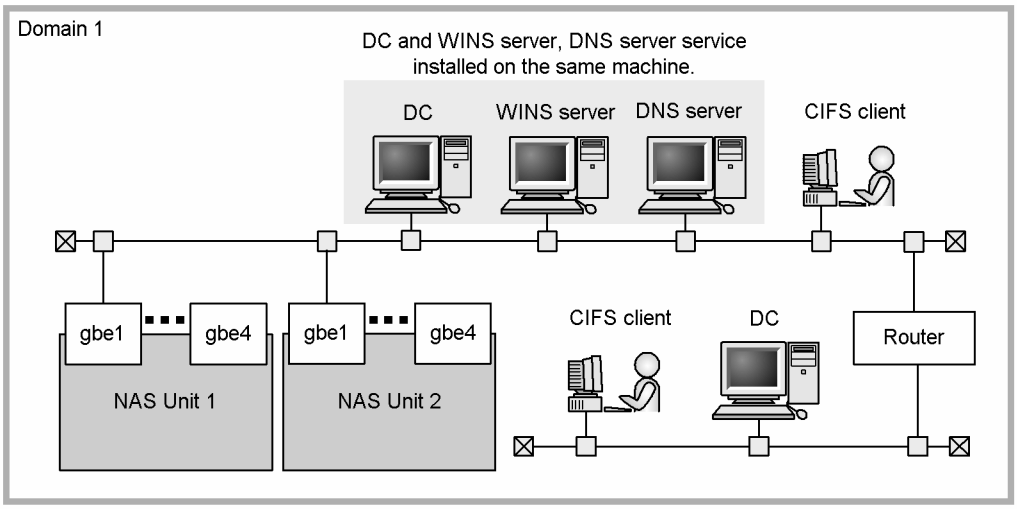



**Figure 2.9 Network with NAS Unit and Primary Domain Controller in Same Subnet**

### 2.2.1.3 Using a Network where CIFS Service is Used by Multiple Ports

When the CIFS service is used by the multiple ports from gbe1 to gbe4, a WINS server is required for the subnets connected to *gbe1*, *gbe2*, *gbe3*, and *gbe4*. All the CIFS clients connected to the network specify either of the WINS servers to select the access path to the NAS Unit. For example, when the WINS server on the subnet where gbe1 is connected is selected, you can access the NAS Unit through gbe1.

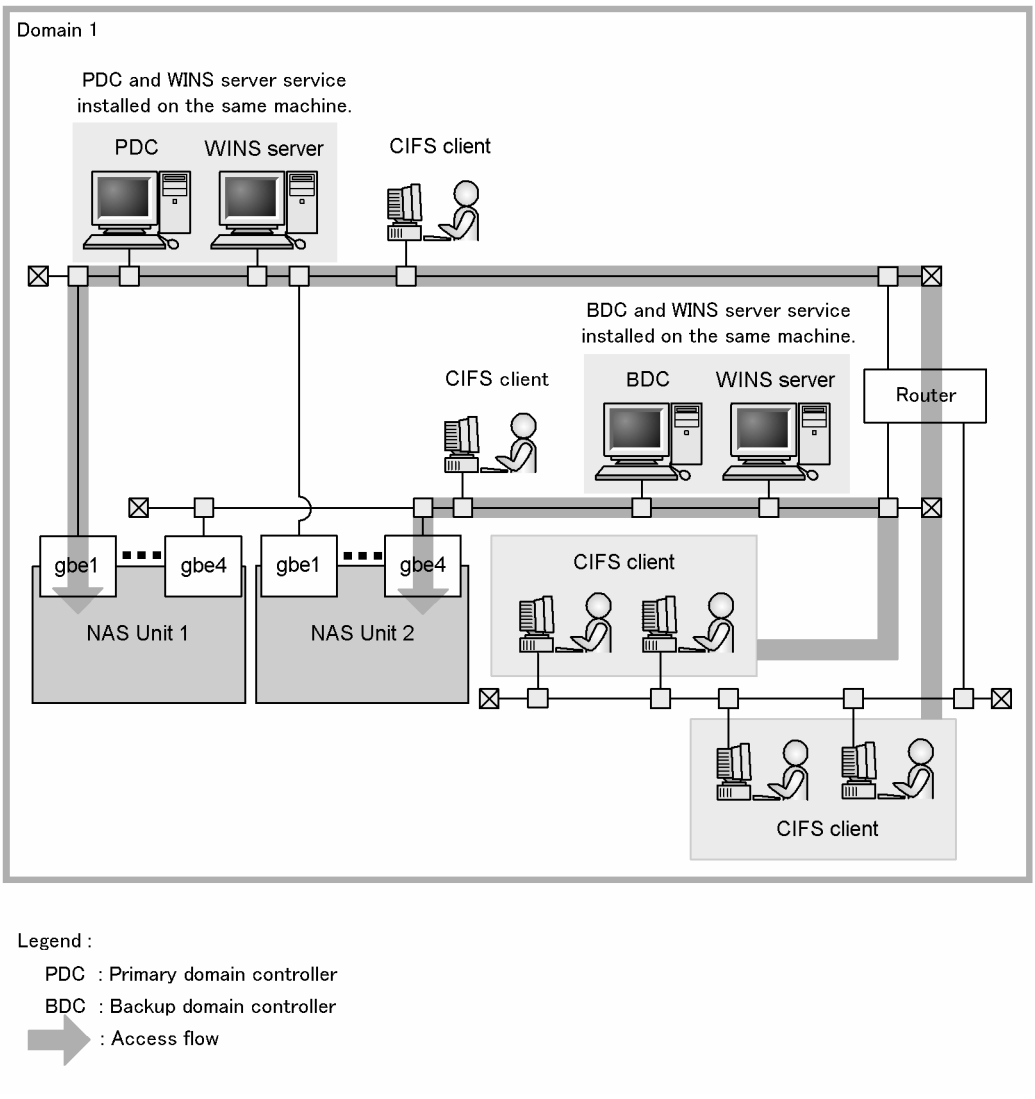



**Figure 2.10 Network with gbe1 and gbe4 in a CIFS Service**

## 2.3 Reviewing a Trunking Configuration in a NAS Modular System

Trunking can be used in a NAS Modular system. This section describes a network configuration when trunking is used in a NAS Modular system.

### 2.3.1 Trunking Definition

*Trunking* is a technology used to create a group of ports as a virtual network interface. By using trunking, you can achieve the following benefits:

- IP addresses can be managed more easily.

In a network that uses trunking, one IP address is assigned to the interface for a group created by trunking. This eases IP address management.

- Load on paths can be distributed.

In a network that uses link aggregation, multiple links can be used concurrently as a single group. For users, this makes it seem as if the bandwidth has been increased.

- A highly available network can be designed.

In a network that uses link aggregation, if an error occurs on any of the links, processing can be continued using the other links. Also, in a network that uses link alternation, if an error occurs in a switch, processing can be continued using the standby port. Thus, tolerance to link errors and switch errors can be improved.

Normally, a NAS Modular system uses ports *mng1* and *gbe1* to *gbe4* as physical interfaces to configure a network.

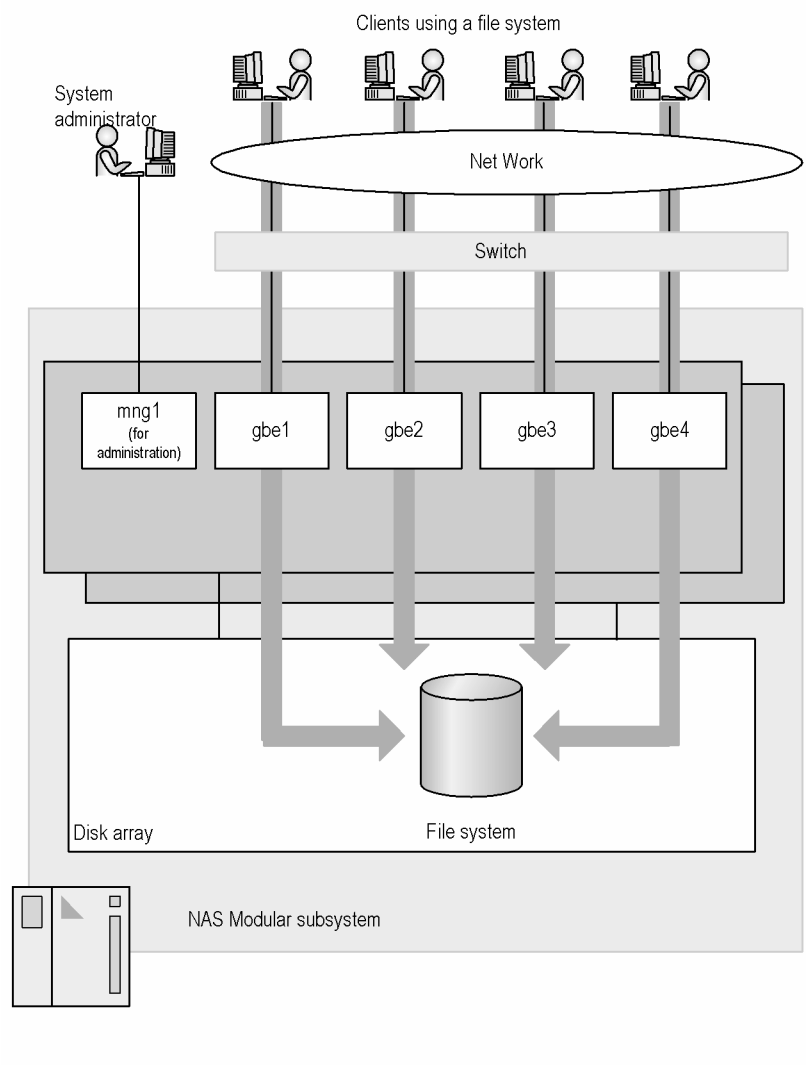


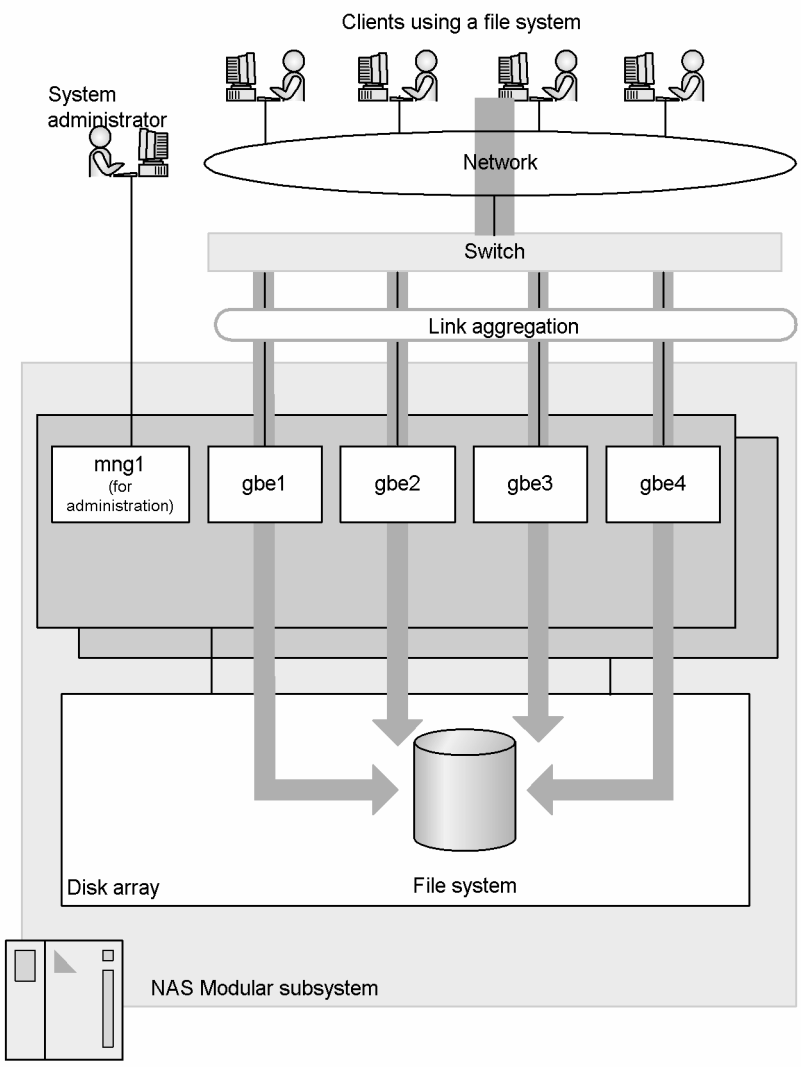

**Figure 2.11 Network Configuration that Does Not Use Trunking**

With a NAS Modular system, you can use trunking to configure a network from *gbe1* to *gbe4* as logical ports. The management LAN port, mng1, cannot be used for trunking.

A NAS Modular system supports link aggregation, link alternation, and cascaded trunking as trunking methods. Cascaded trunking enables concurrent use of link aggregation and link alternation. Link aggregation, link alternation, and cascaded trunking are described below.

### 2.3.1.1 Link Aggregation

Link aggregation connects aggregated links with the same switch to allow each link to be used concurrently. For users, this makes it seem as if the bandwidth has been increased. If an error occurs on a link, the processing can be continued with other normal links.




Note: A switch compliant with IEEE802.3ad (Dynamic LACP) is required.

**Figure 2.12 Network Configuration with Link Aggregation (with No Error)**

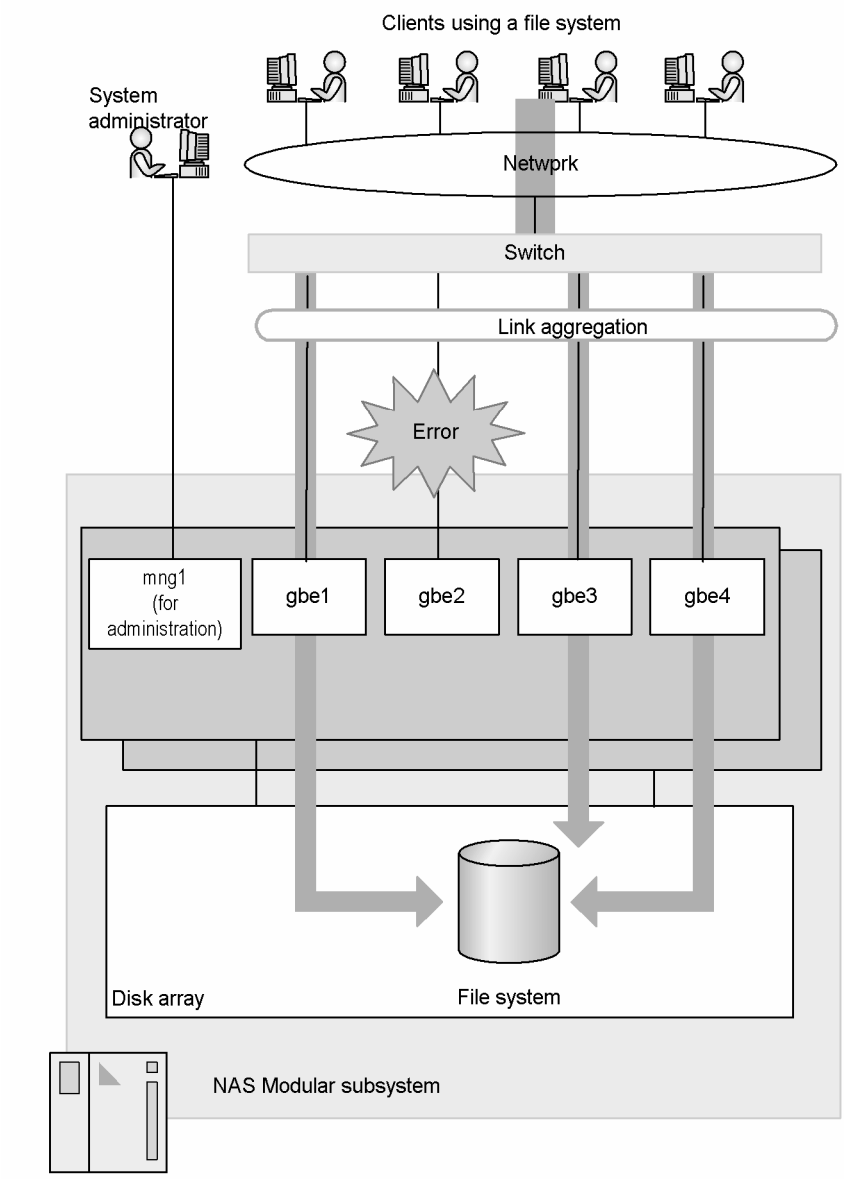



**Figure 2.13 Network Configuration with Link Aggregation (with an Error)**

### 2.3.1.2 Link Alternation

Link alternation creates a port group, consisting of any two of the ports from gbe1 to gbe4, as a virtual port, and allows either port in the group to be used for communication. If a hardware error occurs (in a switch or NIC), link alternation automatically performs a switchover to the other standby port to continue communication. Thus, link alternation improves tolerance to hardware errors.

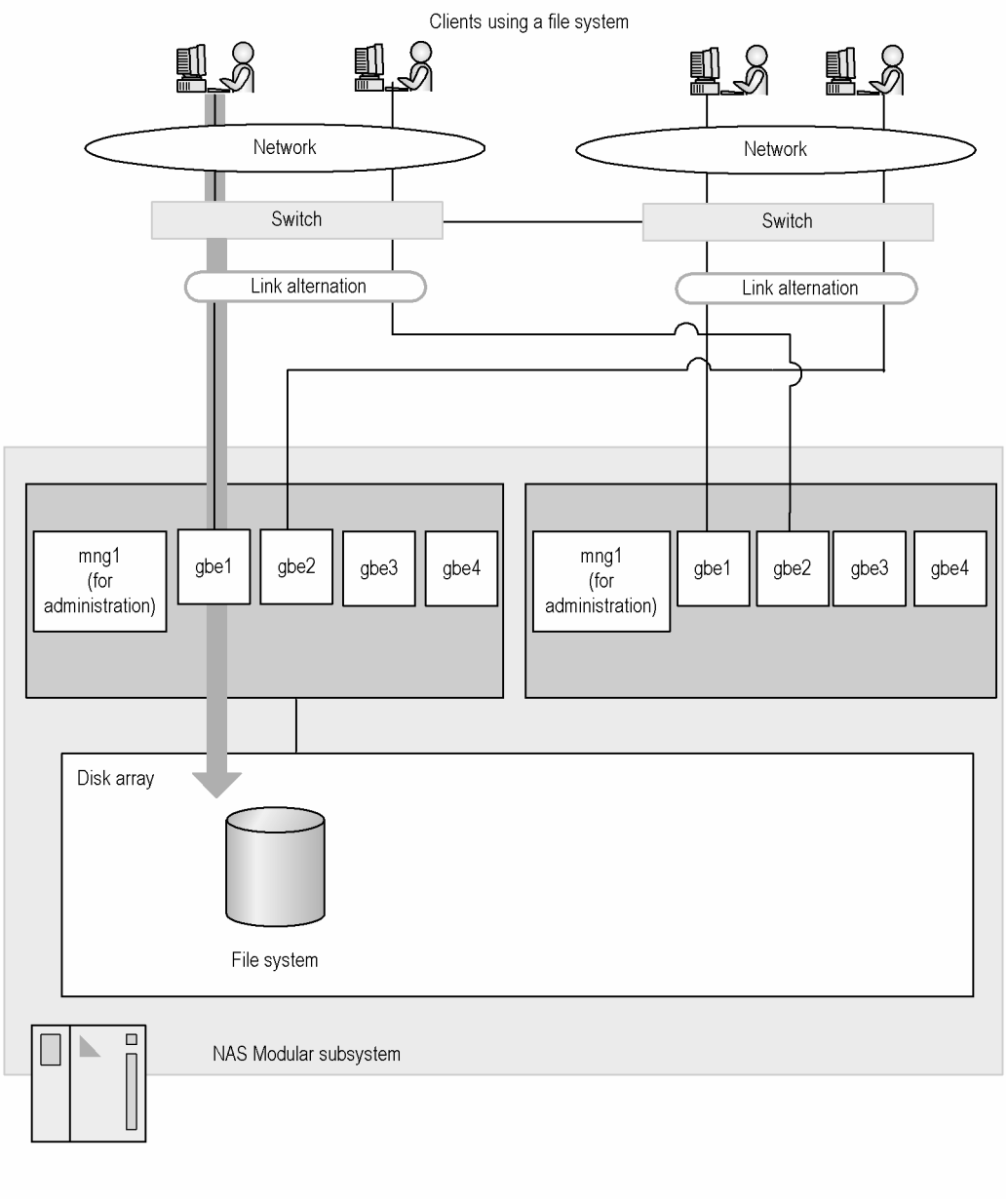



**Figure 2.14 Network Configuration with Link Alternation (with No Error)**

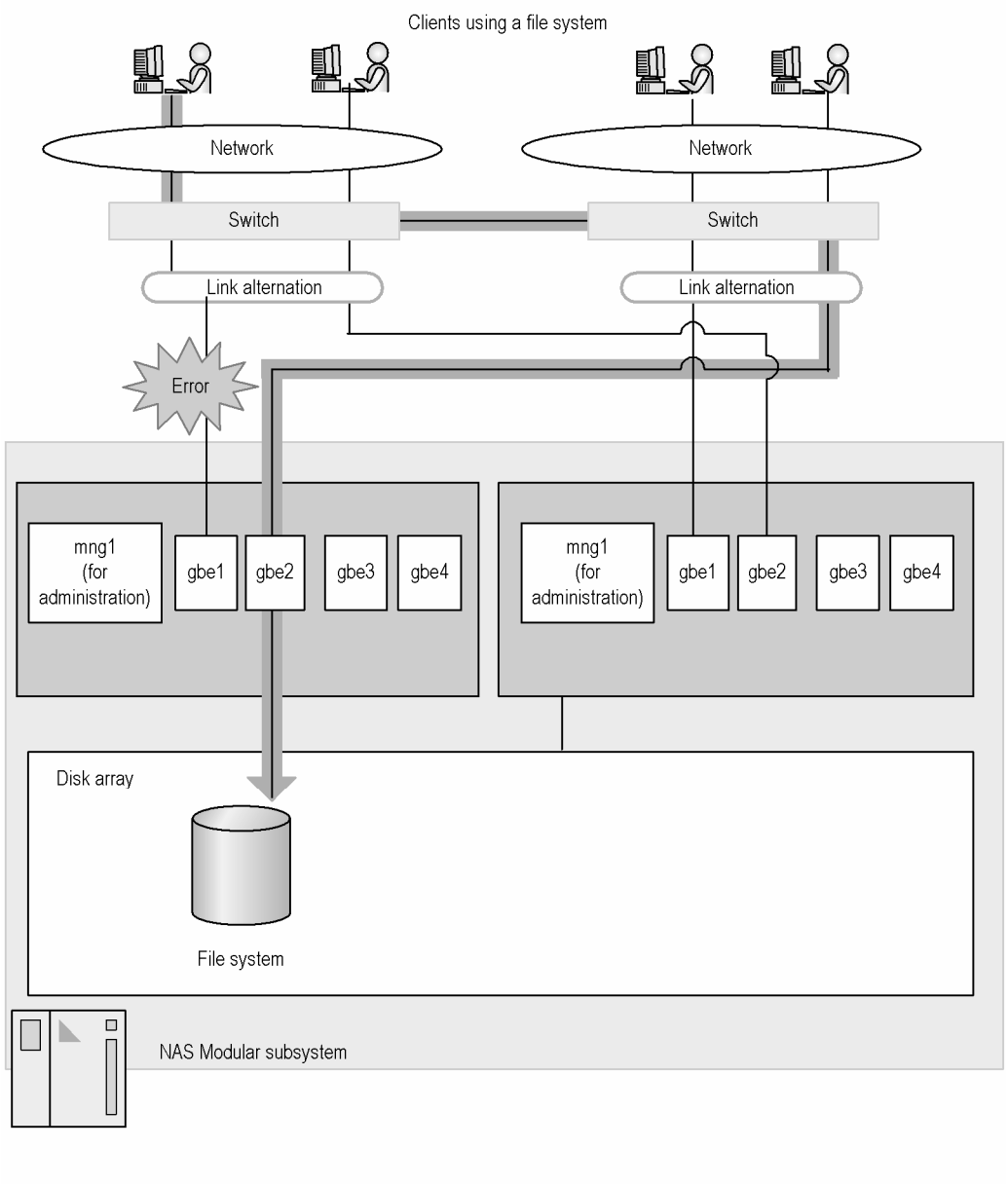
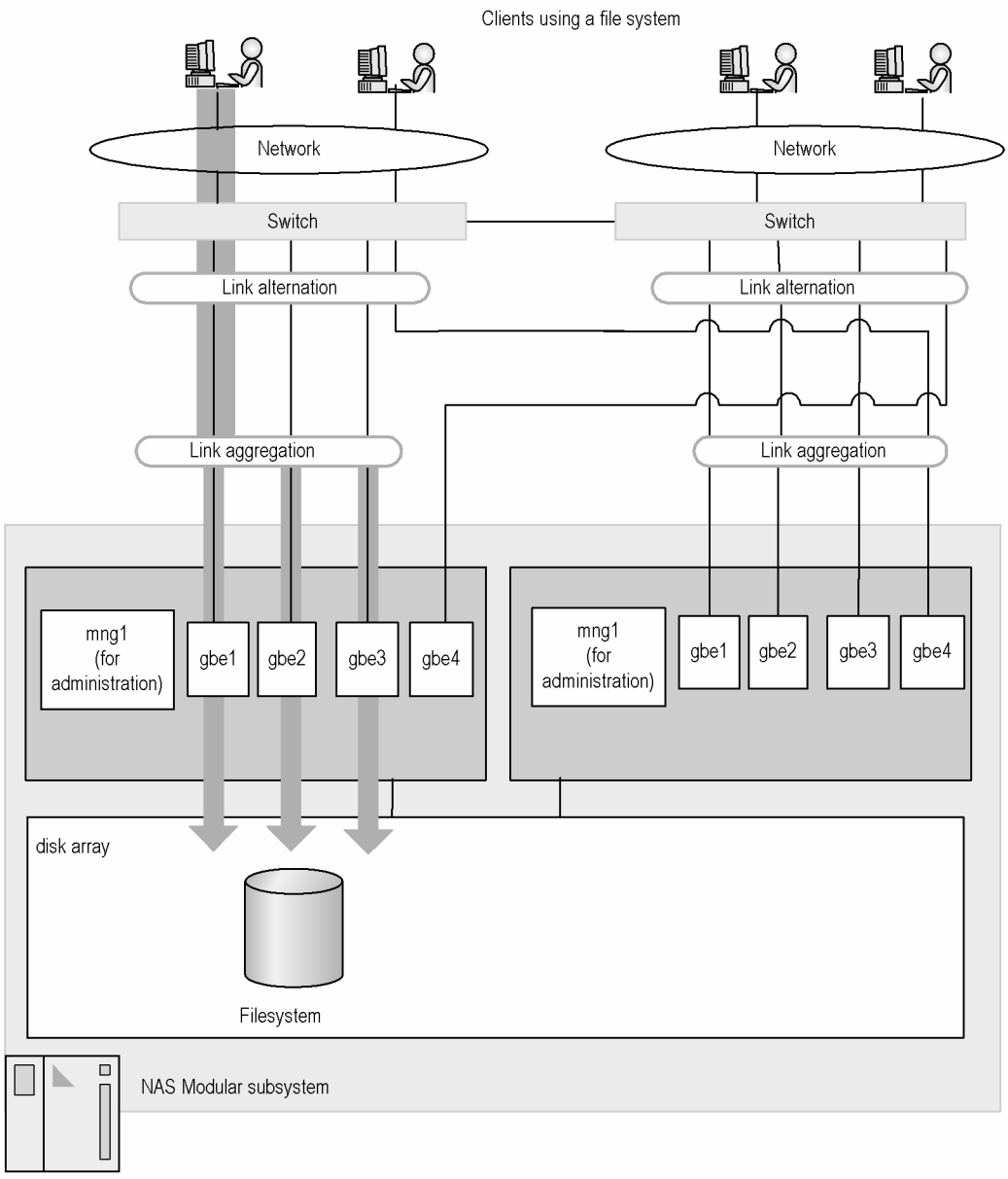



**Figure 2.15 Network Configuration with Link Alternation (with an Error)**

### 2.3.1.3 Cascaded Trunking

Cascaded trunking enables simultaneous link aggregation and link alternation to provide improved tolerance to link errors and load distribution with increased bandwidth. When trunking is used in a NAS Modular system, it is recommended that cascaded trunking be used to configure the network.




Note: The switches to which link aggregation is connected must be compliant with IEEE802.3ad (Dynamic LACP).

**Figure 2.16 Network Configuration with Cascaded Trunking (with No Error)**

### 2.3.2 Using Trunking in a NAS Modular System

This subsection describes benefits that can be achieved by using trunking in a NAS Modular system, and provides an overview of how to set up trunking.

System administrators can set link aggregation in the **Link Aggregation Setup** window, and can set link alternation in the **Link Alternation Setup** window. This subsection describes the benefits and recommended configurations for trunking in a NAS Modular system.

#### 2.3.2.1 Benefits

By using trunking in a NAS Modular system, you can achieve the following benefits:

- If some of the links have failed, the NAS Modular system can continue processing without causing a failover to occur (unless all links fail).
- Link aggregation can raise the communication rate per network interface to 2 or 3 Gbps by aggregating multiple ports that provide communication at 1 Gbps, each.
- An IP address is assigned to the network interface for a group created by trunking. This improves IP address management.
- Trunking and a VLAN can be used concurrently.

#### 2.3.2.2 Trunking Setup

This subsection provides an overview of setting up trunking in a NAS Modular system.

**Prerequisites for using trunking:**

- To use trunking, you must define the cluster configuration and configure a network environment to which a NAS Modular system is connected (for example, set a switch).
- To use link aggregation in a NAS Modular system, a switch compliant with IEEE802.3ad (Dynamic LACP) is required.
- Among the switches that are connected to the NAS Modular system, there is a switch that has a fast-forwarding (or Port Fast/Uplink fast) function as an advanced feature of STP (Spanning Tree Protocol). For continuous use of the service, we recommend that you enable the fast-forwarding function of a port that is directly connected to the NAS Modular system via link trunking.

**Procedure for setting up trunking:**

The following procedure shows how the system administrator can set up trunking.

1. Stop the cluster and the resource groups on both nodes.
2. Set up trunking.

   The NAS Modular system recommends cascaded trunking. To set up cascaded trunking, set up both link aggregation and link alternation.

3. Set the interface information and network information. If necessary, specify the VLAN settings.
4. Start the cluster and the resource groups on both nodes.
5. Specify the service settings, user or group settings, file system settings, file share settings, and any other settings as required.
6. Save the system LU. At this time, the network information, including the information on trunking, is saved.

**GUI used to set up trunking:**

Link aggregation is set up using the **Link Aggregation Setup** window. Link alternation is set up using the **Link Alternation Setup** window.

To set up cascaded trunking, first, set up link aggregation on the **Link Aggregation Setup** window. Then, on the **Link Alternation Setup** window, use the ports with link aggregation set and port that is not trunked to set up link alternation.

For details on the pages used for setting up trunking, see section 4.7.2.

#### 2.3.2.3 Recommended Trunking Configurations in a NAS Modular System

When a node contains a port for which trunking is not set, a failover occurs if an error occurs on the port. Therefore, to use trunking in a NAS Modular system, it is recommended that a network be configured using cascaded trunking to prevent a failover from occurring.

The cascaded trunking configurations recommended in a NAS Modular system are as follows:

- **Configuration 1:** The default active and standby ports have the same performance.
- **Configuration 2:** The default active port has higher performance than the standby port.

  Link aggregation is set among ports `gbe1`, `gbe2`, and `gbe3`, which are defined as the default active port, and link alternation is set between the default active port and port `gbe4`, which is defined as the standby port.

The following figure illustrates an example of the cascaded trunking configuration recommended for the NAS Modular system.

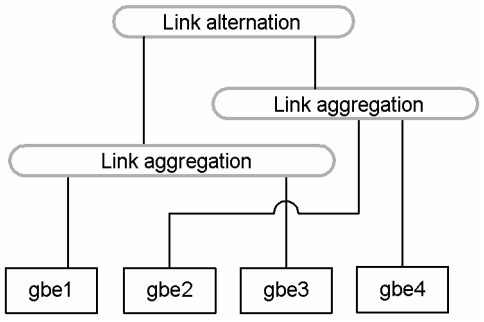



**Figure 2.17 Recommended Trunking Configuration 1**

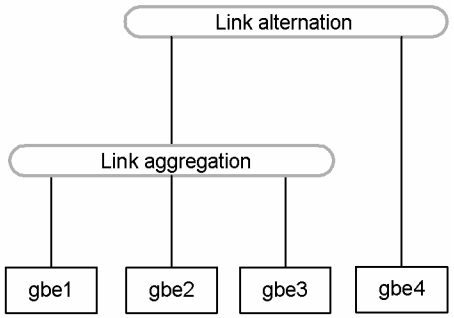



**Figure 2.18 Recommended Trunking Configuration 2**

The NAS Modular system does not support the following trunking configurations because system performance might be degraded with these configurations:

- Link alternation set among three or more ports
- Trunking set using a port for which link alternation is set
- Link aggregation set for a port for which link aggregation is already set

## 2.4 Using a Virtual LAN (VLAN) Configuration in a NAS Modular system

A VLAN is technology that virtually divides a physical network configuration, LAN. When you virtually divide a LAN, you can configure it independently from the physical network topology. This enables you to design a highly flexible network to respond to changes in the network configuration.

In a NAS Modular system, mng1 (management LAN port) and gbe1 to gbe4 (data LAN ports) are used as the physical interface needed to configure a LAN.

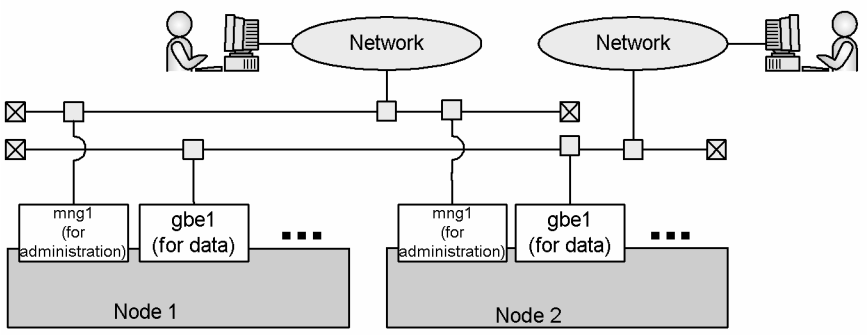



**Figure 2.19 Usual LAN Network Configuration**

In a NAS Modular system, you can set a virtual interface for the ports gbe1 to gbe4, user LAN ports, to configure a network using the VLAN. You cannot set a virtual interface for mng1, the management LAN port, to configure a network using the VLAN.

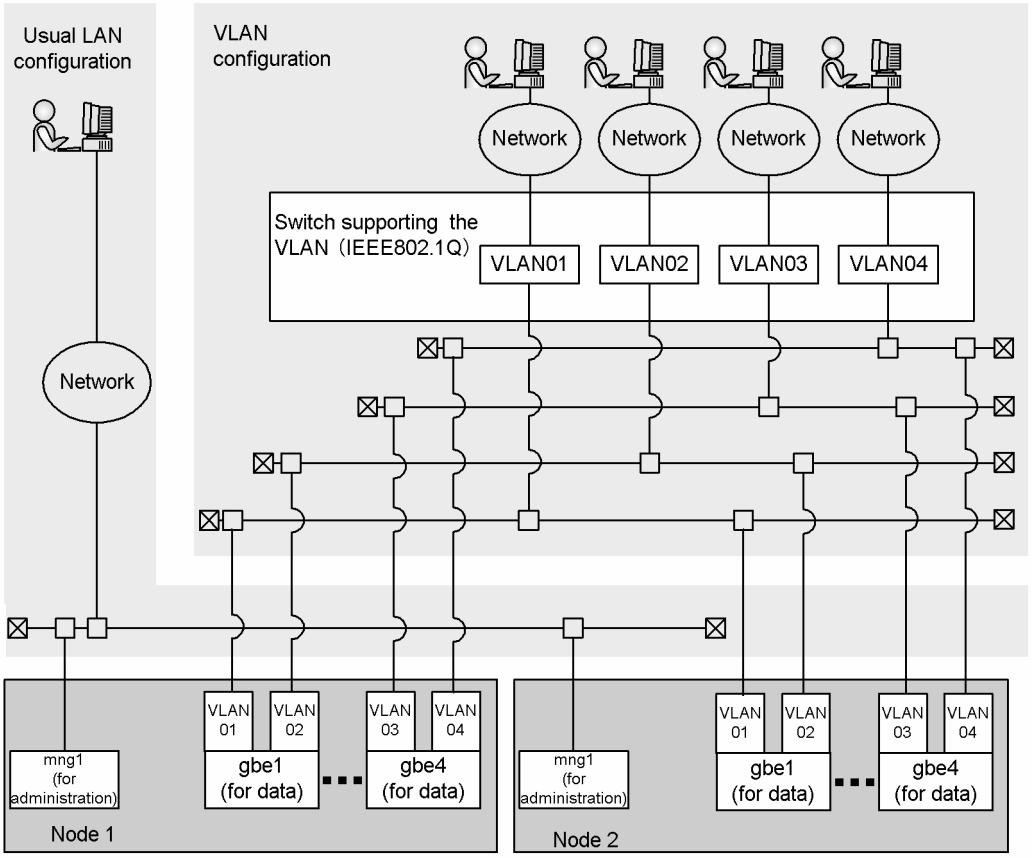



**Figure 2.20 Network Configuration when a VLAN is Used**

A VLAN lets you do the following:

- **Design a highly flexible network**

  When designing a network connected to a NAS Modular system, if you use a VLAN, you can design a highly flexible network. For example, if you use a VLAN, you can integrate the existing network and a network you are going to add, into a single physical network.

- **Respond to changes of the network configuration**

  When using a VLAN, you can logically define a network that is independent of a physical device configuration, thus you can respond to changes of the network configuration flexibly. You can change the network configuration without worrying about the physical location of the connected machine. Even if you move the machine, you do not have to change the machine settings.

- **Improve the security between networks**

  When you use a VLAN, you can logically place into another network, a machine that exists in the same network when a usual LAN configuration is used. This allows you to improve the security between networks.

### 2.4.1 Setting up a VLAN

System administrators can set a VLAN in the **Add Interface** window. When setting up a VLAN, you must set the VLAN ID. This subsection describes the features of VLANs in a NAS Modular system and summarizes VLAN setup.

**Features**

The following features are available when a VLAN is used in a NAS Modular system:

- You can use an IEEE802.1Q tag-based VLAN.
- When a network is configured using a VLAN and an error occurs in a NAS Unit, a resource group is moved to the other node by failover. Therefore, you can perform maintenance procedures such as error recovery or replacement while the service is continually provided.
- You can set an MTU value (the maximum value of data that can be transmitted for each transfer operation in the communication network) for each VLAN.

**Prerequisites**

- To use a VLAN, a switch supporting an IEEE802.1Q tag-based VLAN is required.
- To set a VLAN, the NAS OS of both nodes must be running.
- Before setting a VLAN, the cluster and resource groups must be stopped.

**VLAN Operational Flow**

The system administrator performs the following tasks when using a VLAN:

a) Stop the cluster and the source groups of both nodes.

b) Set the VLAN.

c) Start the cluster and source groups of both nodes.

d) If necessary, set the service settings, user or group settings, file system settings, and file share settings.

e) Save the system LU. At this time, the network information, including VLAN information, is saved.

**VLAN Interface Settings**

When you use a VLAN in a NAS Modular system, a virtual network interface (VLAN interface) is created for *gbe1* to *gbe4*. An identifier called VLAN ID must be given for the VLAN interface. Also, the service IP address can be set for the VLAN interface so that the resource group can be connected using the same IP address during failover. To detect an error such as a link down in both nodes, we recommend that you specify the service IP address for both nodes. If you do not specify the service IP address, you must check whether an error occurs in the **List of RAS Information** window.

VLAN settings are set in the **Add Interface** window. In the **Add Interface** window, when you add an interface, you can select whether you want to use a VLAN for the interface. When you want to use a VLAN, specify the VLAN ID. For details on the **Add Interface** window, see section 4.7.4.3.

The following describes the number and range of specifiable VLAN IDs per cluster and the number of service IP addresses:

- Number of specifiable VLAN Ids

  You can set a maximum of 256 VLAN IDs per cluster. When the number of service IP addresses reaches the maximum (256 per cluster), you cannot set any more VLAN IDs.

- Range of specifiable VLAN Ids

  A value from 1 to 4094 can be specified for a VLAN ID. The same VLAN ID cannot be duplicated within the cluster.

- Number of specifiable service IP addresses

  Up to 256 service IP addresses can be specified per cluster.

### 2.4.2 Using a VLAN and Trunking in a NAS Modular system

In a NAS Modular system, you can use both a VLAN and trunking to configure a network that can provide both VLAN features and trunking features. The VLAN features improve security, and provide an easy and flexible network design. Trunking features communicate with increased bandwidth, and with high availability.

To configure a network using both a VLAN and trunking, set trunking to combine multiple ports into one logical port, and then set the VLAN interface for this logical port. You cannot set trunking for multiple VLANs.

If trunking is set for a port for which the interface information and network information has already been set, the interface information (including the VLAN settings) and network information is automatically deleted.

## 2.5 Considerations Before Using User Mapping

The types of IDs used for identifying clients differ between NAS Modular systems and Windows systems. NAS Modular systems use user IDs and group IDs, while Windows uses unique IDs called security identifiers (*SIDs*).

If CIFS clients are to be authenticated via Active Directory authentication or NT domain authentication without using *user mapping*, you must register the same user information as registered by the domain controller on the NIS server, LDAP server, or NAS Manager that manages user information, as well as manage the user IDs and group IDs used in the NAS Modular system. If you use user mapping, user IDs and group IDs will be assigned automatically and there is no need to duplicate management of the user information registered in the domain controller.

This section explains how user mapping is handled in a NAS Modular system and describes the settings you need to consider before using user mapping.

### 2.5.1 Domains that allow Access to a NAS Modular System

When user mapping is used, users who belong to a domain in a trust relationship with the domain to which the NAS Units are joined can also access the CIFS shares in a NAS Modular system.

To access the NAS Modular system, such users must belong to a domain that is in a one-to-one trust relationship with the domain to which the NAS Units are joined.

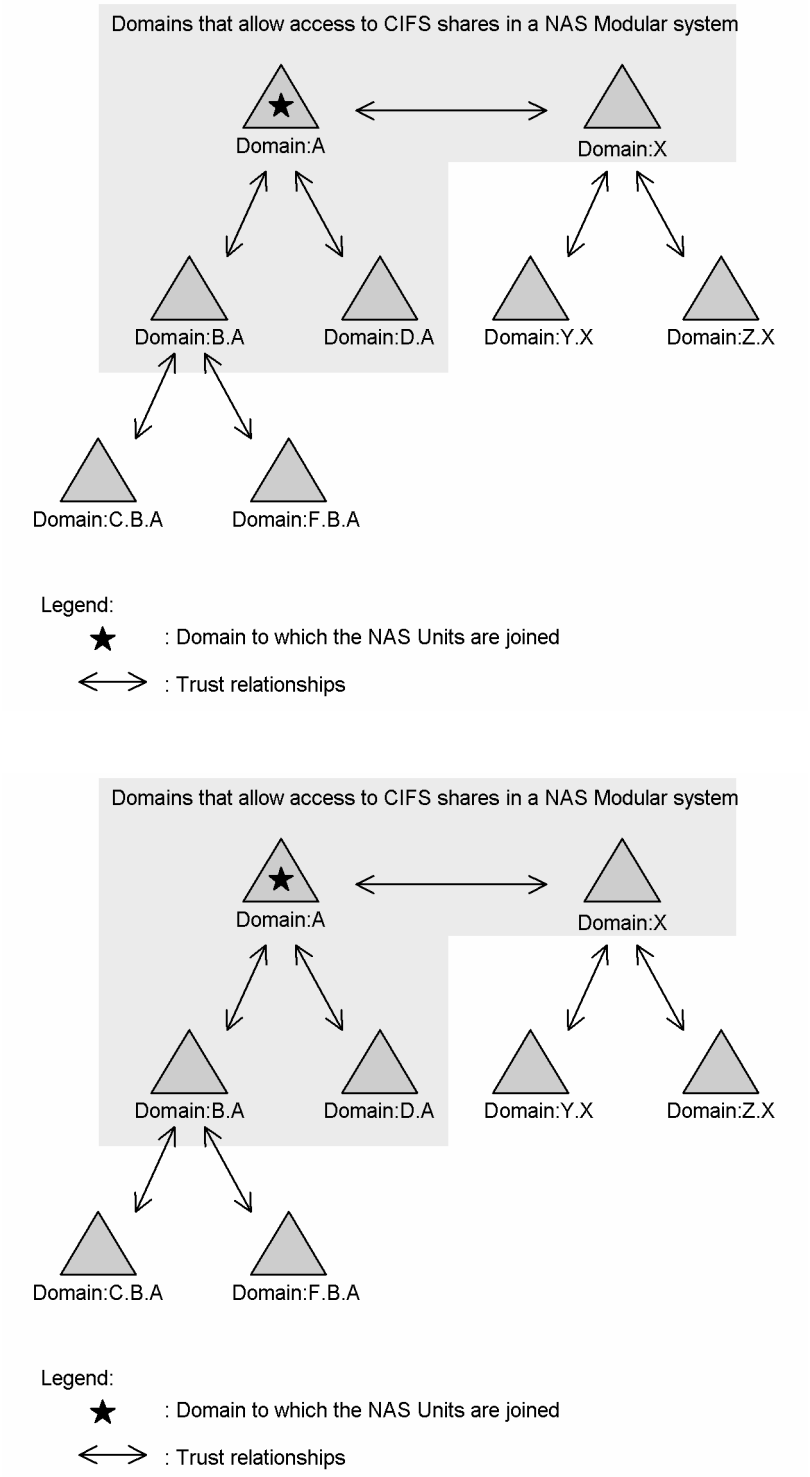



**Figure 2.21 Domains that allow access to CIFS shares in a NAS Modular system**

To access the NAS Modular system when the NAS Units are joined to an Active Directory domain, users who belong to a domain that is not in a parent-child relationship with the domain to which the NAS Units are joined must explicitly set a trust relationship with that domain.

### 2.5.2 Method of User Mapping

The following describes the user mappings provided by NAS Modular systems. We recommend that you use Relative Identifiers (RIDs), which will be less susceptible to communication errors in your NAS Modular system.

#### 2.5.2.1 User Mapping using RIDs

With user mapping using RIDs, when a CIFS client accesses a file system in the NAS Modular system, the system converts the set of relative identifiers (*RIDs*) contained in the SID and automatically assigns a user ID or group ID to the client.

With user mapping using RIDs, the system administrator uses NAS Manager to set a range of user IDs and group IDs for each domain, allowing users and groups to be managed by domain. Mapping information does not need to be stored in a database or managed on an external server when user mapping uses RIDs. Thus, assignment of user IDs and group IDs takes less time and the system is less vulnerable to errors on the network or external server.

You can manage a maximum of 6 domains when user mapping uses RIDs. If you have 7 or more domains, select user mapping using LDAP.

#### 2.5.2.2 User Mapping using LDAP

With user mapping using LDAP, when a CIFS client accesses a file system in the NAS Modular system, a user ID or group ID within the range specified in NAS Manager is automatically assigned to the client. Information about the assigned user ID or group ID is registered in the database of the LDAP server set up as an external server. When the CIFS client next accesses the file system, the previously assigned user ID or group ID is used.

If you set up an LDAP server for user authentication, you cannot also set up an LDAP server for user mapping. To enable user mapping in this case, select user mapping using RIDs.

### 2.5.3 Changing the Method of User Mapping

User IDs and group IDs are assigned differently in user mapping using RIDs and using LDAP. These assign different IDs to the same CIFS client.

If you change the method of user mapping after starting operations in the NAS Modular system, the user IDs and group IDs assigned to CIFS clients are altered. This may allow unauthorized users to access files and folders created before you switched the method of user mapping. To replace the user IDs and group IDs associated with files and folders with IDs that will be managed under the changed method of user mapping, the CIFS administrator needs to migrate the file system using the Windows backup function (Microsoft Windows backup for Windows 2000 Server, or the Windows backup utility for Windows Server 2003. For other OSs, see the documentation provided with each OS).

To migrate the file system when changing the method of user mapping:

1. Contact end users.

   Ask end users not to access the CIFS shares during this task.

2. Limit the access from CIFS client hosts.

   In **Host access restrictions** in the **CIFS Service Management** window, allow the CIFS access only to the CIFS client host on which the administrator will perform a migration of the file system.

3. Set up the CIFS administrator.

   In **CIFS Administrator name(s)** in the **CIFS Service Management** window, specify the CIFS administrator who will perform a migration of the file system.

4. Restart the CIFS service.

   In the **List of Services** window, restart the CIFS service.

5. Ask the CIFS administrator to back up the data in the source CIFS shares.

   We recommend that the CIFS administrator use the Windows backup function. If the data is backed up in another way, ACLs and file attributes might not be restored correctly. Note that the data made on the NFS client cannot be migrated by using the Windows backup function.

6. Change the method of user mapping.

   In the **CIFS Service Management** window, specify the required information in **User mapping setup**.

7. Restart the CIFS service.

   In the **List of Services** window, restart the CIFS service.

8. Create and mount the target file system.

   In the **Create New File System** window, create and mount a file system. Configure the target file system capacity so that it is no smaller than the source file system capacity. Do not set the default quota in this step (you will set it in step 13).

   For other items, apply the same settings as those for the source file system.

9. Set user and group quotas for the destination file system.

   If user and group quotas have been set for the source file system, set the same values to the target file system.

   Use the enas_quotaset command to set user and group quotas. For users and groups that will not be subject to limits on block usage and i-node usage, specify 0 for the soft and hard limits.

10. Create the target CIFS shares.

    In the **Create CIFS File Share** window, create the target CIFS shares, and assign them names that differ from the source CIFS share names. For the target CIFS shares, apply the same settings as those for the source CIFS shares.

11. Set a subtree quota.

    If a subtree quota has been set for the source CIFS-shared directory, set the same value to the target CIFS-shared directory.

    Use the stquotaset command to set the subtree quota. For users and groups that will not be subject to limits on block usage and i-node usage, specify 0 for the soft and hard limits.

12. Ask the CIFS administrator to restore the data to the target CIFS shares.

    Ask the CIFS administrator to restore the data backed up at step 5 to the target CIFS shares created at step 10.

13. Make sure that the data has been migrated correctly.

    Compare the data in the source CIFS shares with the data in the target CIFS shares, and make sure the migration has performed successfully. When comparing the source CIFS shares with the target CIFS shares, we recommend that the following points be checked:

    - Structures of the folders are the same.
    - Contents of the files are the same.
    - Information about owners, ACLs, and file attributes are the same.

14. Delete the source CIFS shares if necessary.

    In the **List of File Shares** (List of CIFS File Shares) window, delete the source CIFS shares if necessary (for example, when renaming the target CIFS share names to the source CIFS share names).

15. Delete the source file system if necessary.

    You can delete the source file system in the **List of File Systems** window if it is not needed.

16. Change the target CIFS share names if necessary.

    If the source CIFS shares were deleted at step 14, in the **Edit CIFS File Share** window, you can rename the target CIFS share names to the deleted source CIFS share names.

17. Delete the CIFS administrator you created if necessary.

    If the CIFS administrator created at step 3 is not necessary, delete the CIFS administrator from **CIFS Administrator name(s)** in the **CIFS Service Management** window.

18. Clear the access limit to the CIFS client hosts.

    In **Host access restrictions** in the **CIFS Service Management** window, clear the access limit to the CIFS client hosts that you set at step 2.

19. Restart the CIFS service.

    In the **List of Services** window, restart the CIFS service.

### 2.5.4 Determining the range of user IDs and group IDs by using RIDs (Examples)

An RID is assigned to each user, group, and computer account, regardless of the type of object. Consequently, there will some IDs that are assigned by using RIDs but not actually used for file access. When you consider the range of user IDs and group IDs to set, remember that the range should cover unused IDs.

The following figure shows how user IDs and group IDs are assigned by user mapping using RIDs.

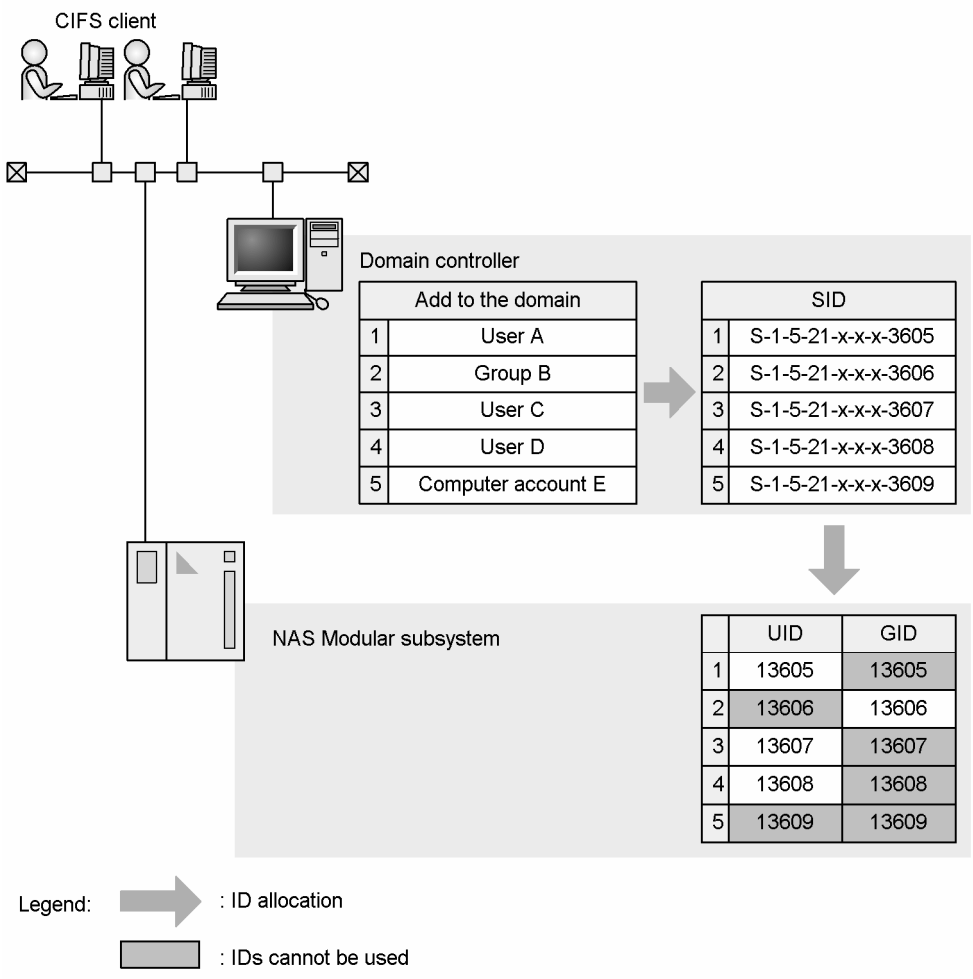



**Figure 2.22 Example of assigning user IDs and group IDs by using RIDs**

Once the range of user IDs and group IDs are enabled, you cannot change the lowest value of the range of user IDs and group IDs available for user mapping. When you consider the range of user IDs and group IDs to be set (when using user mapping), estimate the range with enough margin, taking in to account future operational plans and the range of user IDs and group IDs that will be needed in other domains or by an external server. If there is not enough space allocated for the IDs you want to add when changing the range of user IDs and group IDs, you will need to recreate the file system.

When you set the range of IDs available for user mapping, you must take into consideration future increases in the number of SIDs. At a minimum, the range of IDs you decide upon must contain the range of RIDs that is already in use. To ensure that you set a correct range of IDs available for user mapping, determine what that range is from the largest RID in use.

A system administrator can use an application, such as one provided by Microsoft, to acquire the SID of the object that was last added to the domain controller. From this SID, the system administrator can check the largest RID that is currently in use. If there are multiple domain controllers in the same domain, the system administrator can check the largest RID by acquiring the SID of the last added object for each domain controller. For details on how to acquire a SID, see the documentation for the application.

For example, suppose that user mapping using RIDs will be used under the following conditions:

- There are two domains (`Domain1` and `Domain2`).
- The domains have a direct trust relationship with each other.
- The largest RID that is currently in use is 8,000.
- 1,000 users will be added to each domain annually. (However, from the second year, 1,000 users will be deleted annually.)
- 1,000 computer accounts will be added to each domain annually. (However, from the second year, 1,000 computer accounts will be deleted annually.)
- Groups and other objects will not be added or deleted.
- The domains will be in use for 100 years from the start of operations.
- Add a 50% margin to the range of user IDs and group IDs to be set, to manage with uncertain increase of objects.

Number of SIDs used per domain for calculation purposes:

```
Number-of-SIDs = (largest-RID-currently-in-use) +
        (number-of-users-added) + (number-of-computer-accounts-added)
```

```
=8,000
```

Annual number of SIDs increase per domain after the first year

```
Number-of-SIDs = (number-of-users-added) + (number-of-computer-accounts-added)
```

```
1,000 + 1,000 = 2,000
```

The following figure shows an example of estimating the total number of user IDs and group IDs required under the above conditions.

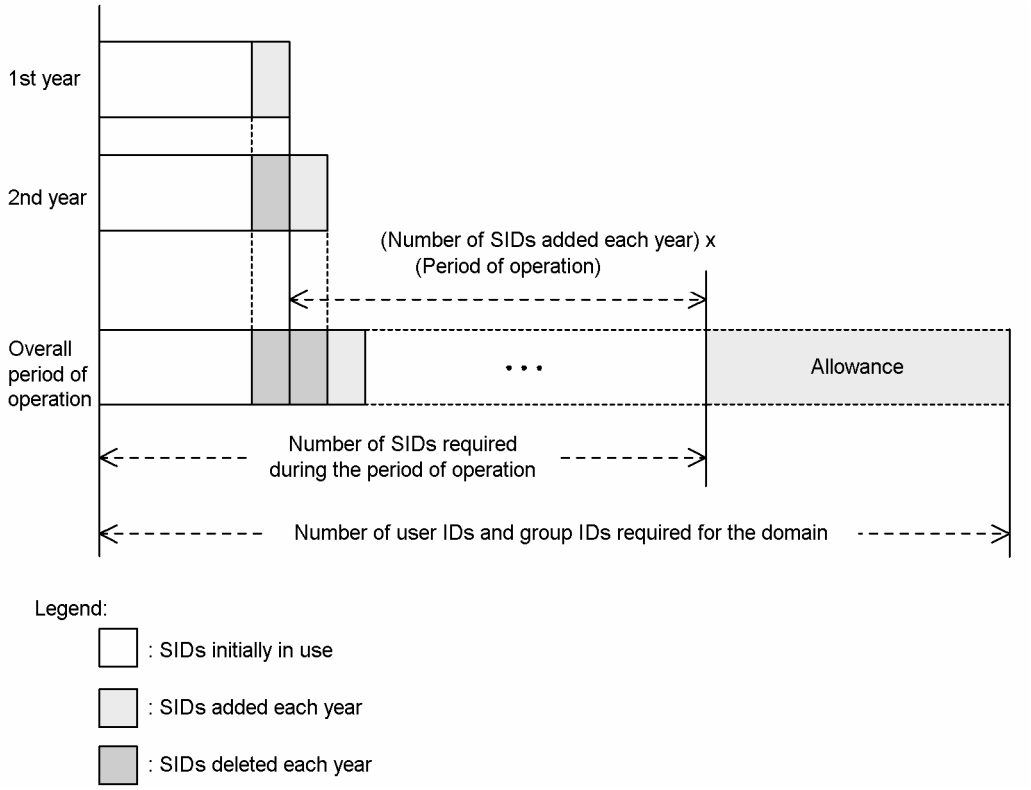



**Figure 2.23 Estimating Total Number of Required User IDs and Group IDs**

A total of 2,000 objects will be added annually. Therefore, the number of SIDs will increase by 2,000 each year. From the second year, a total of 2,000 objects will be deleted annually. However, IDs used for deleted objects cannot be reused.

Number of IDs required for each domain (`Domain1` and `Domain2`):

```
Number-of-IDs-required-per-domain = (number-of-SIDs-currently-in-use +
(increase-in-number-of-SIDs-per-year x number-of-years-operations-will-continue)) x
(100 (%) + margin (%))
```

```
(8,000 + (2,000 * 100)) * 1.5 = 315,000
```

Number of IDs required for all domains (total number of IDs required for all domains):

```
Number-of-IDs-required-for-entire-domains = number-of-IDs-required-for-domain-1 +
                  number-of-IDs-required-for-domain-2 +
                  ...
```

```
312,000 + 312,000 = 624,000
```

The following figure shows the range of user IDs and group IDs set under the above conditions. The minimum value of user IDs and group IDs to be set here is 1,000,000.

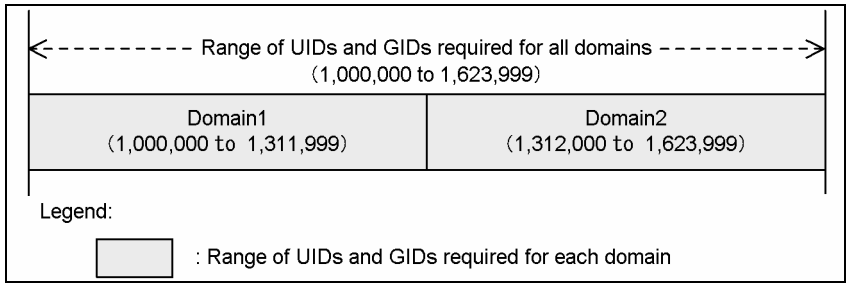



**Figure 2.24 Example of Setting User IDs and Group IDs**

Range of user IDs and group IDs required for entire domains:

1,000,000 to 1,623,999

Range of user IDs and group IDs required for `Domain1`:

1,000,000 to 1,311,999

Range of user IDs and group IDs required for `Domain2`:

1,312,000 to 1,623,999

## 2.6 Considerations before setting quotas

The NAS Modular system allows you to set user and group quotas for a file system. You can also set subtree quotas for directories immediately under a mount point, and for users and groups that use the directories.

When the user and group quotas set for a file system are used with a subtree quota, quota management becomes complicated. This is because when a user cannot create or update a file or directory, you must check each type of quota information to determine the cause. Therefore, we recommend that you set only one type of quota management in the NAS Modular system.

A system administrator must consider whether to set quotas for each file system or for each directory in order to efficiently manage quotas according to the operational requirements of the file systems.

This section explains examples of setting quotas according to the operational requirements of file systems.

### 2.6.1 Setting quotas for each file system

When many users share one file system, you can set quotas for the file system to prevent specific users or groups from stressing the system by using too much disk space.

The following shows an example of setting quotas for this purpose.

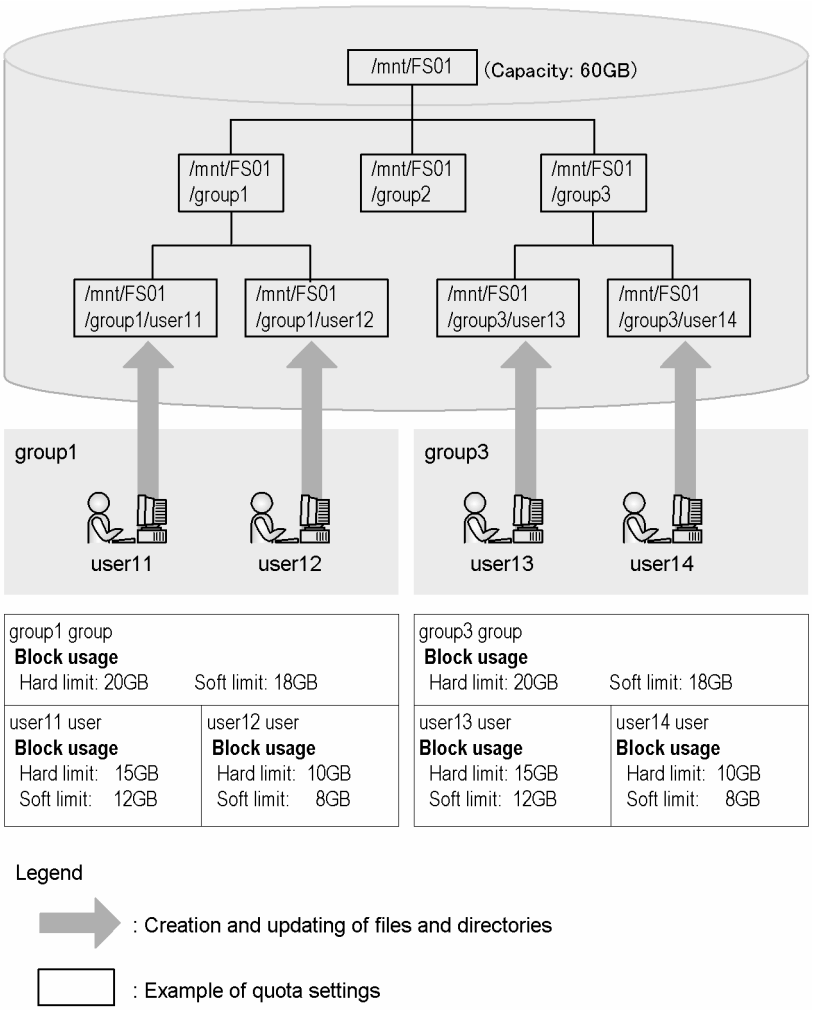



**Figure 2.25 Example of setting quotas for a file system**

For example, you can set quotas for `user11` and `group1`, which are using the `FS01` file system, to limit the block capacity usage.

### 2.6.2 Setting quotas for each directory

When you set the directories under the mount point for a file system made public to users and groups, you can set a subtree quota for each shared directory to prevent a particular directory from occupying too much space in the entire file system.

When you set a subtree quota, you can limit the capacity available in the directory. This enables you to operate a directory in the same way as a file system. Since you can specify any value for the capacity as a subtree quota, you can expand or contract the capacity flexibly.

The following shows an example of setting subtree quotas for these purposes.

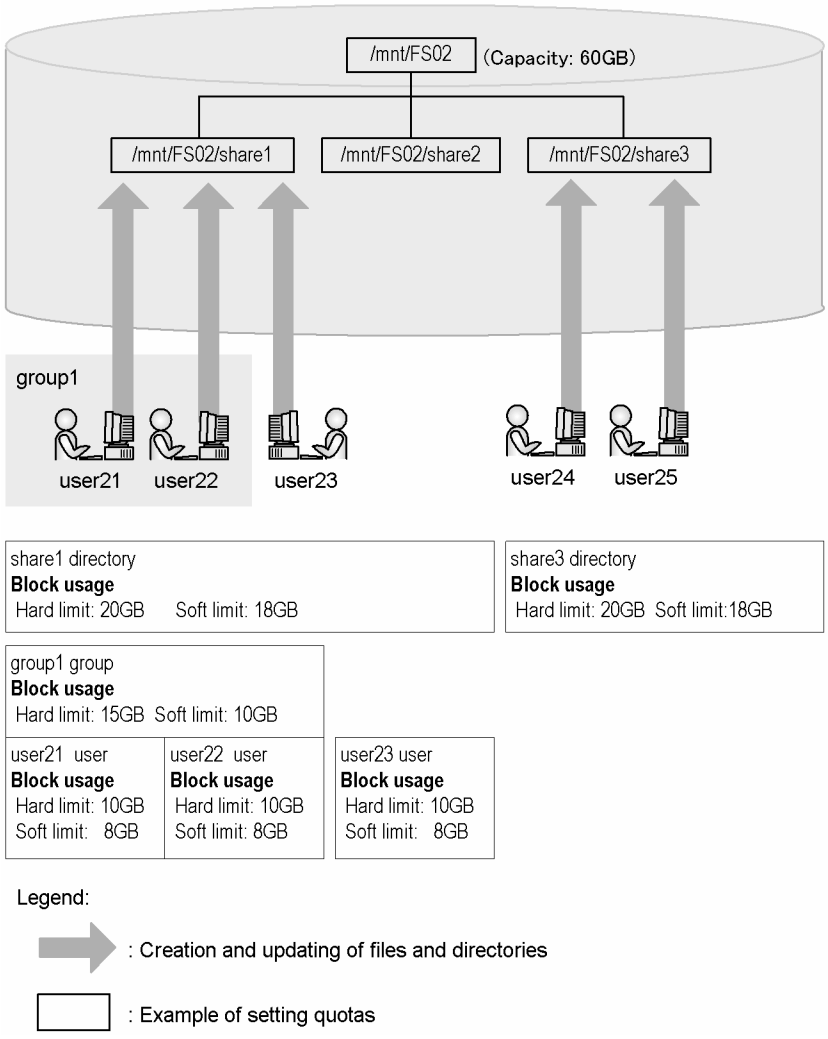



**Figure 2.26 Example of setting subtree quotas**

For example, you can set quotas for the `share1` directory in the `FS02` file system to limit the available block capacity for the directory. Also, you can set quotas for `user21` and `group1`, which are using the `share1` directory, to limit the block capacity available to `user21` and `group1` in this directory.

In this example, available block capacity for the `share3` directory in the `FS02` file system is limited to a maximum of 20 GB, but it can be expanded depending on the file system operation.

## 2.7 Verifying Environment Settings in a NAS Modular system

Before running the NAS Modular system, you (the system administrator) must first set the information required to operate the system, including the cluster configuration, network information, and system information. After you set the information from the NAS Manager, create a file system (or a file share) to start NAS Modular system operations.

A system administrator must confirm the server information such as server names and IP addresses in the NAS Modular system. Change the settings before starting NAS Modular system operations if necessary. ***Note:*** Host names cannot contain an underscore (_).

Table 2.5 lists the servers that you must check and configure before running the NAS Modular system.

**Table 2.5 NAS Manager Server Configuration**

| Server | Task |
|---|---|
| NTP | Set up NTP servers by using Storage Navigator Modular. You can specify up to two servers. Verify the IP addresses or host names. |
| NIS | Verify the NIS domain name. If necessary, you can set two NIS server host names or IP addresses.<br>For end users, a password must be encrypted using either the DES or MD5 algorithm.<br>If user information is to be managed via an NIS server, make sure that you do not duplicate any user names, group names, user IDs, or group IDs registered by NAS Manager or in an LDAP server for user authentication. If you use user mapping, user IDs and group IDs within the range set for user mapping cannot be registered in the NIS server.<br>You will not be able to set quotas for any user names or group names set in the NIS server that are identical to those registered by NAS Manager. |
| DNS | Verify the IP address of the primary DNS server. If necessary, you can set the IP address of a secondary DNS server. |
| WINS | Make sure that all the CIFS clients on the network are set as WINS clients. Since a NAS Unit does not support the WINS client, register the service IP address and NetBIOS name of the NAS Unit in the WINS server manually. |
| SNMP | Verify the password for the SNMP manager to access the MIB value of the agent, and the server name or network of the SNMP manager. |
| LDAP | To use user mapping, you must configure an LDAP server.<br>One of the following products is needed to configure the LDAP server:<br>▪ OpenLDAP<br>▪ Active Directory Application Mode (ADAM)<br>▪ Sun™ Java™ System Directory Server<br>You can create a replicate of the LDAP server that is configured using the above products. Taking into consideration the possibility of server failure, we recommend that you prepare a replicate server (slave) in addition to the LDAP server (master), to enhance reliability.<br>For details about configuring the LDAP server, see Appendix A.3, Notes on Configuring the LDAP Server. |
| Domain controller | Verify the server names, administrator names, and passwords of the primary domain controller in the domain. The server names of the backup domain controller can also be set if required. |
| LDAP server for user authentication | An LDAP server can be used for user authentication or for user mapping, but can<br>only be used for one purpose in a NAS Modular system.<br>LDAP server for user authentication<br>You can set one or two servers. Confirm the following information: |

| Server | Task |
|---|---|
| | IP address or host name<br>Port number<br>Identification name of the LDAP server root (in DN format)<br>Identification name of the LDAP server administrator (in DN format)<br>LDAP administrator password<br>When you use the LDAP server to manage user information, make sure that the user names, group names, user IDs, and group IDs do not overlap those registered by NAS Manager and the NIS server. User IDs and group IDs within the range set for user mapping using RIDs cannot be registered in the LDAP server.<br>You cannot set quotas for users or groups whose names have also been registered by NAS Manager.<br>If you want to use the NAS Manager end-user service, passwords must be encrypted using the DES algorithm. |
| LDAP server for user mapping | LDAP server for user mapping<br>Confirm the following information:<br>IP address or host name<br>Port number<br>Identification name of the LDAP server root (in DN format)<br>Identification name for which you want to add a user mapping account of the LDAP server (in DN format)<br>Identification name of the LDAP server administrator (in DN format)<br>LDAP administrator password<br>We recommend that you enhance reliability by setting up a replicate (secondary) LDAP server, additional to the primary LDAP server used in normal circumstances, in case a server error occurs. If you switch from one LDAP server to the other, you must change the NAS Manager settings. |

Before running the NAS Modular system, consider the NAS Modular system information to be set in NAS Manager. Verify that there are no duplicate settings between the NAS Units or between the NAS Manager system and your existing system.

Check the following NAS Manager settings before running the NAS Modular system:

- **Cluster name**

  This is the name of the cluster consisting of two NAS Units.

- **Node names**

  These are the names of the nodes of the NAS Units included in the cluster. Node names are used only in cluster management. The node name is different from the NNC name for each NAS Unit.

- **Service IP addresses and subnet masks**

  A service IP address is used by a user to connect to each service on a NAS Unit, and is assigned to each interface in a NAS Unit. The service IP addresses must use different network segments among the interfaces (gbe1 to gbe4) in the same NAS Unit. For details on service IP addresses, see 4.7.4.

- **Fixed IP addresses and subnet masks**

  The fixed IP addresses set for each interface (mng1 and gbe1 to gbe4) in a NAS Unit must use different network segments.

### 2.7.1 Operating with more than 10,000 Users or Groups

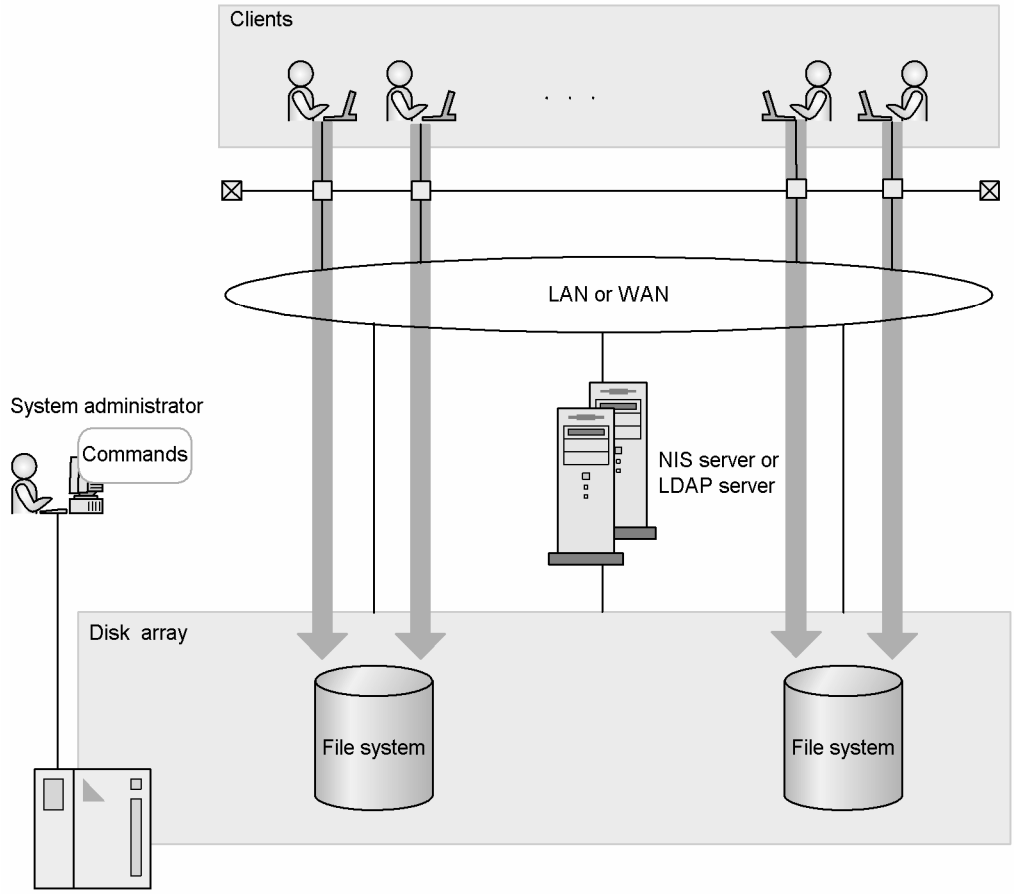
User information or group information may take a long time to acquire if a large number of users and groups are registered in the directory server connected to the NAS Modular system, or if a considerable load is placed on an external server or network. If the NAS Manager GUI remains inactive for longer than your Web browser's connection timeout (30 minutes), the transaction is forcibly disconnected and processing may not complete successfully.

To avoid such problems, the system administrator should switch to command operation mode in the **Select User Interface** window for running the NAS Modular system.

The following describes operation in an environment with more than 10,000 users or groups accessing a NAS Modular system.

#### 2.7.1.1 System requirements

The following figure shows the system requirements in an environment where the total number of users or groups exceeds 10,000.


Clients
LAN or WAN
System administrator
Commands
NIS server or
LDAP server
Disk array
File system
File system

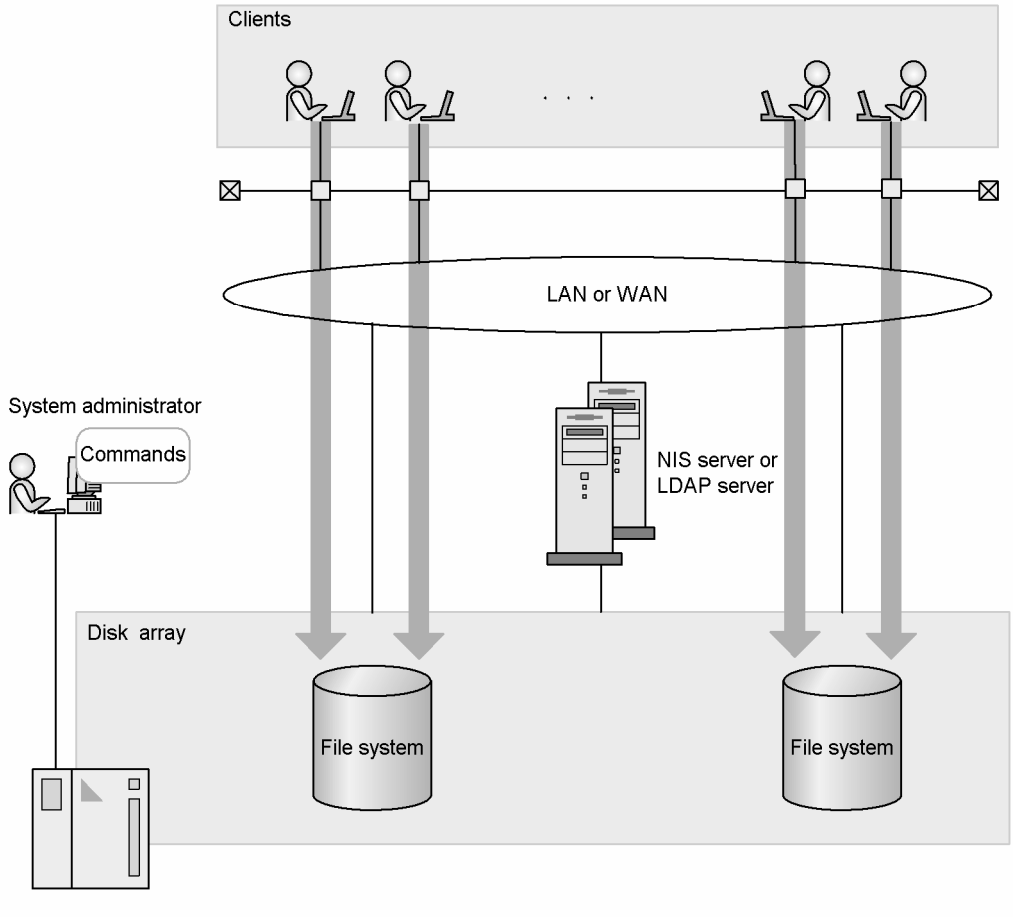



**Figure 2.27 System Requirements with more than 10,000 Users or Groups**

User information can be managed via an NIS server or LDAP server for user authentication.

Use a high-performance machine as the NIS server or LDAP server, and configure the network so that the traffic between the server and NAS Units will not affect performance.

Set up the NIS server or LDAP server before starting NAS Modular system operations.

### 2.7.1.2 GUI operations Deprecated in Command Operation Mode

When you switch from GUI operation mode to command operation mode, processing is suppressed for operations in the following windows where a timeout may occur:

- Setting users and groups without write permission to a CIFS share (**Write Disallowed Users / Groups** Setup window)
- Setting users and groups with write permission to a CIFS share (**Write Allowed Users / Groups** Setup window)
- Setting quotas for a user or group (Quota Setup window)
- Displaying quota information for users or groups (**List of Quota Information** window)

### 2.7.1.3 Operation in Command Operation Mode

Operation in command operation mode is as follows.

Setting users and groups with or without write permission to a CIFS share

You can set users or groups who are granted or denied write permission to a CIFS share in either of the following ways:

- Create the CIFS share in the **Create CIFS File Share** window, and then use the `enas_cifsedit` command to set the users and groups granted or denied write permission to that share.
- Using the `enas_cifscreate` command, create the CIFS share and set the users and groups granted or denied write permission to that share at the same time.

Managing quotas

Set the default quota for controlling the block usage and i-node usage by file system users. If you need to set a quota for a specific user or group, use the `enas_quotaset` command.

By using the `enas_quotaget` command in combination with the SNMP trap notification in summary notification mode, a system administrator can efficiently monitor file system usage for each user even in an environment with a large number of users and groups. For details on typical quota management, see section 1.2.5.

## 2.8 Reviewing a Client's Operating Environment

This section describes the operating environment for clients that use a file system provided by a NAS Modular system.

### 2.8.1 Notes on Using a File System from an NFS Client

Note the following points when you use a file system from an NFS client:

- We recommend that you mount the NFS share directory itself when mounting a file system of the NAS Modular system from an NFS client.

  If you mount a subdirectory of the NFS share directory from an NFS client and then unmount that subdirectory, you might be unable to delete or rename that subdirectory from the NFS client that is mounting the upper directory of that subdirectory. If this problem occurs, correct it by using the following procedure:

1. In the **Main Menu** window, click the **File Share Management** button.
2. In the **List of File Shares** window, select the target NFS share, and then click the **Edit** button.

   For details on the **List of File Shares** window, see section 4.11.1.
3. In the **Edit NFS File Share** window, click the **OK** button without editing the information about the NFS share.

   For details on the **Edit NFS File Share** window, see section 4.11.4.

- We recommend that you specify the `hard` option when mounting a file system of a NAS Modular system from an NFS client. If you specify the `soft` option, a failover may occur while your NFS client is using the NAS Modular system. Also, if you access the NAS Modular system when the system has failed over, a request issued from your NFS client may result in an error (`ETIMEDOUT` or `ECONNRESET`).

  The `hard` option is specified by default for most NFS clients.

- Specify the NFS version 3 protocol (vers=3) explicitly in the mount option of the NFS client when you use a file whose size is equal to or more than 2 GB in an NFS environment. If you do not specify the NFS protocol explicitly, a file whose size is equal to or more than 2 GB might not be usable (depending on the NFS client) in an NFS environment because the NFS version 2 protocol might be applied.

- When mounting a file system of the NAS Modular system from an NFS client, contact the system administrator and find out the NAS Modular system's service IP address that is to be used to access the file system. If the service IP address of the NAS Modular system is not correct, you will be unable to use that file system from the NFS client after failover.

- If using file locking, when mounting a file system from the NFS client make sure that you specify the host name that corresponds to the service IP address. The file lock may not function properly if the service IP address is specified, instead of the host name, when the file system is mounted.

- When *file locking* is used, the name resolution (conversion from an IP address to a host name) of a service IP address and host name of an NFS client must be identical between the NAS Modular system and the NFS client.

- If you manage the IP addresses and the host names in a system file of the NAS Modular system, add them to the `/etc/hosts` file.
- You must specify the `hard` and `intr` options when mounting a file system of the NAS Modular system from an NFS client (using Linux®, for example) that cannot interrupt file operations. If you do not specify these options, it might not be possible to stop file operations if an error occurs.
- When the administrator of the NAS Modular system uses a policy that creates other NFS shares for directories at a higher or lower level than the NFS-shared directory, an NFS client must mount the shared directory itself.

  When the NFS client has mounted the shared directory's subdirectories, if the client machine goes down or is stopped before they are unmounted, the subdirectories can no longer be deleted or renamed.

  In such a case, contact the administrator of the NAS Modular system.
- When using the NFS version 2 protocol on the NFS client side, if you also use the functions of NAS Backup Restore or NAS Sync Image, perform a hard mount (that is, specify `hard` for the NFS mount option).

  If you perform a soft mount (that is, specify `soft` for the NFS mount option), a timeout error (`ETIMEDOUT`) may occur when an NFS client attempts to access an NFS share. For most NFS clients, a `hard` mount is the default option.
- When you create a directory that will be mounted from an NFS client, you must use only ASCII characters.
- If some or all of the NFS client machines have multiple network interfaces that are used to communicate with the NAS Modular system, accesses to the NFS share might not be allowed and result in errors (ESTALE error). This problem is caused because, depending on the usage of cluster management software and other software, the IP address used to mount the NFS share and the IP address used to access the NFS share may be different. When you use a file system on a NAS Modular system from an NFS client in the above environment, specify all the host names corresponding to all the IP addresses of the machines that mount or access the NFS share as the NFS share public destinations while creating the NFS share. If you specify a wildcard (`*`), IP network, or net group as the NFS share public destinations, NFS clients might not be able to access the NFS share.

- In the OS used for an NFS client, note the following points for each operating system:
  - IRIX® (SGI)

    When the NFS client using SGI creates a new directory in the mounted directory and then creates a new file in the new directory, and the same operation is repeated under the new directory, the directories are deeply nested and the operation might stop.
  - HP-UX®

    When the operation is stopped while the NFS client using HP-UX® is performing a file copy by using the `cp` command, the copy-destination file privilege becomes 000.

    When failover occurs in the NAS Modular system while the NFS client using HP-UX® (11i) updates the file system, the process updating the file system might end abnormally after failover is performed. To prevent these failures, install PHNE_28567 (for 11.00) or PHNE_28568 (for 11.11) from the HP-UX® patch programs, which are provided by the Hewlett-Packard home page. For details on the patch programs, contact the vendor.
  - Linux®

    When the NFS client using Linux® locks a file in a directory that was mounted using the TCP protocol, it might take some time to release the wait for the file lock.

    ***Note:*** If a process that is locking a file is interrupted from an NFS client running on Linux®, the file lock information remains in the NAS Modular system and the system may be unable to lock the corresponding file.
- If a file is locked in a directory that was mounted from an NFS client using a Linux® kernel earlier than 2.4.21, the file may be unlocked when:
  - A failover or failback occurs.
  - The cluster is stopped and then restarted.

  If the file is unlocked as described above, other processes can lock this file and possibly corrupt it.

#### 2.8.1.1 Notes on using a File System from an NFS client

Note the following points when you use a file system from an NFS client:

- From an NFS client, do not use a file system for which an ACL is made available in a CIFS share. If, in a CIFS share of the NAS Modular system, an ACL is set to available for a file system and an NFS client uses that file system, when the files and directories are accessed, the access permission for those files and directories may not function as specified depending on the NFS implementation in the NFS client host.
- If a failover occurs in a NAS Modular system while an operation (such as creating, updating, or deleting a file or directory) is being performed due to an action (system call, library function, or command) from an NFS client, even if the operation finishes normally in the NAS Modular system, an error might occur on the NFS client.
- When you use the TCP protocol with an NFS client host to mount a file system of a NAS Modular system, a subsequent access might require from 1 to 10 seconds, depending on the implementation of the NFS client host. This situation arises when the directories and files in the file system have not been accessed for some time. Although an `ECONNRESET` error may be output to a system log, programs that access the file system using an NFS service will operate normally.
- When you create a special file for the NAS Modular system using an NFS client, note the following points:
  - If you use the NFSv3 protocol and specify a value of 256 or more for the major number or minor number, executing the `mknod` command causes an error.
  - If you use the NFSv2 protocol and use an OS other than Linux® for an NFS client, and then create a special file using an NFS client, a special file with the major number and minor number different from the specified values might be created. Even when Linux® is used, the same phenomenon might occur depending on the distribution. Thus, do not create a special file from an NFS client under the above conditions.
- When the NFS client using IRIX® creates a new directory in the mounted directory and then creates a new file in the new directory, and the same operation is repeated under the new directory, the directories are deeply nested and the operation might stop.
- When the operation is stopped while the NFS client using HP-UX® is performing a file copy by using the `cp` command, the copy-destination file privilege becomes 000.

  When failover occurs in the NAS Modular system while the NFS client using HP-UX® updates the file system, the process updating the file system might end abnormally after failover is performed. To prevent these failures, install PHNE_28567 (for 11.00) or PHNE_28568 (for 11.11) from the HP-UX® patch programs, which are provided by the HP (Hewlett-Packard) home page. For details on the patch programs, contact the vendor.

- When using Linux® kernel 2.4.x for an NFS client host, make sure that you apply the latest patch. If you use the kernel without the latest patch to perform an NFS access during any of the following types of processing, an error (error number 528) may occur:
  - NAS Backup Restore is copying or restoring data in the disk array.
  - NAS Sync Image is creating a differential-data snapshot of the file system.
  - An I/O operation is being performed on the file system.
- When AIX® is used as an NFS client host, NFS communication with a NAS Modular system uses a non-privileged port (internet port 1024 or higher) by default. To improve security, we recommend that you use a privileged port (internet port lower than 1024) that only the superuser can create. When privileged ports are used, general users must use an AIX NFS client system to access a NAS Modular system. This improves security when NFS services are used. For details about the settings required for using privileged ports, contact the vendor.

  When using a privileged port, in the **Create NFS File Share** window or **Edit NFS File Share** window, choose **Perform** for **Transmission port restriction**. For details about the **Create NFS File Share** window, see section 4.11.2. For details about the **Edit NFS File Share** window, see section 4.11.4.
- When a machine that uses HP-UX® or the RPC program number 100020 (`the host machine on which rpcinfo -p displays 100020 in program`) is used as an NFS client, you might not be able to correctly reference the contents of the hard link file that is under the directory mounted by an NFS client.

  When you create an NFS share or edit NFS share information, and specify the following settings, you can reference the contents of the hard link file correctly. If AIX®, IRIX®, Linux®, or Solaris is used as an NFS client, you do not need to specify the following settings:
  - When an NFS share is created

    Select **Do not perform** for **Subtree check** in the **Create NFS File Share** window. Alternatively, specify `do_not_perform` for the `-s` option in the `enas_nfscreate` command.
  - When NFS share information is edited

    Select **Do not perform** for **Subtree check** in the **Edit NFS File Share** window. Alternatively, specify `do_not_perform` for the `-s` option in the `enas_nfsedit` command.
- When an NFS client accesses a file system of the NAS Modular system, the following message may appear: file temporarily unavailable on the server, retrying... . In such a case, the system administrator might be intentionally preventing access to the target file system.

### 2.8.1.2 Notes on Changing the NAS Modular System Settings

Note the following points when you change the settings in the NAS Modular system:

- If you want to change a device in a file system in the NAS Modular system that was mounted by an NFS client, use an NFS client to unmount the NAS Modular system before changing the device, and then re-mount the NAS Modular system after changing it.
- If you delete an NFS share for the NAS Modular system with a file system mounted from an NFS client host, it may not be possible to unmount that file system depending on the implementation of the NFS client host. If you cannot unmount the file system, restart the NFS client host to release the file system from the mount state.
- Before a system administrator changes the maximum buffer size of data transmission in the configuration definition for a service, the NFS client host's administrator needs to unmount the file system from the NFS client. The NFS client host's administrator unmounts the file system from the NFS client as requested by the system administrator, and after confirming the changes in the configuration definition, mount the file system again on the NFS client.

## 2.8.2 Notes on Using a File System from a CIFS Client

**Name Resolution**

- When you access a shared directory from a CIFS client, use the following:

  `\\`*`NNC-name`*`\`*`CIFS-share-name`*`\`*`directory-path-to-be-used`*

  `\\`*`service-IP-address`*`\`*`CIFS-share-name`*`\`*`directory-path-to-be-used`*

  ***Note:*** An NNC name is equivalent to a NetBIOS name in a CIFS environment. To check an NNC name, service IP address, or CIFS shared name, contact the system administrator.

- The name resolution services that a CIFS client uses are WINS, DNS, or lmhosts. Note the following points when you use these name resolution services:
  - When using WINS

    Make sure that all the CIFS clients on the network are set as WINS clients. Since a NAS Unit does not support the WINS client, register the service IP address and NetBIOS name of the NAS Unit on the WINS server manually.
  - When using DNS

    Register the service IP address and NetBIOS name of the NAS Unit on the DNS server manually.
  - When using `lmhosts`

    In the lmhosts file provided for each CIFS client, register the service IP address and NetBIOS name of the NAS Unit.

**User Authentication**

- When the user mapping is used for Active Directory® domain authentication or NT domain authentication, and shared access authentication from the CIFS client fails, the possible causes are as follows:
  - A user ID or group ID could not be assigned, because a new user accessed the file system after all user IDs or group IDs within the available range were assigned. In such a case, expand the range for the user ID or group ID.
  - A user ID or group ID assigned by user mapping could not be accessed, or a user ID or group ID could not be assigned. In such a case, make sure that the CIFS service is running correctly, in the **List of Services** window. For details about how to view the status of the CIFS service, see 4.6.1.
  - If the CIFS service is running correctly, make sure that the LDAP server specified in the CIFS service configuration definition is running correctly.
  - Also check the CIFS logs to see whether or not error information was output.
- To perform Active Directory authentication or NT domain authentication without user mapping, the users registered in the domain controller must also be registered by NAS Manager, the NIS server, or LDAP server for user authentication.

  For group authentication, the group name you set in NAS Manager, the NIS server, or LDAP server for user authentication, does not need to match the group name registered in the domain controller. However, we recommend that you set the same name. Otherwise, the name you set will need to be associated with the group name registered in the domain controller when viewing or setting ACLs.
- If connection to the LDAP server for user mapping fails, access to the LDAP server will not be possible for five minutes after the connection failure is detected. As a result, users that need to access the LDAP server to use the CIFS service (new domain users and domain users whose cache is cleared) will be unable to access the CIFS service.

  In this case, remove the connection error to the LDAP server, wait for five minutes or restart the CIFS service, and then access the CIFS service. If restarting the LDAP server to remove an error, restart the CIFS service after restarting the LDAP server.
- When a CIFS client logs on to Windows® and accesses a CIFS share for the first time, an authentication request will be sent to the NAS Unit with the user name and password used when logging on to Windows®. Therefore, when access permissions for CIFS shares are granted to guest account users and the user logging on to Windows® is applied to the user specified in **Mapping to guest account** in the **CIFS Service Management** window, the user might access CIFS shares as a member of the guest account, and will not be requested to enter a user name and password. Note this when access permissions for a CIFS share are granted to guest account users.

  For Active Directory® authentication, entering the user name and password is requested when authentication using the user name and password used by the user logging in to Windows® fails. The user accesses CIFS shares as guest account when authentication fails.

- If using the Windows NT® domain controller or the Active Directory® domain controller to authenticate users, when an error occurs in the domain controller, the domain configuration information is changed, or the NAS Unit configuration is changed (when the NAS Unit is reinstalled or restored after an error occurs, and such.), the NAS Unit information in the Active Directory® domain or the Windows NT® domain may not match the domain configuration information in the NAS Unit, causing the authentication to fail. In this case, the following shows the method so that the CIFS client can connect the CIFS share:
  - If the Windows NT® domain controller is used to authenticate users, restart the CIFS service. For details on how to restart the CIFS service, see 4.6.3.3.
  - If the Active Directory® domain controller is used to authenticate users, rejoin the NAS Unit to the Active Directory® domain. For details on how to rejoin the NAS Unit to the Active Directory® domain, see 4.6.3.3.
- If the Active Directory® domain controller or the Windows NT® domain controller authenticates users and you are not using user mapping, the CIFS client needs to log on to the domain containing the NAS Unit, even if it has trust relationships with multiple Active Directory® domains when accessing a shared directory created by a NAS Unit.

  When using the domain controller for Active Directory® authentication to verify a user, and an attempt to access the CIFS share from a CIFS client fails during authentication, authentication ticket verification for the CIFS client might have failed. Log in to the CIFS client again or restart Windows.

**CIFS Client Access**

- When a file system is used from a CIFS client and a system administrator makes changes in the configuration definition for the CIFS service, the operation from the CIFS client might not finish normally. If this occurs, run the operation again after modifying the configuration definition for the CIFS service.
- If a system administrator changes CIFS share information when a CIFS client is using a file system, the changed contents might not take effect. Re-connect the CIFS share or restart Windows to apply the changed contents.
- If the CIFS service is restarted when access to file systems is blocked, a CIFS client might not be able to connect to the CIFS file share. In such a case, an operation that blocks access to file systems might be in progress. If so, wait until this operation finishes, and then restart the CIFS service.
- The following table lists the operations that can block access to file systems, and explains how to check if an operation has completed.

**Table 2.6 Verification Tasks before Restarting CIFS Service**

| Operation | Items to Verify |
|---|---|
| Creating a differential-data snapshot (NAS Sync Image) | ▪ Ensure that a differential-data snapshot is not being created in the Create a Differential-Data Snapshot or Delete and Create Differential-Data Snapshot Windows.<br>▪ Ensure that a differential-data snapshot is not being created by the `syncadd` command.<br>▪ Ensure that automatic creation of differential-data snapshots is not scheduled in the **List of File Systems** used for Sync Image or Set up Automatic Creation of Differential-Data Snapshots windows.<br>Also, if automatic creation of a differential-data snapshot is scheduled to be performed at the present time, acquire the system message or SNMP trap to make sure that the automatic creation has finished.<br>For details about the system message to be output and SNMP trap to be issued when automatic creation is performed, see the *NAS Sync Image User's Guide*. |
| Expanding a differential-data storage device (NAS Sync Image) | ▪ Ensure that a differential-data storage device is not being expanded in the Expand a Differential-Data Storage Device window.<br>▪ Ensure that a differential-data storage device is not being expanded by the `syncexpand` command. |
| Executing the `horc_pvol_freeze` command (NAS Backup Restore) | Use the `horc_pvol_unfreeze` command for the file system for which writing was disabled with the `horc_pvol_freeze` command, then check whether the file system is write-enabled. |
| Performing online backup (NAS Backup Restore) | Ensure that online backup is not being performed:<br>▪ Ensure that `stopped` is displayed for **NDMP server status**, or `running` is displayed for **NDMP server status** and the **Stop** button is displayed in the NDMP Server Control window.<br>▪ Ensure that the values for `backupsvrstatus` and `mediasvrstatus`, which are displayed when executing the `NDMPcontrol` command with the `-l` option, are both `disconnected`. |

For details about the windows and commands of NAS Backup Restore and NAS Sync Image, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide* and *Hitachi AMS/WMS NAS Sync Image User's Guide*.

- The number of CIFS clients that can connect simultaneously are limited to 2000 users per node for TagmaStore AMS500 or AMS1000, and limited to 1000 users for TagmaStore AMS200 or TagmaStore WMS100. Disconnection is not performed if the process is still active even after access has been stopped. Even when multiple resource groups are running on a single node due to the occurrence of a failover, the number of CIFS clients that can connect to a single node is 100 or fewer.
- The number of CIFS clients that can connect concurrently is limited to 2,000*(see**Note**)* users per node when no user file access occurs. Disconnection is not performed if the process is still active even after access has been stopped. Even when multiple resource groups are running on a single node due to the occurrence of a failover, the number of CIFS clients that can connect to a single node is 2,000[#1] or fewer .

  ***Note:*** Limited to 2,000 users for the TagmaStore AMS 500 or TagmaStore AMS 1000, and 1,000 users for the TagmaStore AMS 200 or TagmaStore WMS 100.
- If an error occurs on the CIFS client or network when a write request is cached on the CIFS client, the data might not be guaranteed. Note this when specifying that updated data in CIFS share files is to be cached on the client.
- In a CIFS share where the updated data in files is specified to be cached on the client, and synchronous control for writing is configured, if another CIFS client tries to open the file that was first accessed by the CIFS client on which a write request is cached, writing and disk flushes are performed by priority. Therefore, it might take a long time for the second CIFS client to open the file.
- If a CIFS client moves a folder in a CIFS share, the timestamp of the folder is updated to the time at which the folder was moved.

**Files, ACLs, and Permissions in a CIFS Share**

- If user mapping is to be used, the names of users and groups you register in NAS Manager, the NIS server, or LDAP server for user authentication, must not be the same as any user or group names registered in the domain controller.

  When accessing a CIFS share from an CIFS client while using a user or group name registered in the domain controller (which was set by NAS Manager, the NIS server, or LDAP server for user authentication) with an ID that differs from the user ID or group ID assigned by user mapping, folders and files might be created under the user ID or group ID set by NAS Manager, the NIS server, or LDAP server for user authentication, and not under the user ID or group ID assigned by user mapping.

  This occurs when the user ID or group ID has exceeded the specified range, or when the user ID or group ID has not been assigned due to a problem such as an LDAP server (for user mapping) failure.
- Even if execution permissions are set for the owner of a file in a CIFS share, the settings are not in effect.
- If an ACL is specified in the Folder Properties window for a file created in a CIFS share, the default ACL and access ACL change.

If, in the File or Folder Properties window, an ACL is set up for a folder created in a CIFS share, the Name field of the Properties window displays the comment entered by the system administrator when the user was registered.

- If, in the File or Folder Properties window, an ACL is set up for a folder created in a CIFS share, select a user or group as follows, depending on the authentication method for the CIFS service:
  - When you are not using user mapping for the local authentication, NT server authentication, Active Directory® authentication, or NT domain authentication

    Select a user or group where the NNC name of the NAS Unit is displayed in the Lo**OK** in field of the Properties window. When you select Active Directory® authentication or NT domain authentication, the Lo**OK** in field of the Properties window might display the domain controller. However, in this case, an ACL is not set even if an ACL is set to the user or the group.
  - When you are using user mapping for the Active Directory® authentication or the NT domain authentication

    Select a user or group where the domain controller is displayed in the **LoOK in** field of the Properties window.
- If an ACL is specified in the File or Folders Properties window for a file or folder created in a CIFS share, the user who created the target file or folder cannot be deleted.
- Only the user or CIFS administrator who created the target file or folder in a CIFS share can set an ACL.
- The owner of the file or folder created in a CIFS share cannot be changed.
- Full control permissions are set for creators of folders in a CIFS share. This setting cannot be changed.
- You cannot remove the read permissions from the creator of files created in a CIFS share.
- If a CIFS client sets an ACL from the properties window of a folder, full control (rwx) is set for the mask regardless of the set access permissions.

**Sharing with NFS**

- When the CIFS service and the NFS service share a directory, the user ID and group ID used for both services must be identical. When using user mapping, first assign a user ID and group ID to be used in the CIFS service, and then assign the same user ID and group ID to the corresponding user in the NFS client host. Check information about user IDs and group IDs assigned by user mapping as follows:

  User mapping using RIDs

  Use the `enas_umidget` command to check the IDs or names of the users and groups that are mapped using RIDs. For details, see 5.7.4.

  User mapping using LDAP

- In the **List of RAS Information** (Batch-download) window, you can download user-mapping information. For details on how to download the information, see section 4.13.10.
- A CIFS client cannot access the symbolic link created in a CIFS share. A symbolic link in a CIFS share is created, for example, by an NFS client.
- Permissions set for files and directories shared in a CIFS share of NAS Manager operate in the same manner as with access permissions set for an NFS share.
- When the CIFS service and NFS service share the same directory and file, specify that updated data in CIFS share files is not to be cached on the client. If the data is cached on the client, data inconsistencies might occur because the CIFS service manages this setup.
- When an NFS client uses a file for which a CIFS client has set read-only permissions, if the NFS client sets read-only permissions, those permissions will not be effective.

**Failover**

Operations on CIFS clients that were using resource group services moved by failover or failback are suspended forcibly.

**Using a File System from an FTP Client**

If a failover or failback occurs while an FTP client is accessing a file system that belongs to the target resource group, the connection is forcibly disconnected or is placed in the response- wait status. To restart access to the file system, reconnect to the file system.

### 2.8.3 Configuring the LDAP Server

You must configure the LDAP server when setting user mapping. This section provides information on configuring the LDAP server using OpenLDAP, ADAM or Sun Java System Directory Server.

You must restart the CIFS service when the LDAP server is initialized or re-configured. Make sure that no user is accessing the CIFS share before restarting the CIFS service.

The following products are required for configuring an LDAP server to be used in a NAS Modular system. Use any one of these products to configure the LDAP server.

Configuring an LDAP server for user authentication

- OpenLDAP
- Sun Java System Directory Server

Configuring an LDAP server for user mapping

- OpenLDAP
- Sun Java System Directory Server
- ADAM

After initializing or reconfiguring an LDAP server, you must restart the CIFS service. Before you restart the CIFS service in the **List of Services** window, make sure that no users are accessing any CIFS shares.

#### 2.8.3.1 Configuring the LDAP Server by using OpenLDAP

The following gives notes on configuring the LDAP server by using OpenLDAP. There is no need to create a schema file when using an LDAP server for user authentication.

**Table 2.7 Configuration Tasks for Configuring the LDAP Server using OpenLDAP**

| Operation | Description |
|---|---|

| Operation | Description |
|---|---|
| Creating a schema file | When using user mapping, use OpenLDAP to create a schema file that defines the attribute and object classes recognized on the LDAP server. You must define the attribute and object classes to store the user IDs and group IDs that have been converted by user mapping.<br>The NAS Modular system provides a schema file (`samba.schema`) for user mapping using LDAP. Use SSH to log on to the NAS Unit, and then obtain the schema file from the following directory with FTP:<br>`/usr/share/doc/samba/examples/samba.schema`<br>When you create a schema file for the LDAP server that is configured by using OpenLDAP, define the following attribute and object classes:<br>`attributetype ( 1.3.6.1.4.1.7165.2.1.20 NAME 'sambaSID'`<br>`DESC 'Security ID'`<br>`EQUALITY caseIgnoreIA5Match`<br>`SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{64} SINGLE-VALUE )`<br>`objectclass ( 1.3.6.1.4.1.7165.1.2.2.7 NAME 'sambaUnixIdPool' SUP top AUXILIARY`<br>`DESC 'Pool for allocating UNIX uids/gids'`<br>`MUST ( uidNumber $ gidNumber ) )`<br>`objectclass ( 1.3.6.1.4.1.7165.1.2.2.8 NAME 'sambaIdmapEntry' SUP top AUXILIARY`<br>`DESC 'Mapping from a SID to an ID'`<br>`MUST ( sambaSID )`<br>`MAY ( uidNumber $ gidNumber ) )`<br>`objectclass ( 1.3.6.1.4.1.7165.1.2.2.9 NAME 'sambaSidEntry' SUP top STRUCTURAL`<br>`DESC 'Structural Class for a SID'`<br>`MUST ( sambaSID ) )`<br>After a schema file is created or obtained, add the `include` directive to the LDAP server definitions to read the schema file required for user mapping.<br>The following shows an example of describing the include directive when the schema file is stored in the directory `/etc/ldap/schema`:<br>`include /etc/ldap/schema/samba.schema` |
| Setting the Index Directive | When you store a large number of user IDs and group IDs on the LDAP server configured using OpenLDAP, the search performance for the LDAP server might deteriorate. If this happens, set the index directive. We recommend that the index directive in the LDAP server definitions be set as follows:<br>LDAP server for user authentication:<br>`index uidNumber,gidNumber,objectClass,uid,cn,memberUid eq`<br>LDAP server for user mapping:<br>`index uidNumber,gidNumber,objectClass,sambaSID eq`<br>If you have changed the index directive, you must re-create an index based on the database currently stored in the LDAP server. Use the `slapindex` command to re-create an index. When executing the `slapindex` command, stop the LDAP server, use the `slapindex` command, and then restart the LDAP server. |

| Operation | Description |
|---|---|
| Setting the Sizelimit Directive | When you use an OpenLDAP LDAP server, you can specify a maximum search number (number of entries returned by search requests from an LDAP client). The default is 500 entries. When the number of user mapping information entries in the LDAP server exceeds the maximum number, downloading of user mapping information in the **List of RAS Information** (Batch-download) window or viewing quotas in the **List of Quota Information** window will fail. To resolve this problem, add the following sizelimit directive to the LDAP server definitions:<br>`sizelimit -1` |

### *2.8.3.2* Notes on configuring the LDAP server by using ADAM

The following gives notes on configuring the LDAP server by using ADAM.

**Table 2.8 Configuration Tasks for Configuring the LDAP Server using ADAM**

| Operation | Description |
|---|---|
| Creating a schema file | When using user mapping, create a schema file that defines the attribute and object classes recognized on the LDAP server that is configured using ADAM. You must define the attribute and object classes to store the user IDs and group IDs that have been converted by user mapping.<br>The NAS Modular system provides a schema file (`samba.ldf`) required for user mapping. Use SSH to log on to the NAS Unit, and then obtain the schema file from the following directory with FTP. If the FTP server is not provided on the Windows system, use the FTP function of the NAS Modular system to temporarily copy the following file to a directory that can be transferred with FTP, and then obtain the schema file.<br>`/usr/share/doc/samba/examples/samba.ldf`<br>When you create a schema file for the LDAP server that is configured using ADAM, define the following attribute and object classes:<br>`dn: CN=uidNumber,CN=Schema,CN=Configuration,DC=X`<br>`changetype: ntdsSchemaAdd`<br>`objectClass: top`<br>`objectClass: attributeSchema`<br>`cn: uidNumber`<br>`attributeID: 1.3.6.1.1.1.1.0`<br>`attributeSyntax: 2.5.5.9`<br>`isSingleValued: TRUE`<br>`showInAdvancedViewOnly: FALSE`<br>`adminDisplayName: uidNumber`<br>`adminDescription: An integer uniquely identifying a user in an`<br>`administrative domain`<br>`oMSyntax: 2`<br>`searchFlags: 1`<br>`lDAPDisplayName: uidNumber`<br>`systemOnly: FALSE`<br>`systemFlags: 16`<br><br>`dn: CN=gidNumber,CN=Schema,CN=Configuration,DC=X`<br>`changetype: ntdsSchemaAdd` |

| Operation | Description |
|---|---|
| | objectClass: top<br>objectClass: attributeSchema<br>cn: gidNumber<br>instanceType: 4<br>attributeID: 1.3.6.1.1.1.1.1<br>attributeSyntax: 2.5.5.9<br>isSingleValued: TRUE<br>showInAdvancedViewOnly: FALSE<br>adminDisplayName: gidNumber<br>adminDescription: An integer uniquely identifying a group in an<br>administrative domain<br>oMSyntax: 2<br>searchFlags: 1<br>lDAPDisplayName: gidNumber<br>systemOnly: FALSE<br>systemFlags: 16<br><br>dn: CN=sambaSID,CN=Schema,CN=Configuration,DC=X<br>changetype: ntdsSchemaAdd<br>objectClass: top<br>objectClass: attributeSchema<br>cn: sambaSID<br>instanceType: 4<br>attributeID: 1.3.6.1.4.1.7165.2.1.20<br>attributeSyntax: 2.5.5.12<br>isSingleValued: TRUE<br>showInAdvancedViewOnly: FALSE<br>adminDisplayName: sambaSID<br>adminDescription: Security ID<br>oMSyntax: 64<br>searchFlags: 1<br>lDAPDisplayName: sambaSID<br>systemOnly: FALSE<br>systemFlags: 16<br><br>dn: CN=sambaUnixIdPool,CN=Schema,CN=Configuration,DC=X<br>changetype: ntdsSchemaAdd<br>objectClass: top<br>objectClass: classSchema<br>cn: sambaUnixIdPool<br>instanceType: 4<br>possSuperiors: container<br>subClassOf: top<br>governsID: 1.3.6.1.4.1.7165.1.2.2.7 |

| Operation | Description |
|---|---|
| | rDNAttID: cn<br>showInAdvancedViewOnly: FALSE<br>adminDisplayName: sambaUnixIdPool<br>adminDescription: Pool for allocating UNIX uids/gids<br>objectClassCategory: 3<br>lDAPDisplayName: sambaUnixIdPool<br>systemOnly: FALSE<br>systemPossSuperiors: organizationalUnit<br>systemPossSuperiors: domainDNS<br>mustContain: uidNumber<br>mustContain: gidNumber<br>defaultSecurityDescriptor:<br><br>D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDS<br>DDTSW;;;SY)(A;;RPLCLORC;;;AU)<br>systemFlags: 16<br>defaultHidingValue: FALSE<br><br>dn: CN=sambaIdmapEntry,CN=Schema,CN=Configuration,DC=X<br>changetype: ntdsSchemaAdd<br>objectClass: top<br>objectClass: classSchema<br>cn: sambaIdmapEntry<br>instanceType: 4<br>possSuperiors: container<br>subClassOf: top<br>governsID: 1.3.6.1.4.1.7165.1.2.2.8<br>rDNAttID: cn<br>showInAdvancedViewOnly: FALSE<br>adminDisplayName: sambaIdmapEntry<br>adminDescription: Mapping from a SID to an ID<br>objectClassCategory: 3<br>lDAPDisplayName: sambaIdmapEntry<br>systemOnly: FALSE<br>systemPossSuperiors: organizationalUnit<br>systemPossSuperiors: domainDNS<br>mustContain: sambaSID<br>mayContain: gidNumber<br>mayContain: uidNumber<br>defaultSecurityDescriptor:<br><br>D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDS<br>DDTSW;;;SY)(A;;RPLCLORC;;;AU)<br>systemFlags: 16 |

| Operation | Description |
|---|---|
| | defaultHidingValue: FALSE<br><br>dn: CN=sambaSidEntry,CN=Schema,CN=Configuration,DC=X<br>changetype: ntdsSchemaAdd<br>objectClass: top<br>objectClass: classSchema<br>cn: sambaSidEntry<br>instanceType: 4<br>possSuperiors: container<br>subClassOf: top<br>governsID: 1.3.6.1.4.1.7165.1.2.2.9<br>rDNAttID: sambaSID<br>showInAdvancedViewOnly: FALSE<br>adminDisplayName: sambaSidEntry<br>adminDescription: Structural Class for a SID<br>objectClassCategory: 1<br>lDAPDisplayName: sambaSidEntry<br>systemOnly: FALSE<br>systemPossSuperiors: organizationalUnit<br>systemPossSuperiors: domainDNS<br>mustContain: sambaSID<br>defaultSecurityDescriptor:<br><br>D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDS<br>DDTSW;;;SY)(A;;RPLCLORC;;;AU)<br>systemFlags: 16<br>defaultHidingValue: FALSE<br>After a schema file is created or obtained, enter the following command, on one line, at the command prompt to use user mapping.<br>ldifde -i -f C:\samba.ldf -s localhost:*port* -j . -k -c "CN=Schema,CN=Configuration,DC=X" #schemaNamingContext<br>In this example, the schema file is saved as C:\samba.ldf. For *port*, specify the LDAP port number that was specified when ADAM was installed. The ldifde command exists in the system when ADAM or Active Directory is installed. To use the ldifde command for ADAM, choose **Start**, **All programs**, **ADAM**, and then **ADAM Tool command Prompt**. |

| Operation | Description |
|---|---|
| Setting an index | When you store a large number of user IDs and group IDs on the LDAP server configured using ADAM, the search performance for the LDAP server might deteriorate. In such a case, set an index.<br>When you use ADAM to expand a schema, an index is set for the expanded attributes `uidNumber`, `gidNumber`, and `sambaSID`. The following describes the procedure for setting an index for `objectClass` that is the system's existing attribute. For details on the **ADAM ADSI Edit** tool and the terms used in the procedure, see the Microsoft documentation.<br>To set an index:<br>Use the **ADAM ADSI Edit** tool to connect to the schema partition.<br>Expand the console tree. In the Details window, double-click **cn=Object-Class**.<br>In the Properties window, double-click the **searchFlags** attribute to edit the attribute value.<br>The current setting is `8`. Change it to `9`.<br>If the setting has already been changed, set as follows according to the setting:<br>Odd number:<br>Use the setting without change.<br>Even number:<br>Increase the set value by one.<br>Click **OK** twice to close the dialog box. |
| Setting the search limit | When you use an ADAM LDAP server, you can specify a maximum search number (number of entries returned in response to search requests from an LDAP client). The default is 1,000 entries.<br>When the number of user mapping information entries in the LDAP server exceeds the maximum number, downloading of user mapping information in the **List of RAS Information** (Batch-download) window will fail. To prevent this problem, increase the limit value in `MaxPageSize` so that the maximum number of search results does not exceed the total number of managed users and groups.<br>The following describes the procedure for increasing the limit in `MaxPageSize`. For details on the **ADAM ADSI Edit** tool and the terms used in the procedure, see the Microsoft documentation.<br>To expand the limit:<br>Use the **ADAM ADSI Edit** tool to connect to the configuration partition.<br>Expand the console tree, and then click **CN=Services**, **CN=Windows NT**, **CN=Directory Service**, and then **CN=Query-Policies**.<br>In the Details window, double-click **cn=Default Query Policy**. In the Properties window, double-click the **lDAPAdminLimits** attribute to edit the attribute value.<br>Select `MaxPageSize=1000`, and then click the **Remove** button.<br>Enter `MaxPageSize=`*limit*, and then click the **Add** button.<br>For *limit*, enter the sum of the maximum number of users and the maximum number of groups, considering the range of user IDs and group IDs to be set when you set user mapping for the NAS Modular system.<br>Click **OK** twice to finish the setting. |

### 2.8.3.3 Notes on configuring the LDAP server by using Sun Java System Directory Server

The following gives notes on configuring the LDAP server by using Sun Java System Directory Server.

**Table 2.9 Configuration Tasks for LDAP Server using Sun Java System Directory Server**

| Operation | Description |
|---|---|
| Creating a schema file | When using user mapping, create a schema file that defines the attribute and object classes recognized on the LDAP server that is configured using Sun Java System Directory Server. You must define the attribute and object classes to store the user IDs and group IDs that have been converted with user mapping.<br>The NAS Modular system provides a schema file (`samba.ldif`) required for user mapping. Use SSH to log on to the NAS Unit, and then obtain the schema file from the following directory with FTP:<br>`/usr/share/doc/samba/examples/samba.ldif`<br>When you create a schema file for the LDAP server that is configured using Sun Java System Directory Server, define the following attribute and object classes:<br>`dn: cn=schema`<br>`changetype:modify`<br>`add: attributeTypes`<br>`attributeTypes: ( 1.3.6.1.4.1.7165.2.1.20 NAME 'sambaSID' DESC 'Security ID'`<br>`SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE X-ORIGIN 'user defined' )`<br>`-`<br>`add:objectClasses`<br>`objectClasses: ( 1.3.6.1.4.1.7165.1.2.2.7 NAME 'sambaUnixIdPool' SUP top`<br>`AUXILIARY MUST ( uidNumber $ gidNumber ) X-ORIGIN 'user defined' )`<br>`-`<br>`add:objectClasses`<br>`objectClasses: ( 1.3.6.1.4.1.7165.1.2.2.8 NAME 'sambaIdmapEntry' SUP top`<br>`AUXILIARY MUST sambaSID MAY ( uidNumber $ gidNumber ) X-ORIGIN`<br>`'user defined' )`<br>`-`<br>`add:objectClasses`<br>`objectClasses: ( 1.3.6.1.4.1.7165.1.2.2.9 NAME 'sambaSidEntry' SUP top`<br>`STRUCTURAL MUST sambaSID X-ORIGIN 'user defined' )`<br>`-` |

| Operation | Description |
|---|---|
| | After a schema file is created or obtained, enter the following command to expand the schema so that you can read the schema file for user mapping. If you are prompted for a password, enter the password that was set for `cn=Directory Manager` during installation.<br>`#ldapmodify -h` *host-name* `-p` *port-number* `-D "cn=Directory Manager" -w - -f samba.ldif`<br>Use the `ldapmodify` command provided by Sun Java System Directory Server (do not use the same command provided by OpenLDAP). For *host*, specify the host name of the LDAP server configured using Sun Java System Directory Server. For *port*, specify the LDAP port number that was specified when Sun Java System Directory Server was installed. |

| Operation | Description |
|---|---|
| Setting an index | When you store a large number of user IDs and group IDs on the LDAP server configured using Sun Java System Directory Server, the search performance for the LDAP server might deteriorate. In such a case, set indexes.<br>When you use Sun Java System Directory Server, an equivalent index is set for the `objectClass` attribute. When using user mapping, you should set an equivalent index (`eq`) for `uidNumber`, `gidNumber`, and `sambaSID` in the Sun Java System Directory Server definition.<br>We recommend that you set an equivalent index in the Sun Java System Directory Server definitions, as follows:<br>-LDAP server for user authentication:<br>Set an equivalent index (`eq`) for `uidNumber`, `gidNumber`, `memberUid`, `uid`[#1], and `cn`[#1].<br>[#1:] An equivalent index is set by default.<br>-LDAP server for user mapping:<br>Set an equivalent index (`eq`) for `uidNumber`, `gidNumber`, and `sambaSID`.<br>The procedure for setting an equivalent index is described below. For details on the terms used in the procedure, see the Sun Microsystems documentation.<br>To set an equivalent index:<br>In the Configuration page at the top level in the LDAP server that is configured using Sun Java System Directory Server, expand the **Data** node, and then select the suffix for which you want to create an index.<br>In the right panel, choose the **Indexes** tab.<br>You cannot change the system index table.<br>Add an index with the attribute shown in the **Additional Indexes** table.<br>To add an index whose attribute is not generated, click the **Add Attributes** button.<br>In the dialog box that appears, select the attributes for generating the index, and then click **OK**.<br>-LDAP server for user authentication<br>Select `uidNumber`, `gidNumber`, `memberUid`, `uid`[#1], and `cn`[#1].<br>[#1:] An equivalent index is set by default.<br>-LDAP server for user mapping<br>Select `uidNumber`, `gidNumber`, and `sambaSID`..<br>To change the index of an attribute, in the **Additional Indexes** table, select the check box for the index type that you want to maintain with the attribute.<br>-LDAP server for user authentication<br>Make sure that the check boxes for the **Equivalent** index are selected for `uidNumber`, `gidNumber`, and `memberUid`. Clear the check boxes for the **Presence** index. Do not select any other check box.<br>-LDAP server for user mapping<br>Make sure that the check boxes for the **Equivalent** index are selected for `uidNumber`, `gidNumber`, `sambaSID`, and `uid`. Clear the check boxes for the **Presence** index. Do not select any other check box. Make sure that the check boxes for the **Equivalent**, **Presence**, and **Partial String** indexes are selected for `cn`. Do not select any other check box.<br>Click **Save** to save the new index setting.<br>A warning dialog box appears, indicating that the database file must be updated before you can use the new index.<br>You can either re-create the index for the suffix or re-initialize the suffix. Here, since mapping information is not registered yet, select **Do nothing**. |

| Operation | Description |
|---|---|
| Setting the limit on the number of clients | For an LDAP server for Sun Java System Directory Server, you can specify the maximum search number (number of entries that can be returned in response to search requests from an LDAP client). The default is 2,000 entries.<br>When the number of user mapping information entries in the LDAP server exceeds the maximum number, downloading of user mapping information in the **List of RAS Information** (Batch-download) window or viewing quotas in the Quota Information window will fail. To prevent this problem, change the maximum number of search results to **Unlimited** for the LDAP server configured using Sun Java System Directory Server.<br>The following describes the procedure for changing the maximum number of search results to **Unlimited**. For details on the terms used in the procedure, see the Sun Microsystems documentation.<br>To change the maximum number of search results:<br>In the Configuration page at the top level in the LDAP server that is configured using Sun Java System Directory Server, display the directory tree, and then select **Performance**.<br>In the right panel, choose the **Client Control** tab.<br>For **Size Limit** and **Look-through Limit**, select the check box for **Unlimited**.<br>Click the **Save** button.<br>A message appears, indicating that Sun Java System Directory Server must be restarted.<br>Click the **OK** button.<br>Click the **Tasks** tab, and then click the **Yes** button for restarting Sun Java System Directory Server.<br>Click the **Close** button to close the Restart Directory Server dialog box. |

### 2.8.4 Notes on using ADAM

The following gives notes on configuring an LDAP server for user mapping by using ADAM. Note that ADAM does not support configuration of an LDAP server for user authentication and cannot be used for that purpose.

**Table 2.10 Configuration Tasks for LDAP Server using Sun Java System Directory Server**

| Operation | Description |
|---|---|
| Creating a schema file | dn: CN=uidNumber,CN=Schema,CN=Configuration,DC=X<br>changetype: ntdsSchemaAdd<br>objectClass: top<br>objectClass: attributeSchema<br>cn: uidNumber<br>attributeID: 1.3.6.1.1.1.1.0<br>attributeSyntax: 2.5.5.9<br>isSingleValued: TRUE<br>showInAdvancedViewOnly: FALSE<br>adminDisplayName: uidNumber<br>adminDescription: An integer uniquely identifying a user in an administrative domain<br>oMSyntax: 2<br>searchFlags: 1<br>lDAPDisplayName: uidNumber<br>systemOnly: FALSE<br>systemFlags: 16 |

| Operation | Description |
| --- | --- |
| | dn: CN=gidNumber,CN=Schema,CN=Configuration,DC=X<br>changetype: ntdsSchemaAdd<br>objectClass: top<br>objectClass: attributeSchema<br>cn: gidNumber<br>instanceType: 4<br>attributeID: 1.3.6.1.1.1.1.1<br>attributeSyntax: 2.5.5.9<br>isSingleValued: TRUE<br>showInAdvancedViewOnly: FALSE<br>adminDisplayName: gidNumber<br>adminDescription: An integer uniquely identifying a group in an administrative domain<br>oMSyntax: 2<br>searchFlags: 1<br>lDAPDisplayName: gidNumber<br>systemOnly: FALSE<br>systemFlags: 16 |
| | dn: CN=sambaSID,CN=Schema,CN=Configuration,DC=X<br>changetype: ntdsSchemaAdd<br>objectClass: top<br>objectClass: attributeSchema<br>cn: sambaSID<br>instanceType: 4<br>attributeID: 1.3.6.1.4.1.7165.2.1.20<br>attributeSyntax: 2.5.5.12<br>isSingleValued: TRUE<br>showInAdvancedViewOnly: FALSE<br>adminDisplayName: sambaSID<br>adminDescription: Security ID<br>oMSyntax: 64<br>searchFlags: 1<br>lDAPDisplayName: sambaSID<br>systemOnly: FALSE<br>systemFlags: 16 |

| Operation | Description |
|---|---|
| | dn: CN=sambaUnixIdPool,CN=Schema,CN=Configuration,DC=X<br>changetype: ntdsSchemaAdd<br>objectClass: top<br>objectClass: classSchema<br>cn: sambaUnixIdPool<br>instanceType: 4<br>possSuperiors: container<br>subClassOf: top<br>governsID: 1.3.6.1.4.1.7165.1.2.2.7<br>rDNAttID: cn<br>showInAdvancedViewOnly: FALSE<br>adminDisplayName: sambaUnixIdPool<br>adminDescription: Pool for allocating UNIX uids/gids<br>sobjectClassCategory: 3<br>lDAPDisplayName: sambaUnixIdPool<br>systemOnly: FALSE<br>systemPossSuperiors: organizationalUnit<br>systemPossSuperiors: domainDNS<br>mustContain: uidNumber<br>mustContain: gidNumber<br>defaultSecurityDescriptor:<br><br>D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDS<br>DDTSW;;;SY)(A;;RPLCLORC;;;AU)<br>systemFlags: 16<br>defaultHidingValue: FALSE |
| | dn: CN=sambaIdmapEntry,CN=Schema,CN=Configuration,DC=X<br>changetype: ntdsSchemaAdd<br>objectClass: top<br>objectClass: classSchema<br>cn: sambaIdmapEntry<br>instanceType: 4<br>possSuperiors: container<br>subClassOf: top<br>governsID: 1.3.6.1.4.1.7165.1.2.2.8<br>rDNAttID: cn<br>showInAdvancedViewOnly: FALSE<br>adminDisplayName: sambaIdmapEntry<br>adminDescription: Mapping from a SID to an ID<br>objectClassCategory: 3<br>lDAPDisplayName: sambaIdmapEntry<br>systemOnly: FALSE<br>systemPossSuperiors: organizationalUnit<br>systemPossSuperiors: domainDNS<br>mustContain: sambaSID<br>mayContain: gidNumber<br>mayContain: uidNumber<br>defaultSecurityDescriptor:<br><br>D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDS<br>DDTSW;;;SY)(A;;RPLCLORC;;;AU)<br>systemFlags: 16<br>defaultHidingValue: FALSE |

| Operation | Description |
|---|---|
| | dn: CN=sambaSidEntry,CN=Schema,CN=Configuration,DC=X<br>changetype: ntdsSchemaAdd<br>objectClass: top<br>objectClass: classSchema<br>cn: sambaSidEntry<br>instanceType: 4<br>possSuperiors: container<br>subClassOf: top<br>governsID: 1.3.6.1.4.1.7165.1.2.2.9<br>rDNAttID: sambaSID<br>showInAdvancedViewOnly: FALSE<br>adminDisplayName: sambaSidEntry<br>adminDescription: Structural Class for a SID<br>objectClassCategory: 1<br>lDAPDisplayName: sambaSidEntry<br>systemOnly: FALSE<br>systemPossSuperiors: organizationalUnit<br>systemPossSuperiors: domainDNS<br>mustContain: sambaSID<br>defaultSecurityDescriptor:<br><br>D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;RPLCLORC;;;AU)<br>systemFlags: 16<br>defaultHidingValue: FALSE |
| | After a schema file is created or obtained, enter the following command at the command prompt, on one line, to read the schema file for using the user mapping functionality.<br><br>`ldifde -i -f C:\samba.ldf -s localhost:`*port* `-j . -k -c "CN=Schema,CN=Configuration,DC=X" #schemaNamingContext`<br><br>In this example, the schema file is saved as `C:\samba.ldf`. For *port*, specify the LDAP port number that was specified when ADAM was installed. The `ldifde` command exists in the system when ADAM or Active Directory is installed. To use the `ldifde` command for ADAM, choose **Start**, **All programs**, **ADAM**, and then **ADAM Tool command Prompt**. |

| Operation | Description |
|---|---|
| Setting the search limit | When you use an ADAM LDAP server, you can specify a maximum search number (number of entries returned in response to search requests from an LDAP client). The default is 1,000 entries.<br>When the number of user mapping information entries in the LDAP server exceeds the maximum number, downloading of user mapping information in the **List of RAS Information** (Batch-download) window will fail. To prevent this problem, increase the limit value in `MaxPageSize` so that the maximum number of search results does not exceed the total number of managed users and groups.<br>The following describes the procedure for increasing the limit in `MaxPageSize`. For details on the **ADAM ADSI Edit** tool and the terms used in the procedure, see the Microsoft documentation.<br>To expand the limit:<br>Use the **ADAM ADSI Edit** tool to connect to the configuration partition.<br>Expand the console tree, and then click **CN=Services**, **CN=Windows NT**, **CN=Directory Service**, and then **CN=Query-Policies**.<br>In the Details window, double-click **CN=Default Query Policy**. In the Properties window, double-click the **IDAPAdminLimits** attribute to edit the attribute value.<br>Select **MaxPageSize=1000**, and then click the **Remove** button.<br>Enter **MaxPageSize=***limit*, and then click the **Add** button.<br>For *limit*, enter the sum of the maximum number of users and the maximum number of groups, considering the range of user IDs and group IDs to be set when you set user mapping for the NAS Modular system.<br>Click **OK** twice to finish the setting. |
| Setting an index | When you store a large number of user IDs and group IDs in the LDAP server configured using ADAM, the search performance for the LDAP server might deteriorate. In such a case, set an index.<br>When you use ADAM to expand a schema, an index is set for the expanded attributes `uidNumber`, `gidNumber`, and `sambaSID`. The following describes the procedure for setting an index for `objectClass` that is the system's existing attribute. For details on the **ADAM ADSI Edit** tool and the terms used in the procedure, see the Microsoft documentation.<br>To set an index:<br>Use the **ADAM ADSI Edit** tool to connect to the schema partition.<br>Expand the console tree. In the Details window, double-click **cn=Object-Class**.<br>In the Properties window, double-click the **searchFlags** attribute to edit the attribute value.<br>The current setting is `8`. Change it to `9`.<br>If the setting has already been changed, set as follows according to the setting:<br>Odd number:<br>Use the setting without change.<br>Even number:<br>Increase the set value by one.<br>Click **OK** twice to close the dialog box. |

# Chapter 3 Performing Account Administrator Operations

This chapter describes the NAS Manager operations that an account administrator of a NAS Modular system performs to set up and manage system administrators. Account administrator privileges alone are not sufficient to operate a NAS Modular system. Before a NAS Modular system starts operation, the account administrator must set up the system administrators.

- Overview of Operations (see section 3.1)
- Logging in and Logging Out (see section 3.2)
- Window Transitions (see section 3.3)
- Basic GUI Operations (see section 3.4)
- Managing System Administrators (see section 3.5)
- Editing the Account Administrator's Personal Information (see section 3.6)

## 3.1 Overview of Operations

Before a NAS Modular system starts operation, the account administrator must set up the system administrators. Account administrator privileges alone are not sufficient to operate or manage a NAS Modular system.

The account administrator can use NAS Manager to perform the following tasks:

- Set up system administrators.

  You can register and delete system administrators and change their user information and passwords. For details, see section 3.5.

- Edit personal information.

  You can edit your own information such as the password and comment. For details, see section 3.6.

## 3.2 Logging in and Logging Out

As the account administrator of a NAS Modular system, you can log in to NAS Manager from a Web browser, and end the session by logging out. Before you begin to use the NAS Manager, the system administrator must set up the NAS Manager license. For details on license setup, see the *Storage Navigator Modular User's Guide*.

This section describes the **Login** and logout procedures.

### 3.2.1 Logging In

Figure 3.1 illustrates the **Login** window.

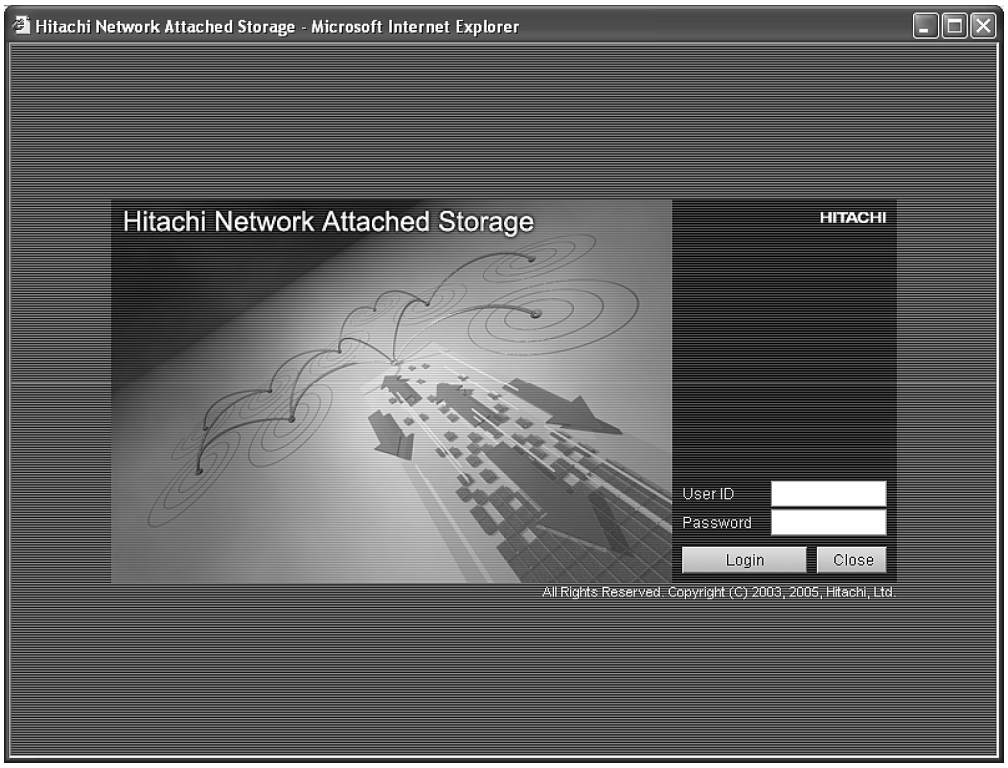



**Figure 3.1 Login (Account Administrator) Window**

To log in to NAS Manager:

a. Start your Web browser, and type the URL of the **Login** (account administrator) window:

   `https://`*`fixed-IP-address-of-mng1-of-the-NAS-Unit-for-connection`*`/admin.cgi`

   You can log in to any NAS Unit. The **Login** (account administrator) window appears.

b. Enter the required information, then click the **Login** button to display the **Main Menu** (account administrator) window.

   For window details, see section 3.3. You must specify the following information:

   – User ID

     Enter the user name of the account administrator (`nasmgr`) for the NAS Modular system.

   – Password

     Enter the password of the account administrator.

     ***Note:*** The initial password is `raid-mgr`. To prevent unauthorized access, make sure you change the password at the first login. For details on how to change the password, see section 3.6.3.

### 3.2.2 Logging Out

At the end of your NAS Manager session, be sure to log out before quitting your Web browser. The logout operations will not be performed if you directly quit your Web browser.

To log out of NAS Manager, click **Close** in the menu area. Then, quit your Web browser.

## 3.3 Window Transitions

As the account administrator, you can set and manage the system administrators and manage your own personal information from the **Main Menu** (account administrator) window. When you log in to NAS Manager as the account administrator from your Web browser, the **Main Menu** (account administrator) window appears. For details on displaying this window, see section 3.2.

The **Main Menu** (account administrator) window displays the NAS Manager function that you use for setting and managing system administrators. Clicking a button displays the window for using the function indicated by the button.

The following figure shows the **Main Menu** (account administrator) window.

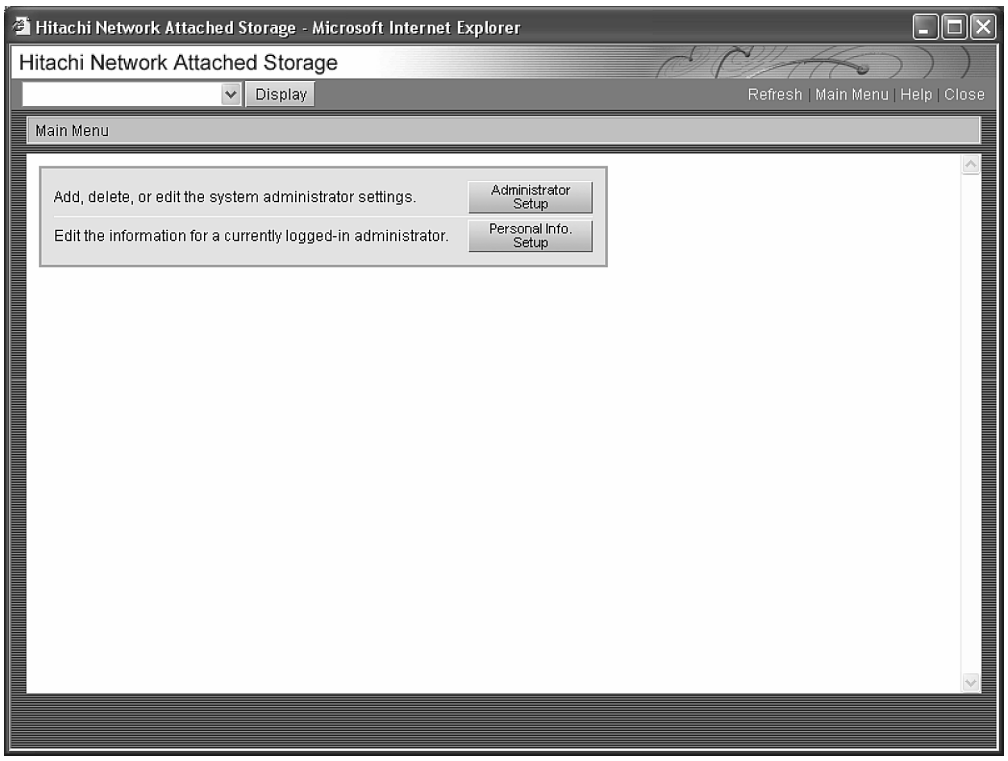



**Figure 3.2 Main Menu (Account Administrator) Window**

The following list describes the NAS Manager function that can be used from the **Main Menu** (account administrator) window:

- **Administrator Setup**

  Add and delete system administrators, and edit their user information and passwords (see section 3.5).

- **Personal Info. Setup**

  Edit the account administrator's own information (see section 3.6).

The following figure shows the window transitions after you log in to NAS Manager.

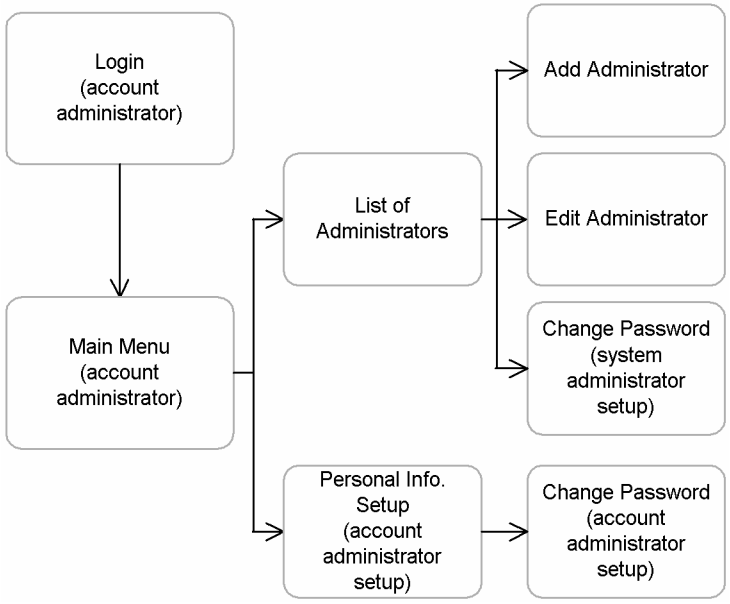



**Figure 3.3 Window Transitions for Account Administrator**

## 3.4 Basic GUI Operations

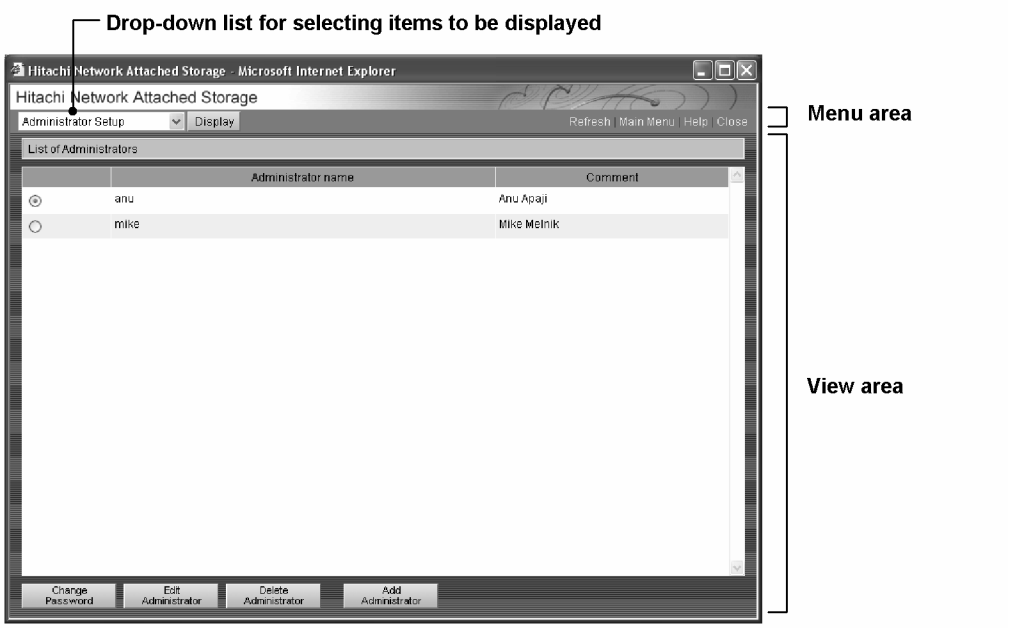
As the account administrator, you use the NAS Manager to set and manage the system administrators, and manage your own personal information. This section describes the basic operations of the NAS Manager GUI.

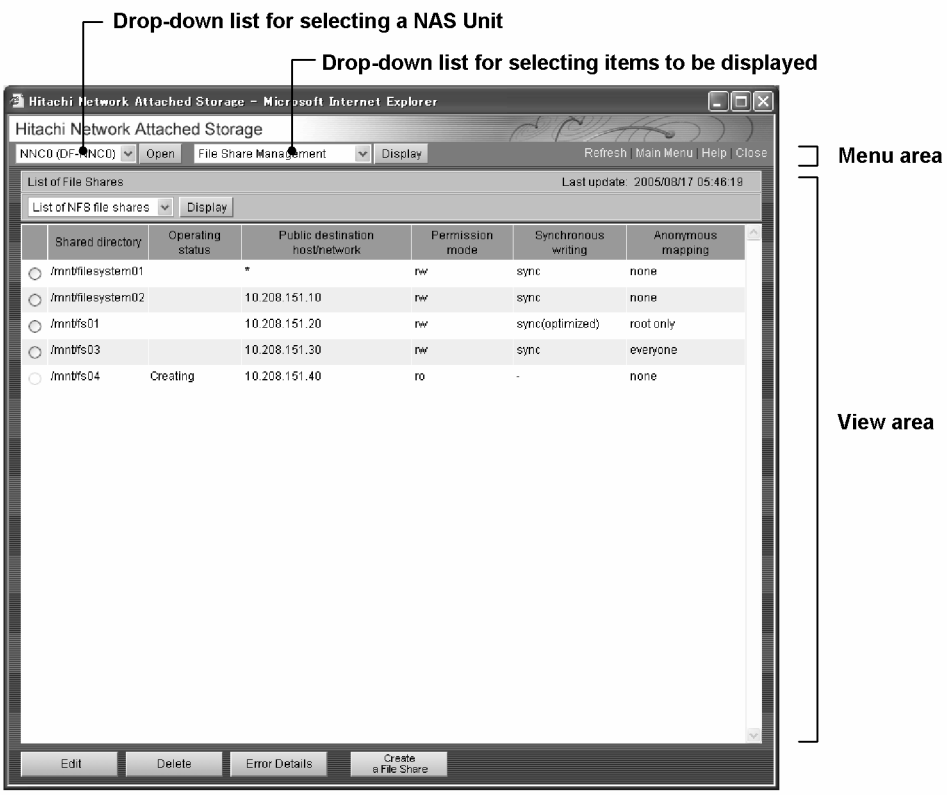
### 3.4.1 Window Layout

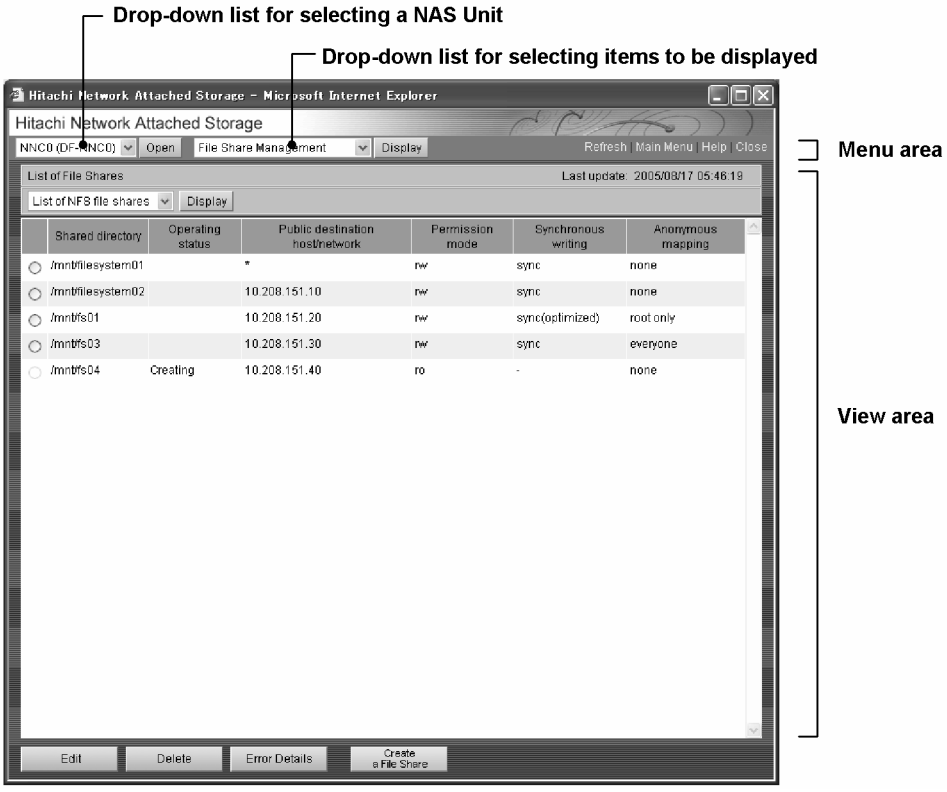
The NAS Manager consists of a menu area and view area. The menu area is common to all windows that you access, except for dialog boxes and the **Login** (account administrator) window.

***Note:*** When using a wheel mouse, do not rotate the wheel while pressing the **Shift** key. Doing so might cause the displayed window to change to another, and processing might not continue. If such an error has occurred, you must log out by clicking **Close** in the menu area, and then log in again.

If the window displayed when the error has occurred does not contain a **Close** button in the menu area, close the window by using the control menu of the web browser, and then log in again. When you log in, a window confirming the forced **Login** appears. Click the **Login** button and log in manually.


Drop-down list for selecting items to be displayed
Hitachi Network Attached Storage - Microsoft Internet Explorer
Hitachi Network Attached Storage
Administrator Setup
Display
Refresh | Main Menu | Help | Close
Menu area
List of Administrators
Administrator name
Comment
anu
Anu Apaji
mike
Mike Melnik
View area
Change Password
Edit Administrator
Delete Administrator
Add Administrator


Drop-down list for selecting a NAS Unit
Drop-down list for selecting items to be displayed
Hitachi Network Attached Storage - Microsoft Internet Explorer
Hitachi Network Attached Storage
NNC0 (DF-NNC0)
Open
File Share Management
Display
Refresh | Main Menu | Help | Close
List of File Shares
Last update: 2005/08/17 05:46:19
List of NFS file shares
Display
Shared directory
Operating status
Public destination host/network
Permission mode
Synchronous writing
Anonymous mapping
/mnt/filesystem01 * rw sync none
/mnt/filesystem02 10.208.151.10 rw sync none
/mnt/fs01 10.208.151.20 rw sync(optimized) root only
/mnt/fs03 10.208.151.30 rw sync everyone
/mnt/fs04 Creating 10.208.151.40 ro - none
Edit
Delete
Error Details
Create a File Share
Menu area
View area


Drop-down list for selecting a NAS Unit
Drop-down list for selecting items to be displayed
Hitachi Network Attached Storage - Microsoft Internet Explorer
Hitachi Network Attached Storage
NNC0 (DF-NNC0)
Open
File Share Management
Display
Refresh | Main Menu | Help | Close
List of File Shares
Last update: 2005/08/17 05:46:19
List of NFS file shares
Display
Shared directory
Operating status
Public destination host/network
Permission mode
Synchronous writing
Anonymous mapping
/mnt/filesystem01 * rw sync none
/mnt/filesystem02 10.208.151.10 rw sync none
/mnt/fs01 10.208.151.20 rw sync(optimized) root only
/mnt/fs03 10.208.151.30 rw sync everyone
/mnt/fs04 Creating 10.208.151.40 ro - none
Edit
Delete
Error Details
Create a File Share
Menu area
View area

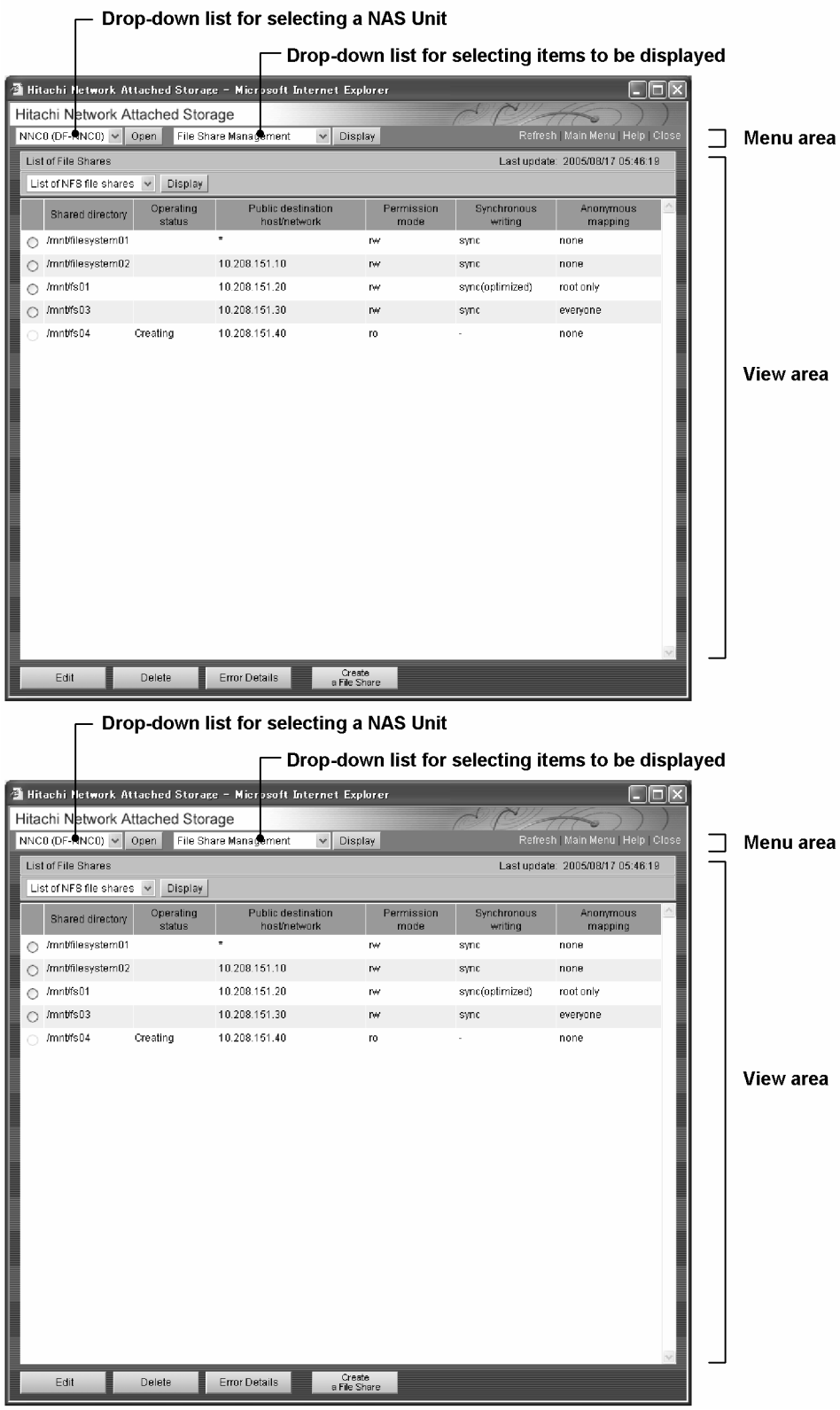



**Figure 3.4 GUI Window Layout (Account Administrator)**

The following describes how to use the components displayed in the menu area:

- **Drop-down list**

  Select the item you want to display in the view area.

  You can select the same item as in the **Main Menu** (account administrator) window. For details on selectable items, see section 3.3.

- **Display**

  Click this button to display the item you selected.

- **Refresh**

  Click this button to refresh the information displayed in a window used to view a list or status. Although this **Refresh** button also appears in windows used for purposes other than viewing information, clicking the button in such windows does not refresh any information.

- **Main Menu**

  Click to display the **Main Menu** (account administrator) window.

- **Help**

  Click to display the HTML manual.

- **Close**

  Click to close the current window by logging out.

### 3.4.2 Navigating the GUI

The following describes the basic GUI operations in NAS Manager:

- Selecting an item to be displayed

  To select the same menu as for the **Main Menu** (account administrator) window from any other window, select the menu from the drop-down list for selecting the item to be displayed, then click the **Display** button. For details about the menus you can select, see section 3.3.

- Refreshing information in a window used to view a list or status

  Click **Refresh** in the menu area to refresh the information displayed in a window used to view a list or status. Although this **Refresh** button also appears in other windows, clicking the button in such windows does not refresh any information.

- Displaying the HTML manual

  Click **Help** in the menu area to display the HTML manual.

- Displaying the **Main Menu** (account administrator) window

  Click **Main Menu** in the menu area to display the **Main Menu** (account administrator) window.

- Logging out from NAS Manager

  Click **Close** in the menu area to log out of NAS Manager.

Note the following points when you use the NAS Manager.

- To end your NAS Manager session, you must always log out by clicking **Close** in the menu area.

  The logout operations will not be performed if you directly quit your Web browser.

- You will be forced to log out if you do not access the program for 30 minutes or more while logged in.

## 3.5 Managing System Administrators

You can use the NAS Manager to register or delete system administrators and to manage information about them, such as allocation of management-target NAS Units, user names, or comments.

This section describes how to view a list of system administrators, add or delete system administrators, and change their user information and passwords.

### 3.5.1 Viewing a List of System Administrators

In the **List of Administrators** window, shown below, you can view a list of currently registered system administrators.

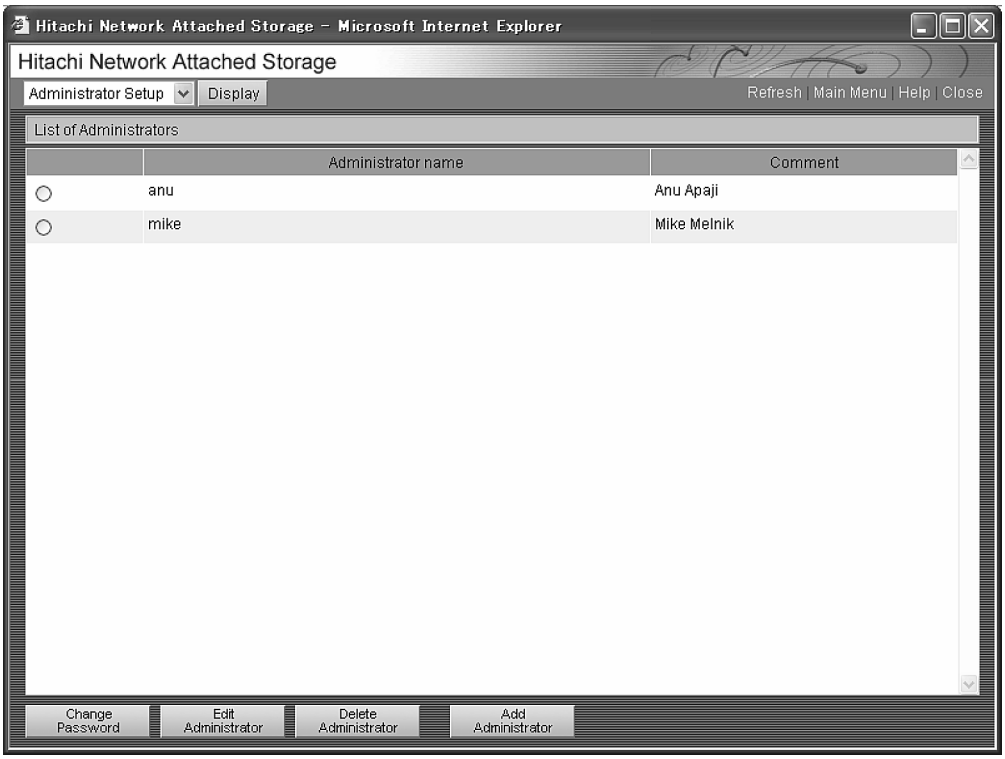



**Figure 3.5 List of Administrators Window**

Following is a description of the information that is displayed in the **List of Administrators** window:

- **Administrator name** the system administrator's user name.
- **Comment** notes entered by the system administrator. Nothing is displayed unless a comment has been set.

To view a list of system administrators, click the **Administrator Setup** button in the **Main Menu** (account administrator) window. The **List of Administrators** window appears.

### 3.5.2 Registering System Administrators

The account administrator can register up to 16 system administrators.

To register a system administrator:

1. In the **Main Menu** (account administrator) window, click the **Administrator Setup** button.

   The **List of Administrators** window appears. For window details, see section 3.5.1.

2. Click the **Add Administrator** button.

   The **Add Administrator** window displays.

3. Enter the required information, as described in Table 3.1, then click the **Add** button.

   The system administrator is added, and the **List of Administrators** window re-displays.

**Table 3.1 Add Administrator Window Contents**

| Item | Description |
|---|---|
| **Administrator name** | Enter the user name of the system administrator you are registering.<br>Specify a maximum of 16 characters.<br>The first character must be an alphabetic character.<br>You can use any alphanumeric character, hyphen (-), or underscore (_) after the first character.<br>Specify a unique user name. This user name must differ from the name of the account administrator. |
| **Comment** | Enter a comment for the system administrator you are registering.<br>Enter a maximum of 32 characters.<br>You can use any alphanumeric character, number sign (#), percent sign (%), ampersand (&), apostrophe ('), left parenthesis ( (), right parenthesis ()), asterisk (*), plus sign (+), hyphen (-), period (.), forward slash (/), semicolon (;), left angle bracket (<), right angle bracket (>), question mark (?), at mark (@), left bracket ( [), right bracket (]), circumflex (^), underscore (_), left brace ({), vertical bar (\|), right brace (}), and tilde (~). You can also specify spaces but spaces cannot be specified at the beginning or at the end of the character string.<br>This item is optional. |
| **Password** | Enter the password of the system administrator you are registering.<br>Specify a maximum of 8 characters.<br>You can use any alphanumeric character, exclamation mark (!), quote ("), number sign (#), dollar sign ($), percent sign (%), ampersand (&), apostrophe ('), left parenthesis ( (), right parenthesis ()), asterisk (*), plus sign (+), comma (,) hyphen (-), period (.), forward slash (/), colon (:), semicolon (;), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at |

| Item | Description |
|---|---|
| | mark (@), left bracket ( [ ), backslash ( \ ), right bracket ( ] ), circumflex ( ^ ), underscore ( _ ), grave accent ( ` ), left brace ( { ), vertical bar ( \| ), right brace ( } ), and tilde ( ~ ). |
| **Re-enter password** | Re-enter the system-administrator password that you specified in **Password**. |
| **Managed NNCs** | NAS Units managed by the system administrator are displayed with their check boxes selected. Use check boxes to select the NAS Units managed by the system administrator.<br>The check boxes are displayed one above the other for NAS Unit combinations that configure a cluster. NAS Units must be selected in units of clusters. (Clusters have check boxes displayed one above the other. |

### 3.5.3 Deleting System Administrators

To delete a system administrator:

1. In the **Main Menu** (account administrator) window, click the **Administrator Setup** button.

   The **List of Administrators** window displays. For window details, see section 3.5.1.

2. Use a radio button to select the system administrator you want to delete, then click the **Delete Administrator** button.

   A dialog box displays, confirming you that you really want to delete the system administrator.

3. Click the **OK** button.

   The system administrator is deleted.

### 3.5.4 Editing User Information for System Administrators

You can change the user information (comments and allocation of management-target NAS Units) for all the registered system administrators.

To change the user information for a system administrator:

1. In the **Main Menu** (account administrator) window, click the **Administrator Setup** button.

   The **List of Administrators** window displays. For window details, see section 3.5.1.

2. Use a radio button to select the system administrator whose user information you want to edit, then click the **Edit Administrator** button.

   The **Edit Administrator** window displays.

3. Edit the user information for the system administrator, then click the **OK** button:

   - **Comment** Enter a comment for the system administrator.
   - **Managed NNCs** NAS Units managed by the system administrator are displayed with their check boxes selected. The NAS Units must be selected in units of clusters. (Clusters have check boxes displayed one above the other.

   The user information for the system administrator changes, and the **List of Administrators** window reappears.

### 3.5.5 Changing the System Administrator Password

As the account administrator, you can change the password for all the registered system administrators. For example, if a system administrator cannot remember his or her password, you can change it without knowing the password that is currently set.

To change the password of a system administrator:

1. In the **Main Menu** (account administrator) window, click the **Administrator Setup** button.

   The **List of Administrators** window displays. For window details, see section 3.5.1.

2. Use a radio button to select the system administrator whose password you want to change, then click the **Change Password** button.

   The **Change Password** (system administrator setup) window displays.

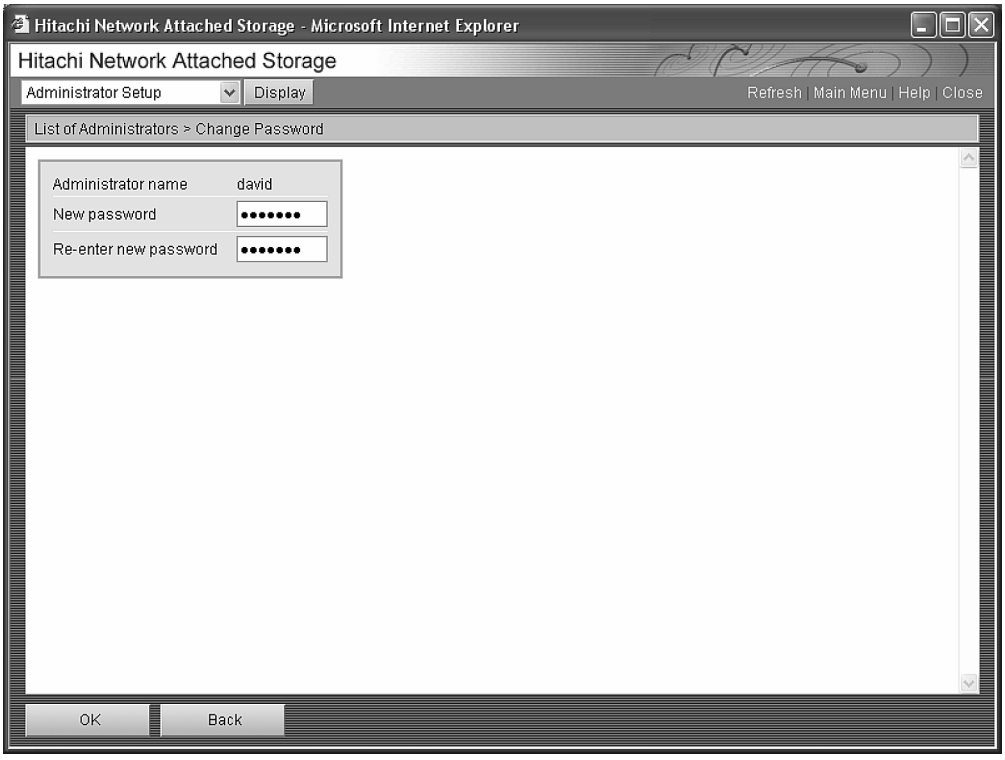



**Figure 3.6 Change Password (system administrator setup) Window**

3. Enter the required information, then click the **OK** button.

   The password of the system administrator changes, and the **List of Administrators** window reappears.

   Information to be specified in the **Change Password** (system administrator setup) window includes the following:

   – **New Password**

     Enter the new password of the system administrator.

– **Re-enter New Password**

  Re-enter the new password that you specified in **New password**.

## 3.6 Editing the Account Administrator's Personal Information

NAS Manager manages your user name, comment, and password. For increased security, you should change the password regularly.

This section describes how to reference and edit your own user information and change the password.

### 3.6.1 Viewing the Account Administrator's User Information

While logged in as the account administrator, you can view your own user information in the **Personal Info. Setup** (account administrator setup) window.

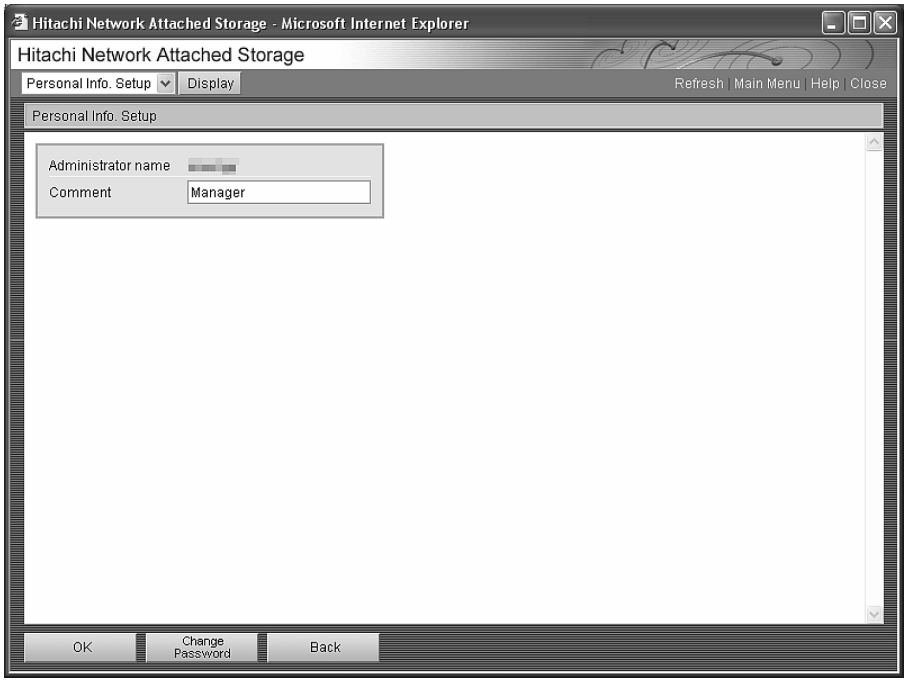



**Figure 3.7 Personal Info. Setup (Account Administrator Setup) Window**

Following is a description of the user information that is displayed in the **Personal Info. Setup** (account administrator setup) window:

- **Administrator name**

  User name of the account administrator.

- **Comment**

  Comment of the account administrator. Nothing is displayed unless a comment has been set.

To view your own user information, click the **Personal Info. Setup** button in the **Main Menu** (account administrator) window. The **Personal Info. Setup** (account administrator setup) window appears.

### 3.6.2 Editing the Account Administrator's User Information

While logged in as the account administrator, you can change your user information.

To change the account administrator's user information:

1. In the **Main Menu** (account administrator) window, click the **Personal Info. Setup** button.

   The **Personal Info. Setup** (account administrator setup) window displays. For window details, see section 3.6.1.

2. Edit the user information of the account administrator.

   You can also edit **Comment** as the user information of the account administrator.

   Enter a maximum of 32 characters.

   You can use any alphanumeric character, number sign (#), percent sign (%), ampersand (&), apostrophe ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), hyphen (-), period (.), forward slash (/), semicolon (;), left angle bracket (<), right angle bracket (>), question mark (?), at mark (@), left bracket ([), right bracket (]), circumflex (^), underscore (_), left brace ({), vertical bar (|), right brace (}), and tilde (~). You can also specify spaces, but spaces cannot be specified at the beginning or at the end of the character string. This item is optional.

3. Click the **OK** button.

   The user information for the account administrator changes, and the **Main Menu** (account administrator) window re-displays.

### 3.6.3 Changing the Account Administrator's Password

While logged in as the account administrator, you can change your own password. The new password will take effect at the next **Login** on all NAS Units in the NAS Modular subsystem.

To change the account administrator's password:

1. In the **Main Menu** (account administrator) window, click the **Personal Info. Setup** button.

   The **Personal Info. Setup** (account administrator setup) window displays. For window details, see section 3.6.1.

2. Click the **Change Password** button.

   The **Change Password** (account administrator setup) window displays.

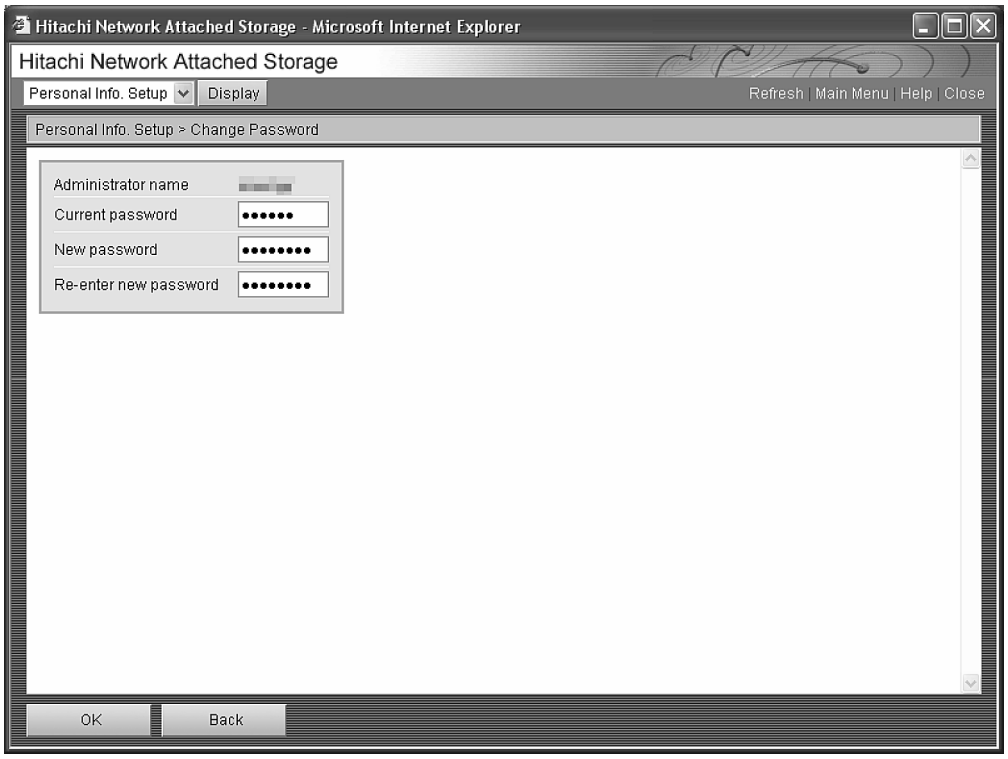



**Figure 3.8 Change Password (Account Administrator Setup) Window**

3. Enter the required information, as described in Table 3.2, and then click the **OK** button.

   The password of the account administrator changes, and the **Personal Info. Setup** (account administrator setup) window re-displays.

**Table 3.2 Change Password (Account Administrator Setup) Window Information**

| Item | Description |
|---|---|
| **Current password** | Enter your password you are currently using. |
| **New password** | Enter your new password. |

| Item | Description |
|---|---|
| | Be careful not to forget the new password you enter.<br>Specify a maximum of 8 characters.<br>You can use any alphanumeric character, exclamation mark ( ! ), quote ( " ), number sign (#), dollar sign ($), percent sign (%), ampersand (&), apostrophe ( ' ), left parenthesis ( ( ), right parenthesis ( ) ), asterisk ( * ), plus sign (+), comma ( , ) hyphen (−), period ( . ), forward slash ( / ), colon ( : ), semicolon ( ; ), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left bracket ( [ ), backslash ( \ ), right bracket ( ] ), circumflex ( ^ ), underscore (_), grave accent ( ` ), left brace ( { ), vertical bar ( \| ), right brace ( } ), and tilde (~). |
| **Re-enter new password** | Re-enter the new password that you specified in **New password**. |

# Chapter 4 Performing System Administrator Operations

This chapter describes how a system administrator uses the NAS Manager GUI to manage a file system service or information about any errors that occur in a NAS Modular system. NAS Manager operations enable users to access file system services that use a disk array.

- Overview of Operations (see section 4.1)
- Logging in and Logging out (see section 4.2)
- Window Transitions (see section 4.3)
- Information Required Before Using the GUI (see section 4.4)
- Managing Clusters (see section 4.5)
- Managing Services (see section 4.6)
- System Setup (see section 4.7)
- Preventing Viruses (see section 4.8)
- Managing User Information (see section 4.9)
- Managing File Systems (see section 4.10)
- Managing File Shares (see section 4.11)
- Managing Quotas (see section 4.12)
- Managing Error Information (see section 4.13)
- Managing Core Files (see section 4.14)
- Managing Programs (see section 4.15)
- Modifying a System Administrator's Personal Information (see section 4.16)
- Saving NAS System LUs (see section 4.17)

## 4.1 Overview of Operations

Before preparing to run the system, the system administrator must be registered in the NAS Modular system. A system administrator who is not registered in the NAS Modular system cannot log in to NAS Manager.

The account administrator manages system administrators. For details on how the account administrator registers system administrators, see section 3.5.

### 4.1.1 Preparing to Run the System

Before running the NAS Modular system, you (the system administrator) must first set the information required to operate the system, including the cluster configuration, network information, and system information. After setting this information, you can then configure the file system and set up file shares. You are then ready to run the NAS Modular system.

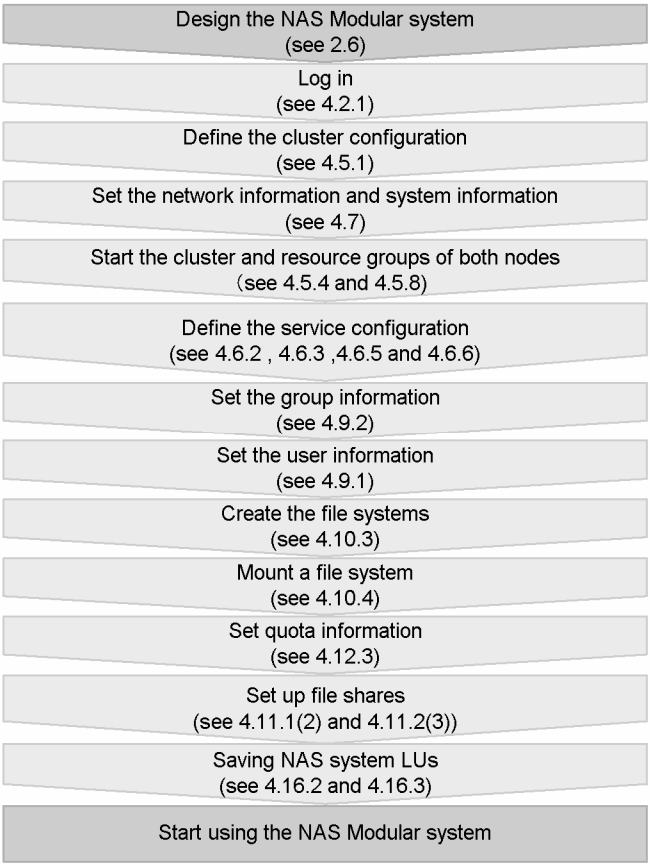



**Figure 4.1 NAS Manager Setup Procedure**

To use virus scanning when you start operating the NAS Modular system, the virus scan function must be started before a file share is created. For more information, see section 4.8.7.

Check whether or not the resource group is partially blocked when the NAS Modular system operation is started.

### 4.1.2 Completing Post-Operation Tasks

The system administrator must manage information about the interrelationships among device files, file systems and file shares to manage use of the NAS Modular system. After starting the NAS Modular system, the system administrator may need to complete the tasks that are outlined in Table 4.1.

**Table 4.1 Post-Operation Tasks**

| Task | Details |
|---|---|
| Usual system operation | ▪ Monitor the status of clusters and resource groups.<br>▪ Monitor file system usage.<br>▪ Monitor the status of the services.<br>▪ Monitor error information such as messages, log files, and core files.<br>▪ Delete old error information when no longer needed.<br>▪ Check information about the programs installed in the NAS Units.<br>▪ Set quota information.<br>▪ Monitor the scan server status (optional). |
| Changing settings | ▪ Change a cluster name, node name, service IP address or NNC name.<br>▪ Edit the `hosts` file as required after changing a service IP address or a fixed IP address.<br>▪ Perform failover or failback as instructed by your HDS representative.<br>▪ Notify your HDS representative at execution and completion of failover or failback.<br>▪ Start, stop, and restart services.<br>▪ Change a service configuration.<br>▪ Change network information such as server information or the fixed IP address of an NIC.<br>▪ Add or delete routing information.<br>▪ Change the time for synchronizing the NAS Modular system time with the time of the NTP server.<br>▪ Change the type and severity level of messages output to syslog files, or change the syslog output destination.<br>▪ Change the log file size and number of files to be kept.<br>▪ Change the core file storage period.<br>▪ Directly **Edit System File**s by using the NAS Manager.<br>▪ Upgrade a program.<br>▪ Change the system administrator's own user information or password.<br>▪ Add, edit, or delete SNMP information.<br>▪ Add, change, or delete the scan server.<br>▪ Start and stop the virus scan function.<br>▪ Change the settings for scanning. |

| Task | Details |
|---|---|
| Changing settings based on user requests | ▪ Configure or delete a file system, or expand its capacity.<br>▪ Unmount a file system before deleting it.<br>▪ Mount a file system when adding it.<br>▪ Create, change, or delete file shares.<br>▪ Add, change, or delete user information or group information.<br>▪ Add, change, or delete settings related to quota information. |
| Regular maintenance tasks | ▪ Check the operation status of the provided services.<br>▪ Perform failover or failback as instructed by your HDS representative.<br>▪ Notify your HDS representative at execution and completion of failover or failback |
| Failure procedures | ▪ Check the error message displayed in the window that shows the results of processing.<br>▪ Check the system messages.<br>▪ Use SNMP notification to check error information.<br>▪ Check the Web server for any problems.<br>▪ If unable to resolve the problem, download error information from the NAS Manager and send it to your HDS representative.<br>▪ Make sure that there are no GUI operation mistakes and run the operation again.<br>▪ Check the actions to be taken for each system message, and resolve the problem.<br>▪ Check error information in the **Browse Cluster Status** window, and resolve the problem.<br>▪ Perform manual failover or failback.<br>▪ Replace the NAS Manager. |

### 4.1.3 Reviewing Critical Operations Notes

- Do not use commands while the GUI is being used to perform operations on the NAS Modular system.
- Attempts by multiple administrators to concurrently set or change system configuration information within the same node and cluster will fail. Therefore, in systems where multiple system administrators are registered in a cluster, make sure that only one system administrator is authorized to set and change such system configuration information.
- When you change setting information for the DNS server after starting a NAS Modular system operation, you must restart the NFS service after the change.
- When changes are made in the NAS Modular system configuration, you need to save the NAS system LUs (NAS OS LUs and NAS Cluster Management LU). For details on the operation that requires saving the NAS system LUs, see section 4.17.1. If failover occurs, information on the failed-over resource group will be unable to be set or changed. The service of the failed-over resource group will also be unable to start.
- When you use an NFS share, after you start NAS Modular system operations, do not change an environment where host names can be resolved (that is, an environment where an IP address and a host name is registered in the hosts file for a NAS Modular system, NIS server, or DNS server and a host name can be converted into an IP address). If the environment where host names can be resolved changes after an NFS share is set, the NFS share that is set might be deleted.
- When operating a NAS Modular system with a policy that creates at least one other NFS share for a directory that is at a higher level or lower level than an NFS-shared directory, the system administrator must ask the administrators of client machines to mount the NFS-shared directory itself.

  If one of the following events occurs or the following operation is performed, you will not be able to delete or rename the subdirectory of an NFS-shared directory:

  - When an NFS client has mounted a subdirectory of a shared directory, the client machine goes down or is stopped without unmounting the subdirectory
  - When an NFS client has mounted a subdirectory of a shared directory, a failover or failback occurs, and then an NFS client unmounts the subdirectory from the node on which the subdirectory was not originally mounted.

  In a such case, the system administrator must take action as described in 2.8.1.
- We recommend that you create a new NFS share in a directory that is not a subdirectory of the existing NFS share directory.

  If you mount a subdirectory of the NFS share directory from an NFS client and then unmount that subdirectory, you might be unable to delete or rename that subdirectory from the NFS client that is mounting the upper directory of that subdirectory. If this problem occurs, correct it by editing the NFS share information as follows:

  a. In the **Main Menu** window, click the **File Share Management** button.
  b. In the **List of File Shares** window, select the target NFS share, and then click the **Edit** button.

     For details on the **List of File Shares** window, see section 4.11.1.

c. In the **Edit NFS File Share** window, click the **OK** button without editing the information about the NFS share.

For details on the **Edit NFS File Share** window, see section 4.11.4.

- In an environment where host names can be resolved, note the following to register or delete a host name:
  - When creating an NFS share for a given host, make sure that you first register the host name.
  - When you use a netgroup, an IP network, or a wildcard character to create an NFS share, use the same name resolution service (conversion from an IP address to a host name, or conversion from a host name to an IP address) for the host name of the NFS client from which a target file system is mounted.
  - When deleting a host name used in an NFS share for a given host, first delete the corresponding NFS share, then delete the host name.
  - When deleting a host name used in an NFS share for no particular host, first unmount the corresponding file system from the NFS client, then delete the host name.
- A file system, an NFS service, a CIFS service, or a service IP address becomes available and can be managed by NAS Manager after the resource group status is displayed as `Online / No error` in the **Resource group status** in the **Browse Cluster Status** (Resource Group Status) window. Since the resource group starts after the cluster runs normally, the resource group is displayed as `Online-Pending` immediately after the cluster status is displayed as `ACTIVE` in the **Cluster status** in the **Browse Cluster Status** (Cluster / Node Status) window. Therefore, a file system, an NFS service, a CIFS service, or a service IP address cannot be used. Before using a file system, an NFS service, a CIFS service, or a service IP address, confirm that the resource group status is `Online / No error`. For details on how to view the resource group status, see section 4.5.7
- The password set by a system administrator when user information is registered should be used only temporarily. For all the users added in the Add User window or the **Batch Operation** window, the system administrator must inform such users that they should change their password respectively. For details on changing the password for each user, see section 7.7.
- When starting a resource group, the NAS Modular system blocks the resource in which an error is detected, and uses other normal resources to configure the resource group. When a resource group is *partially blocked*, some services in the node will be stopped but the remaining services will be provided. In such a case, the **Browse Cluster Status** (Resource Group States) window displays `Online / No error`, and the error information about the resource group cannot be checked in that window.

  A partial blockage of a resource group may occur at the following times:
  - When a NAS Modular system operation starts
  - When a failover or a failback occurs
  - When a resource group restarts

When the operations listed above are performed, or the **Browse Cluster Status** (Resource Group States) window displays `Online / No error` even though you cannot access the file system, in the **List of RAS Information** (List of Messages) window of the NAS Manager you need to check the system messages to see whether a partial blockage occurred in the resource group. For details on how to check the system messages, see section 9.2.3.

The system administrator must check whether the following message ID is output as a system message:

- `KAQG72006-E`

Depending on the resource type, the resources that use the blocked resource may also be blocked. For example, when a logical volume is blocked, the file system created in that logical volume is also blocked. In such a case, the `KAQG72006-E` message will be output for each blocked resource.

- In a NAS Modular system, when the NAS OS LU remaining space or number of remaining i-nodes runs low, an error message will be output as a system message. The NAS OS LU remaining space and number of remaining i-nodes are checked every five minutes. Messages output once will not be output again for another eight hours.

  For details about how to view and download system messages, see section 4.13. Also, if SNMP trap notification is being used, SNMP trap notifications are issued. For more details about SNMP trap notification, see section 4.7.11.

  The system administrator needs to check if any system messages output have one of the following IDs, and act accordingly:

  - `KAQM09046-E` (output when NAS OS LU remaining space is less than 300 MB)
  - `KAQM09047-E` (output when NAS OS LU remaining space is less than 5 MB)
  - `KAQM09048-E` (output when fewer than 10,000 NAS OS LU i-nodes remain)
  - `KAQM09049-E` (output when fewer than 2,000 NAS OS LU i-nodes remain)

  Depending on the message countermeasures, you may need to delete any unnecessary log files or core files, or contact your HDS representative. For more details about deleting unnecessary log files or core files, see section 4.13.

- An error might occur if you perform operations such as stopping a cluster or node, changing the execution node of the resource group, or unmounting a file system while one of the following commands is being used. Wait until the command has finished, then perform the operation:
  - `horc_pvol_freeze` command (for NAS Backup Restore)
  - `horc_pvol_unfreeze` command (for NAS Backup Restore)
  - `syncadd` command (for NAS Sync Image)
  - `syncexpand` command (for NAS Sync Image)
- After following maintenance personnel instructions to use the NAS Manager GUI to stop a cluster, even if `INACTIVE` is displayed for **Node status** in the **Browse Cluster Status** (Cluster / Node Status) window, `ACTIVE` might be displayed in the NNC status that the maintenance personnel can check immediately after they restart the NAS OS. If this happens, either ask maintenance personnel to restart the NAS OS, or restart and then stop the cluster.

## 4.2 Logging In and Logging Out

By logging in to NAS Manager from a Web browser, you can manage each NAS Manager service. End your NAS Manager session by logging out from each window.

***Note:*** You can log in to, and manage, a NAS Unit only if the account administrator has given you those management privileges.

Before you begin using the NAS Manager, your HDS representative must set up the NAS Manager license. If the **Login** window does not appear, contact your HDS representative. For details on license setup, see the *Storage Navigator Modular User's Guide*.

### 4.2.1 Logging In

The system administrator can log in by using a Web browser to display the **Login** window of the selected NAS Unit to be connected.




**Figure 4.2 Login Window**

To log in to NAS Manager:

1. Start your Web browser, and type the URL of the **Login** window for the NAS Unit to which you want to connect:

   `https://`*`fixed-IP-address-of-mng1-of-the-NAS-Unit-for-connection`*`/admin.cgi`

   The **Login** window displays.

2. Enter the required information, then click the **Login** button.
   - If the specified user name is already in use:

     A window confirming the forced **Login** appears. A *forced **Login*** indicates that you previously quit NAS Manager without logging out. Check the name of the currently logged-in user. If you click the **Login** button, the system uses a forced **Login** to log you in and there will be two system administrators logged in under the same accounts.
   - If another system administrator is already logged in:

     A window confirming the forced **Login** appears. Check the name of the currently logged-in user. If you click the **Login** button, the system uses a forced **Login** to log you in. If multiple system administrators enter different settings for the same item, the most recent setting will be applied.

     If another system administrator has already logged in from a program in the HiCommand series, a window confirming the forced **Login** will not be displayed.
   - If you log in to a NAS Unit for which no cluster configuration is defined:

When you log in to NAS Manager, a dialog box prompting you to define the cluster configuration appears. For details on how to define a cluster configuration, see section 4.5.1.

– If you log in to a NAS Unit for which a cluster configuration is defined:

  You are logged in to NAS Manager, and the **Main Menu** window for the NAS Unit to which you are connected appears. For window details, see section 4.3.

Following is the information that you must specify in the **Login** (account administrator) window:

– User ID

  Enter the user name of the system administrator for the NAS Modular system.

– Password

  Enter the password of the system administrator.

### 4.2.2 Logging Out

At the end of your NAS Manager session, be sure to log out before quitting your Web browser. The logout operations are not performed if you directly quit your Web browser.

To log out of NAS Manager, click **Close** in the menu area. You are logged out from the NAS Unit to which you are connected, and your Web browser closes. If you have active windows for multiple NAS Units, click **Close** in the menu area in every window.

### 4.2.3 Notes on Login and Logout

Note the following when using GUI to log in to, or log out from, NAS Manager:

- To end your NAS Manager session, you must always log out by clicking Close in the menu area.

  The logout operation is not performed if you quit your Web browser immediately following the logout.

- During a **Login** session, you will be forced to log out if you do not access the program for more than 30 minutes at a time.

## 4.3 Window Transitions

You can access all NAS Manager functions from the **Main Menu** window, depicted below. This window appears when you log in from a Web browser to a NAS Unit that is defined in a cluster. If no cluster configuration is defined for the NAS Unit, a dialog box prompting you to define the cluster configuration appears instead. In this case, you cannot access any NAS Manager function until you define the cluster configuration. For details on displaying the **Main Menu** window, see section 4.2.1.

The **Main Menu** window displays all the functions provided by NAS Manager. Clicking a button displays the window for using the function indicated by the button. Before you use the function provided by the optional programs you have installed, make sure that licenses are set for them. For details on license setup, see the *Storage Navigator Modular User's Guide*.

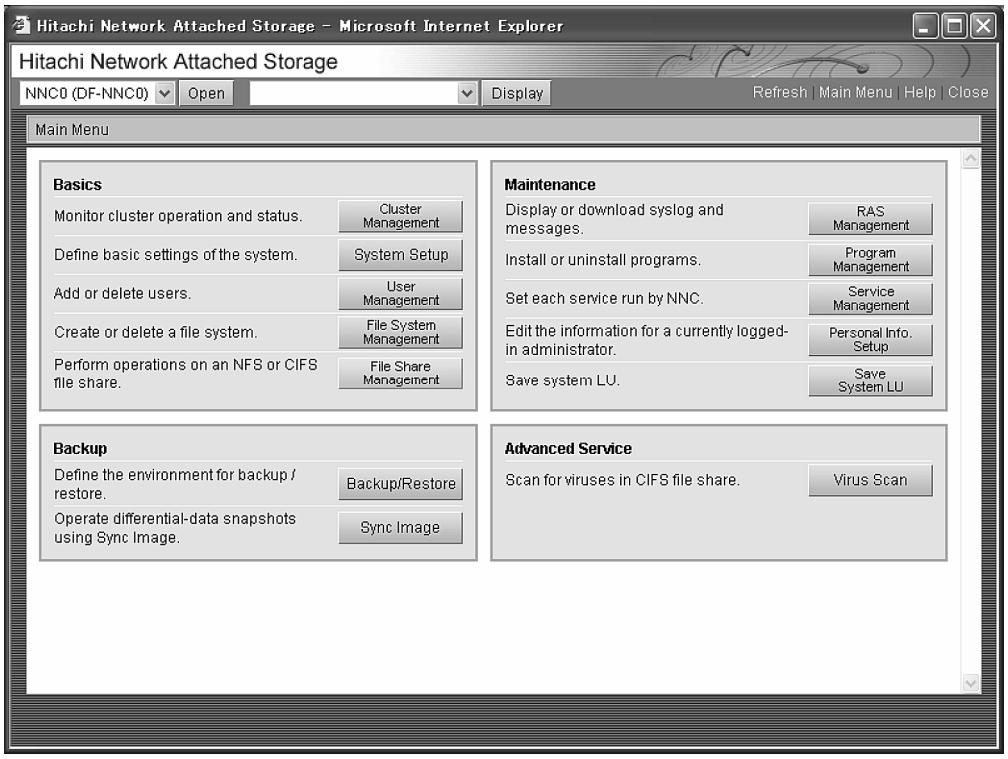



**Figure 4.3 Main Menu Window**

The NAS Manager functions that are available from the **Main Menu** window are explained in Table 4.2. They are classified into the following categories: **Basics**, **Maintenance**, **Backup** (NAS Backup Restore and NAS Sync Image), and **Advanced Service**.

**Table 4.2 Available NAS Manager Functions (Main Menu window)**

| Basic Functions | | |
|---|---|---|
| **Item** | **Description** | **See:** |
| **Cluster Management** | Manage the cluster configuration of NAS Units and resource groups, and control failover execution. | 4.5 |
| **System Setup** | Define the network information and system information for running the NAS Modular system. | 4.7 |
| **User Management** | Manage users who use the NFS or CIFS. | 4.9 |
| **File System Management** | Manage the file systems used in the NAS Modular system. | 4.10 |
| **File Share Management** | Manage file shares based on NFS or CIFS. | 4.11 |
| **Maintenance Functions** | | |

| Basic Functions | | |
|---|---|---|
| **Item** | **Description** | **See:** |
| **RAS Management** | Manage error information such as error messages, syslog files, and core files. | 4.13 |
| **Program Management** | Manage programs running on the NAS Unit: for example, NAS Manager or Backup Restore, Sync Image or Virus Scan modules. | 4.15 |
| **Service Management** | Manage the services provided by the NAS Modular system. | 4.6 |
| **Personal Info. Setup**<br>See ***Note*** | Edit the logged-on system administrator's own information. | 4.16 |
| **Save System LU** | Save the NAS OS LUs and NAS Cluster Management LU that are used by the **Login** NAS Unit. | 4.17 |
| **Backup Functions** | | |
| **Backup/Restore** | Copy the data shared in the disk array to tape device, or restore the copied data in a tape device to the disk array. This is functionality of the optional program NAS Backup Restore. | *Hitachi AMS/WMS NAS Backup Restore User's Guide* |
| **Sync Image** | Create a differential-data snap shot for a file system. This is functionality of the optional program NAS Sync Image. | *Hitachi AMS/WMS NAS Sync Image User's Guide* |
| **Advanced Service Function** | | |
| **Virus Scan** | Set up information about virus scans. | 4.8 |

### 4.3.1 Window Transitions for Each Function

This section explains the window transitions for each NAS Manager function.

#### 4.3.1.1 Cluster Management

The following figure shows the window transitions for cluster management.

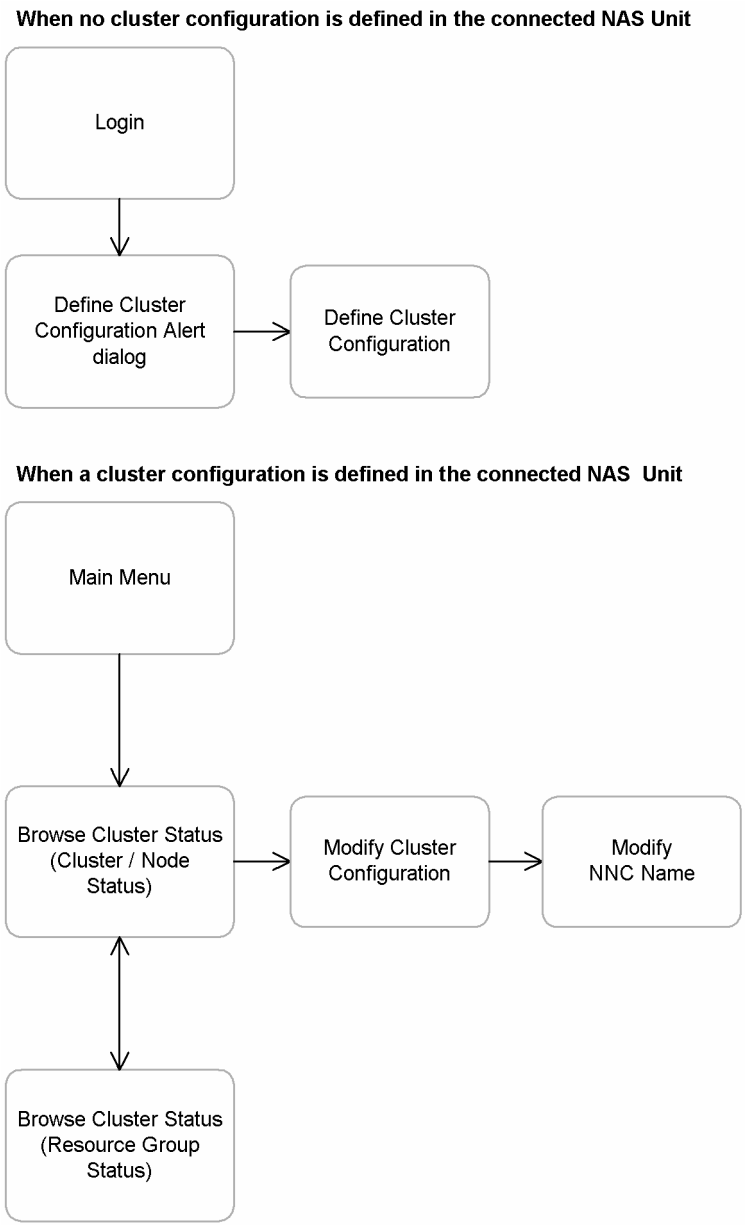



**Figure 4.4 Window Transitions for Cluster Management**

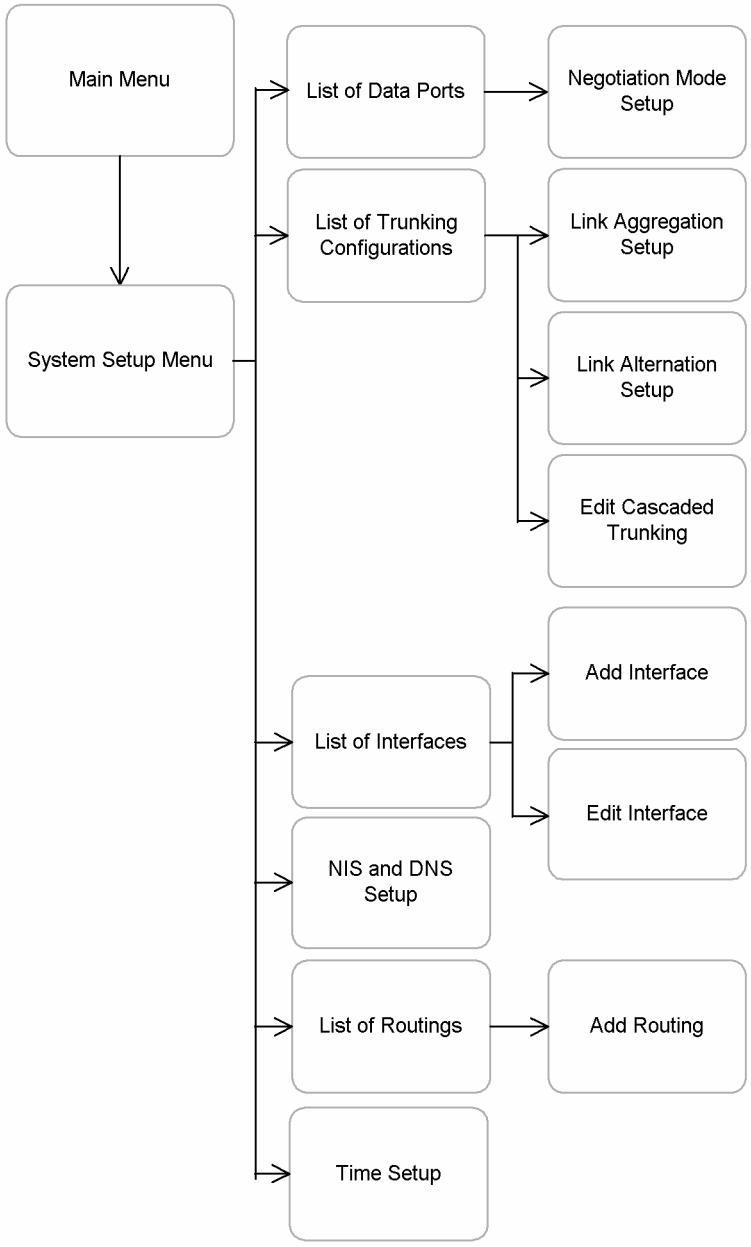



**Figure 4.5 Window Transitions for System Setup (continued on next page)**

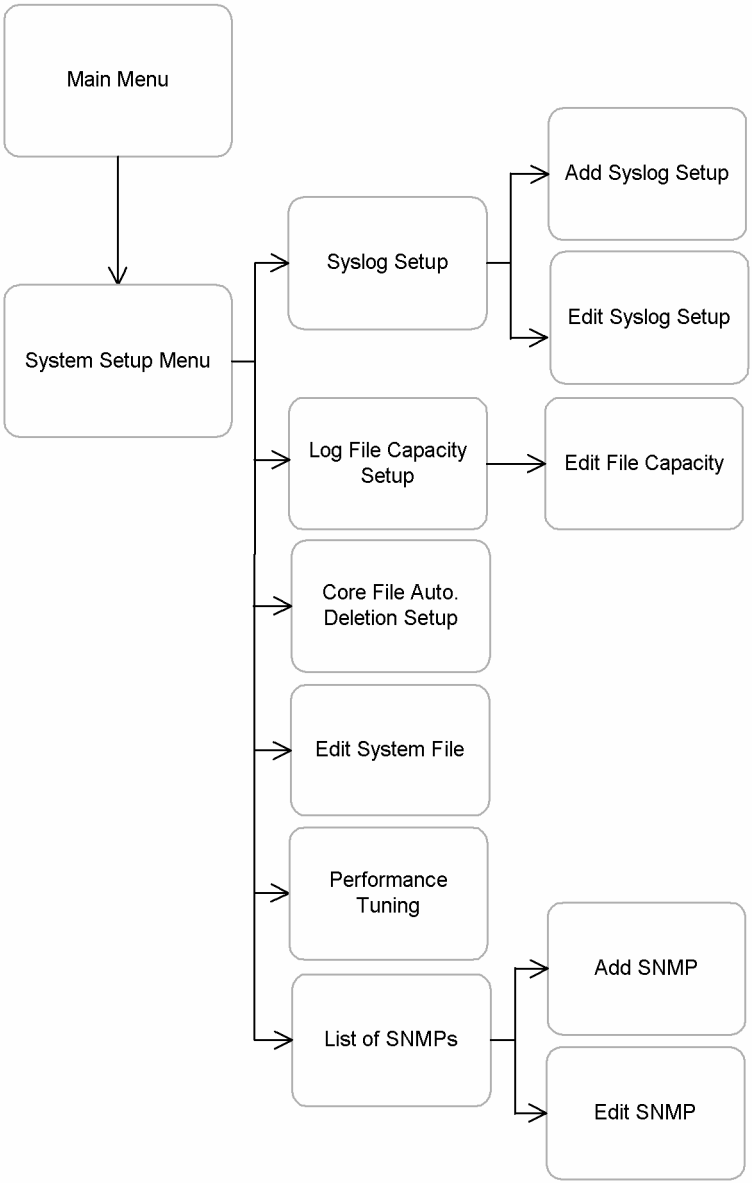



**Figure 4.4 Window Transitions for System Setup (continued)**

#### 4.3.1.2 User Management

The following figure shows the window transitions for user management.

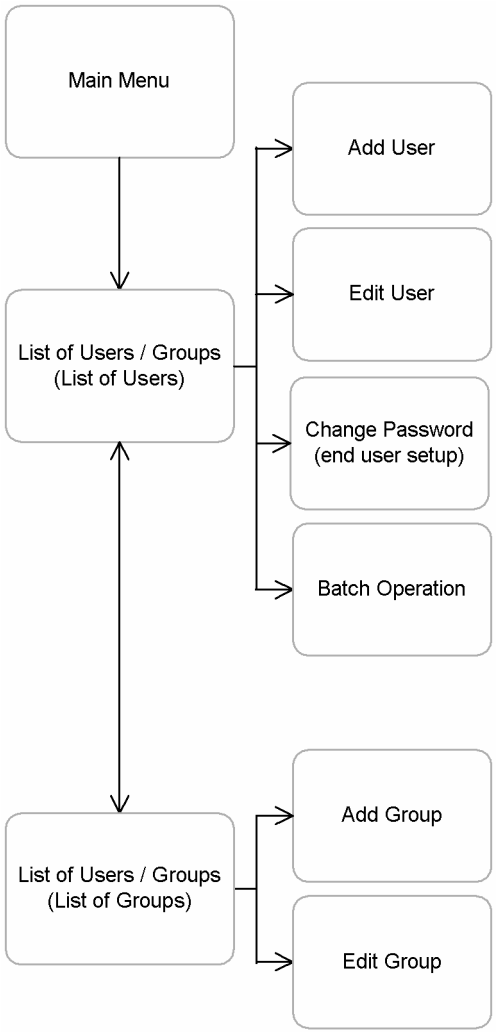



**Figure 4.6 Window Transitions for User Management**

### 4.3.1.3 File System Management

The following figure shows the window transitions for file system management.

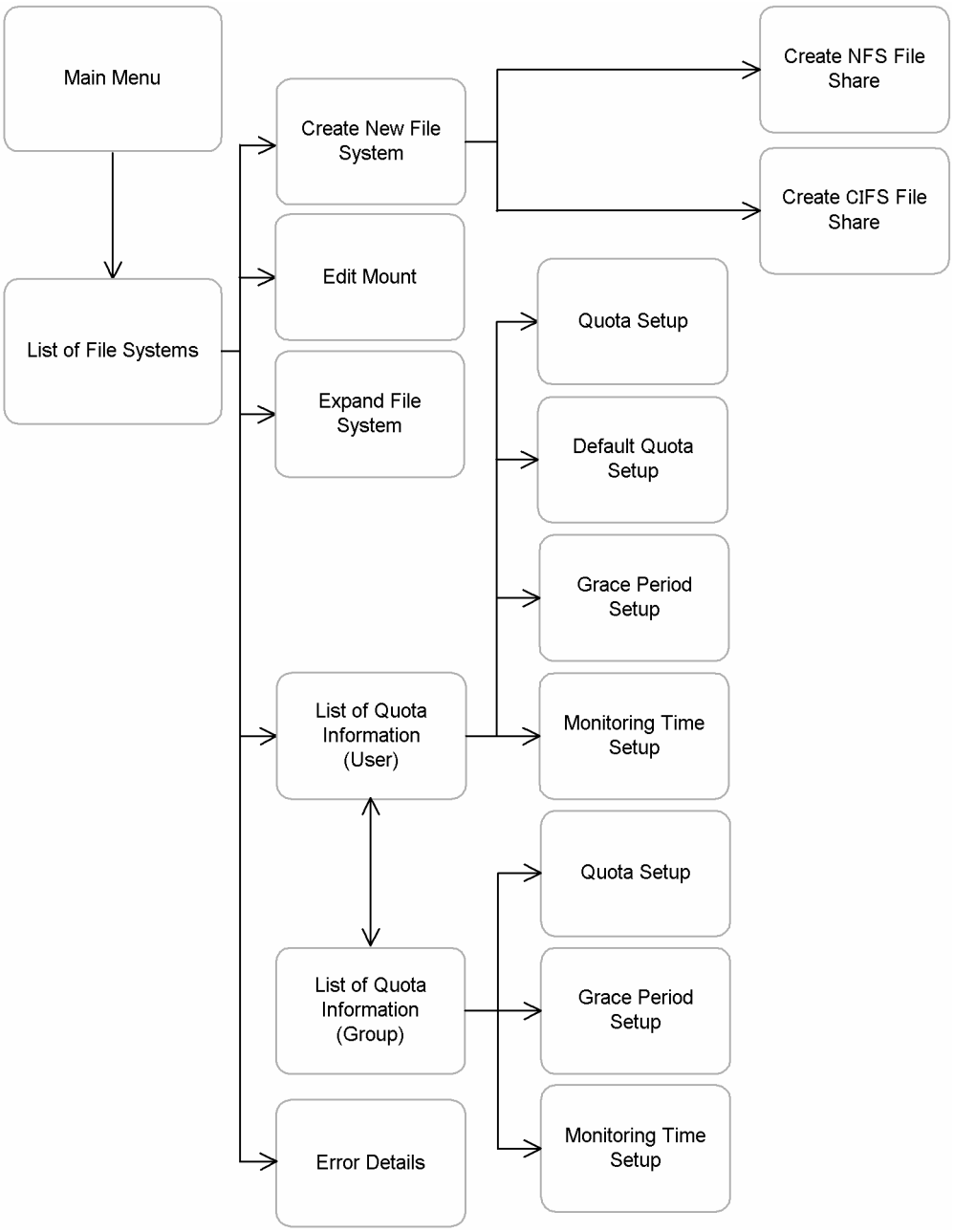



**Figure 4.7 Window Transitions for File System Management** ***Notes:***

- You cannot move to these windows when NAS Manager is in GUI operation mode and the total number of users registered by NAS Manager, the NIS server, and the LDAP server for user authentication exceeds 10,000.You cannot move to these windows when NAS Manager is in GUI operation mode and the total number of groups registered by NAS Manager, the NIS server, and the LDAP server for user authentication exceeds 10,000.

– When NAS Manager is in command operation mode, a listing of quota information is not displayed in the **List of Quota Information** window, and you cannot move to the Quota Setup window.

### 4.3.1.4 File Share Management

The following figure shows the window transitions for file share management.

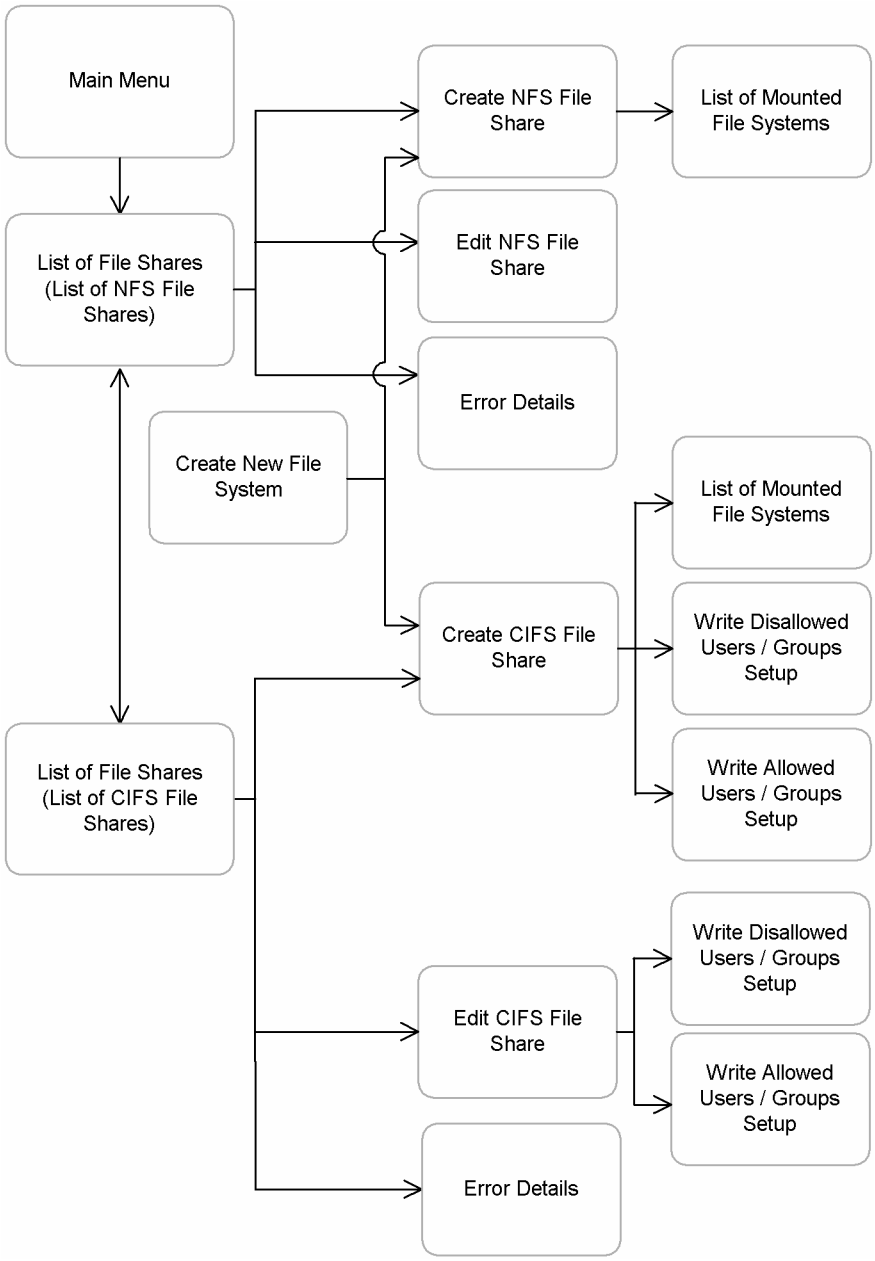



**Figure 4.8 Window Transitions for File Share Management**

***Notes:***

- You cannot move to these windows in either of the following cases:
- The total number of users or groups registered by NAS Manager, the NIS server, and the LDAP server for user authentication exceeds 10,000.
- NAS Manager is in command operation mode.

#### 4.3.1.5 Backup/Restore

For details on the backup and restore window transitions, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

#### 4.3.1.6 Differential-Data SnapShot

For details on the differential-data snapshot window transitions, see the *Hitachi AMS/WMS NAS Sync Image User's Guide*.

### 4.3.1.7 Error Information Management

The following figure shows the window transitions for error information management.

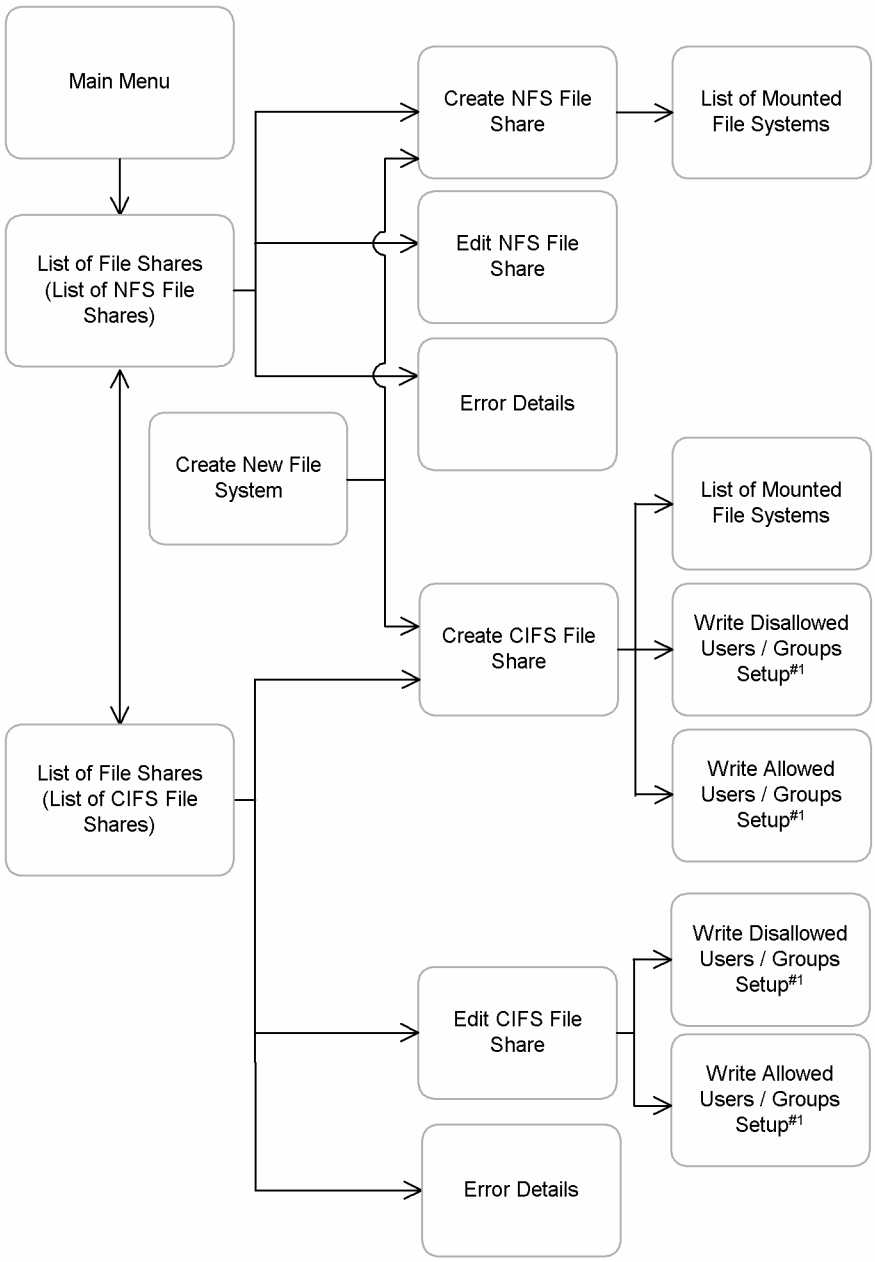



**Figure 4.9 Window Transitions for Error Information Management**

### 4.3.1.8 Program Management

The following figure shows the window transitions for program management.

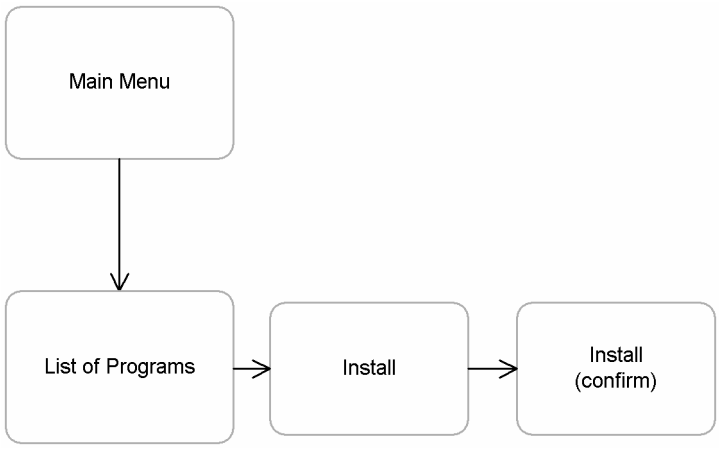



**Figure 4.10 Window Transitions for Error Information Management**

#### 4.3.1.9 Service Management

The following figure shows the window transitions for service management.

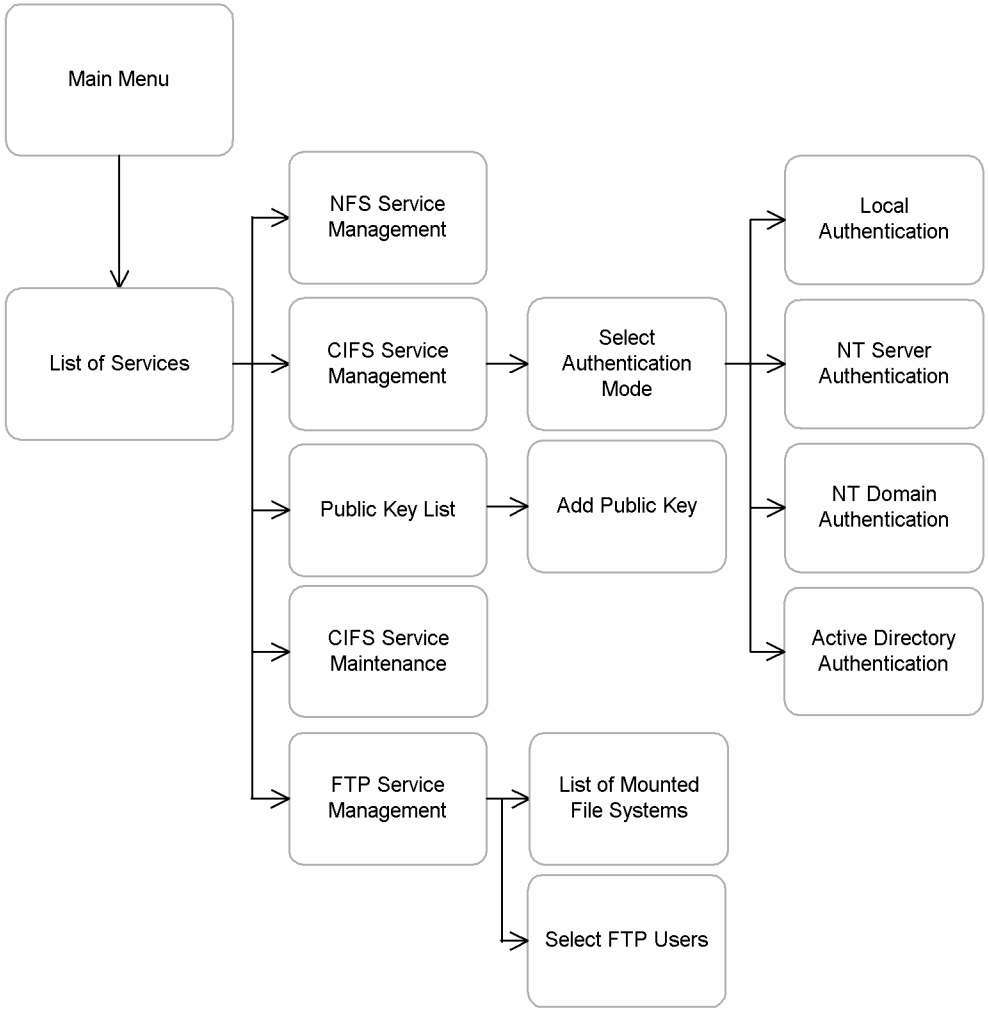



**Figure 4.11 Window Transitions for Service Management**

### 4.3.1.10 Editing System Administrator Personal Information

The following figure shows the window transitions for editing personal information about system administrators.

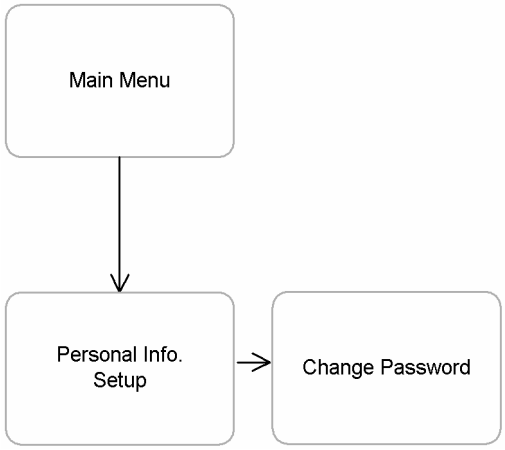



**Figure 4.12 Window Transitions for Editing System Administrator Information**

### 4.3.1.11 Saving the NAS System LUs

The following figure shows the window transitions for saving the NAS system LUs.

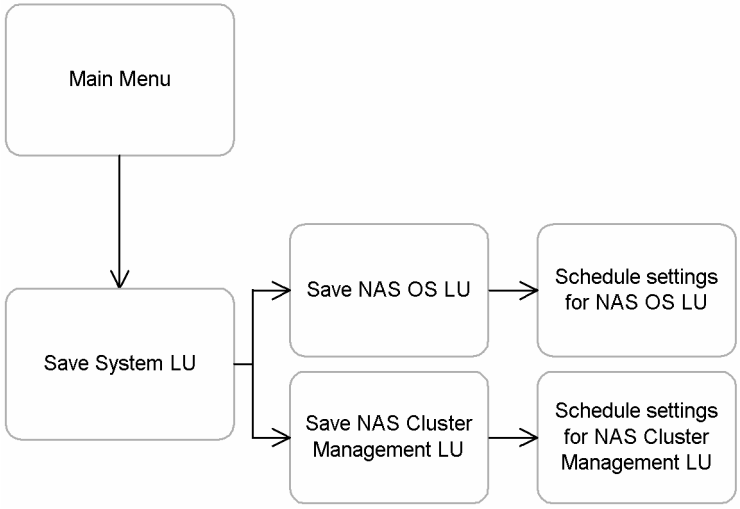



**Figure 4.13 Window Transitions for Saving the NAS System LUs**

#### 4.3.1.12 Anti-Virus Function

The following figure shows the window transitions for virus countermeasures.

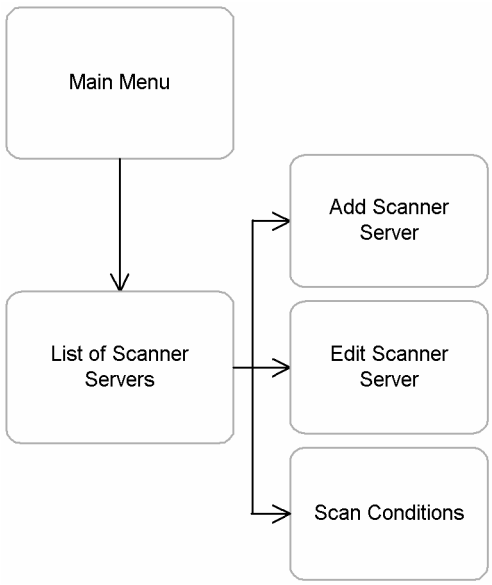



**Figure 4.14 Window Transitions for Virus Countermeasures**

## 4.4 Information Required Before Using the GUI

A system administrator uses NAS Manager functions from the GUI. This section describes the basic information you need to know before using the NAS Manager.

### 4.4.1 Window Layout and Method of Operation

The following describes the window layout in the NAS Manager and explains the basic operations common to all windows.

#### 4.4.1.1 Using a Wheel Mouse

When using a wheel mouse, do not rotate the wheel while pressing the **Shift** key. Doing so might cause the displayed window to change to another, and processing might not continue. If such an error has occurred, you must log out by clicking **Close** in the menu area, and then log in again.

If the window displayed when the error has occurred does not contain a **Close** button in the menu area, close the window by using the control menu of the web browser, and then log in again. When you log in, a window confirming the forced **Login** appears. Click the **Login** button and log in manually.

### 4.4.1.2 Window Layout

The following describes the window layout of the NAS Manager.

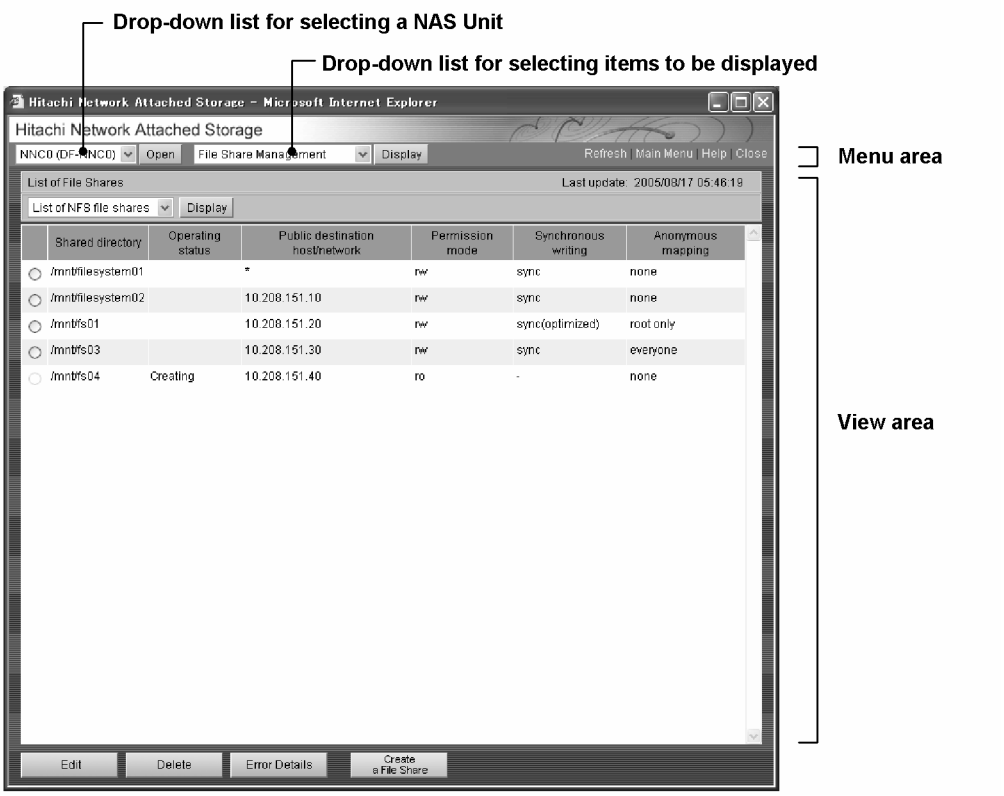



**Figure 4.15 GUI Window Layout**

The NAS Manager GUI for system administrators consists of a menu area and view area. The menu area is common to all windows accessed by system administrators, except for dialog boxes and the **Login** window.

The following describes how to use the components displayed in the menu area.

- Drop-down list for selecting a NAS Unit

  Select the NAS Unit to which you want to connect. When you have logged on from a program in the HiCommand series, only the NAS Unit you are currently connected is displayed.

  - **Open** button

    Click this button to display the **Main Menu** window for the selected NAS Unit.

    A different window is displayed for each NAS Unit. If a window is already displayed for the NAS Unit you selected, that window reverts to the **Main Menu** window. If, however, another system administrator is already logged in to the selected NAS Unit, a window opens prompting you to confirm the forced login.

    ***Note:*** Do not close the window that launched a NAS Unit before the window for the selected NAS Unit opens.

- Drop-down list for selecting items to be displayed

  Select the item whose window you want to display in the view area.

  You can select the same item as in the **Main Menu** window. For details on selectable items, see section 4.3. You cannot select an item for a different NAS Unit.

  - **Display** button

    Click this button to display the item you selected.

  - **Refresh**

    Click to refresh the information displayed in the window used to view a list or status. Although this link also appears in windows used for purposes other than viewing information, clicking the link in such windows does not refresh any information.

  - **Main Menu**

    Click to display the **Main Menu** window for the NAS Unit to which you are connected.

  - **Help**

    Click to display the HTML manual.

  - **Close**

    Click to close the current window by logging out.

#### 4.4.1.3 Method of Operation

The following describes the basic NAS Manager operations performed by a system administrator.

- Connecting to a different NAS Unit

  A system administrator can log in to, and manage, a NAS Unit only if the account administrator set up the system administrator to manage that NAS Unit.

  You can connect to a different NAS Unit after you log in to NAS Manager. In the menu area, from the drop-down list for selecting a NAS Unit, select a NAS Unit, and then click the **Open** button. A new window appears for the selected NAS Unit.

- Selecting an item to be displayed

  The items listed in the **Main Menu** window can be selected from each window also. In the menu area, from the drop-down list for selecting the item to be displayed, select the required item, and then click the **Display** button.

  You can only can select items for the currently running NAS Unit.

  For details on selectable menus, see section 4.3.

- Refreshing information in a window used to view a list or status

  Click **Refresh** in the menu area to refresh the information displayed in a window used to view a list or status. Although this **Refresh** also appears in other windows, clicking the button in such windows does not refresh any information.

- Displaying the HTML manual

  Click **Help** in the menu area to display the HTML manual.

- Displaying the **Main Menu** window

  Click **Main Menu** in the menu area to view the **Main Menu** window for the NAS Unit to which you are connected.

- Logging out from NAS Manager

  To log out from NAS Manager, click **Close** in the menu area of each of the displayed windows for all the NAS Units to which you are connected.

### 4.4.2 GUI Features

The system administrator can start the following tasks from the GUI without waiting for the previous task to finish:

- Creating a file system (including mounting and default quota setup)
- Mounting a file system
- Creating an NFS file share
- Creating a CIFS file share
- Setting up the differential-data storage device (operation from NAS Sync Image)
- Mounting a differential-data snapshot (operation from NAS Sync Image)

A maximum of four tasks can be queued for each node, and they are used in the order in which they are registered. The status of the queued tasks can be checked by viewing **Operating status** in the following windows:

- The **List of File Systems** window
- The **List of File Shares** (List of NFS file shares) window
- The **List of File Shares** (List of CIFS file shares) window
- The **List of File Systems** used for Sync Image window of NAS Sync Image
- The **List of Differential-Data Snapshots** window of NAS Sync Image

The system administrator must check the task results in each window listed above. If the task terminated abnormally after it was queued, first click the **Error Details** button in each window, check the error details in the **Error Details** windows, and then promptly take corrective action. The maximum number of stored error information entries and queued tasks is 64. If you perform an operation from the GUI when the maximum has been reached, the operation fails and an error message is displayed.

When the number of tasks queued in the NAS Modular system has reached the maximum, an attempt to queue a new task from the GUI fails and an error message is displayed. Wait for a queued task to finish, and then try again.

## 4.5 Managing Clusters

In a NAS Modular system, a cluster consists of two NAS Units. These NAS Units are called *nodes*. If a failure occurs in one NAS Unit, you can keep the system running without having to stop any NAS Manager services such as NFS file shares or CIFS file shares.

A system administrator can log in to, and manage, a NAS Unit only if the account administrator set up the system administrator to manage that NAS Unit.

You must define the cluster configuration of the NAS Units you are connecting before using NAS Manager.

This section describes the tasks involved in cluster management, such as defining or changing the cluster configuration.

### 4.5.1 Defining a Cluster Configuration

If no cluster configuration is defined for the NAS Units to be connected, you must define the cluster configuration in the **Define Cluster Configuration** window. Until this operation has finished, you cannot set the information needed to start running the NAS Modular system for the NAS Units to which you are connected. To change a previously defined cluster configuration, see section 4.5.2.

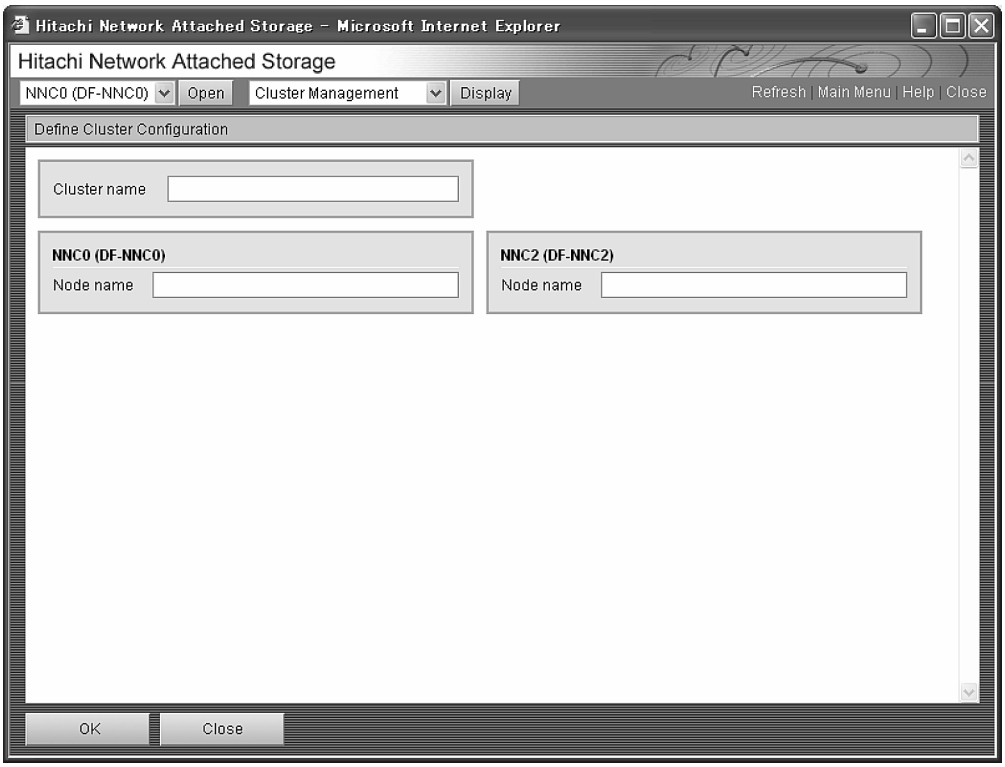



**Figure 4.16 Define Cluster Configuration Window**

To define the cluster configuration:

1. Connect to the NAS Unit that you want to configure.

   The **Define Cluster Configuration** window displays for the NAS Unit you selected, and a dialog box prompts you to define the cluster configuration.

2. Click the **OK** button.

   You can now use the **Define Cluster Configuration** window.

3. Enter the required information, then click the **OK** button. The cluster configuration settings are saved.

   After you click the **OK** button, note the following:

   - A dialog box appears, prompting you to set the interface and network. Click the **OK** button in this dialog box. The **Main Menu** window, which allows you to set the interface and network, appears. For details on settings for the interface and network, see section 4.7
   - Do not perform operations on the nodes that make up the cluster (for example, do not restart the NAS OS or disconnect a cable of the management LAN port until the operation has finished.

     ***Important***: If you do perform an operation on a node before the operation finishes, you must re-install the NAS OS and re-define the cluster configuration.
   - To cancel the settings, click the **Close** button. The window closes.

   The following table lists and describes the information to be specified in the **Define Cluster Configuration** window:

**Table 4.3 Information Specified in the Define Cluster Configuration Window**

| Item | Description |
|---|---|
| **Cluster name** | Enter any name to identify the cluster consisting of nodes, that is, NAS Units in pairs.<br>You can use a maximum of 22 characters.<br>You can use any alphanumeric character, hyphen (-), period (.), forward slash (/), colon (:), at mark (@), and underscore (_).<br>You cannot use an underscore (_) as the first character.<br>You cannot specify words reserved by the system. For details on reserved words, see Appendix A.1, List of Reserved Words. |
| **Node name** | Enter any name as the node name. A *node name* is the name of an element that corresponds to each NAS Unit in the cluster. This node name differs from the NNC name set for the NAS Unit.<br>You can use a maximum of 22 characters.<br>You can use any alphanumeric character, hyphen (-), period (.), colon (:), at mark (@), and underscore (_).<br>You cannot use an underscore (_) as the first character.<br>You cannot specify words reserved by the system. For details on reserved words, see Appendix A.1, List of Reserved Words. |

### 4.5.2 Changing a Cluster Configuration

In the **Modify Cluster Configuration** window, you can change a cluster configuration.

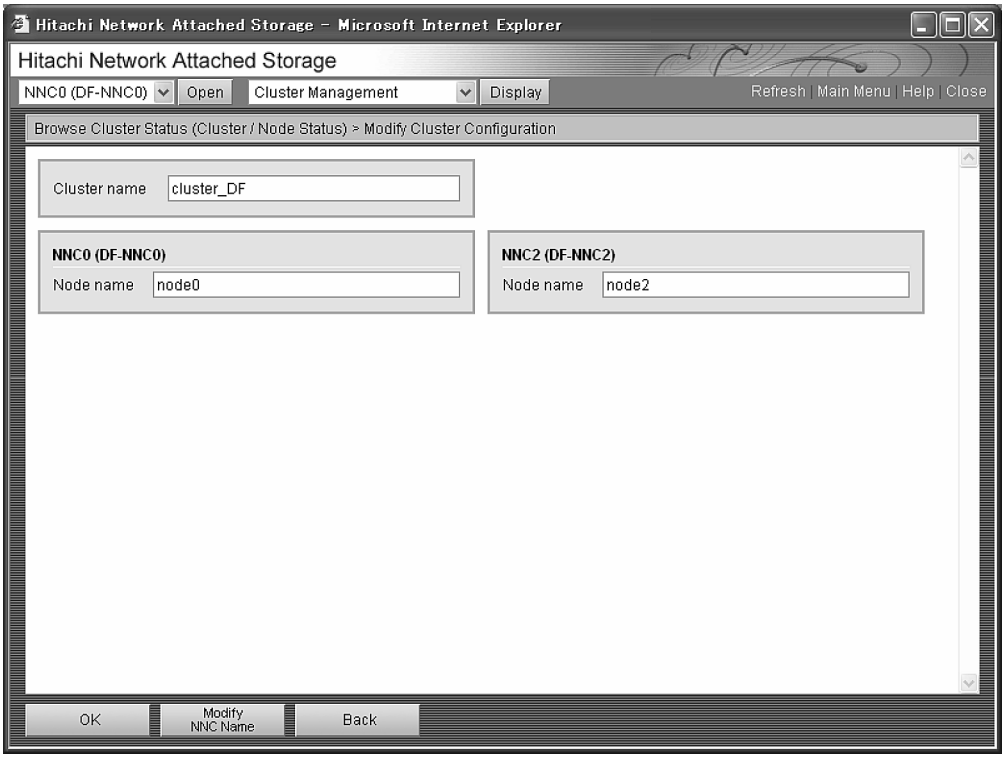



**Figure 4.17 Modify Cluster Configuration Window**

When you re-**Define Cluster Configuration**, the cluster and its resource groups must be stopped. If you want to re-**Define Cluster Configuration** and the cluster or its resource groups have started, you need to stop the cluster and its resource groups and then re-**Define Cluster Configuration**. After you re-define the cluster configuration, if necessary, start the cluster and its resource groups. For details on how to view, start, or stop the status of a cluster and its resource groups, see sections 4.5.3 and 4.5.4.

To change a cluster configuration:

1. In the **Main Menu** window, click the **Cluster Management** button.

   The **Browse Cluster Status** (Cluster / Node Status) window displays. For details on this window, see section 4.5.3.

2. Click the **Modify Configuration** button.

   The **Modify Cluster Configuration** window displays.

3. Change the required information, then click the **OK** button.

   The setting is saved, and the **Browse Cluster Status** (Cluster / Node Status) window reappears. After you click the **OK** button, do not perform operations on the nodes that make up the cluster (for example, do not restart a NAS OS or disconnect a cable of the management LAN port until the operation has finished. If you do perform an operation on a node before the operation finishes, you must re-install the NAS OS and re-define the cluster configuration.

   Depending on the NAS Unit usage status in the cluster (for example, the number of file systems, usage status of the volume manager, or the number of NFS file shares), the processing time might vary between 10 minutes and 50 minutes to save the setting contents.

   If you move to the Modify NNC Name window by clicking the **Modify NNC Name** button without clicking **OK**, the cluster configuration will not be changed.

   The following table lists and describes the information you can redefine in the **Modify Cluster Configuration** window:

**Table 4.4 Information Changed in the Modify Cluster Configuration Window**

| Item | Description |
|---|---|
| **Cluster name** | Enter any name to identify the cluster consisting of nodes, that is, NAS Units in pairs. |
| **Node name** | Enter any name as the node name. A *node name* is the name of an element that corresponds to each NAS Unit in the cluster. This node name differs from the NNC set for the NAS Unit. |

### 4.5.3 Viewing the Status of a Cluster and Nodes

In the **Browse Cluster Status** (Cluster / Node Status) window shown below, you can view the status of a cluster and its nodes.

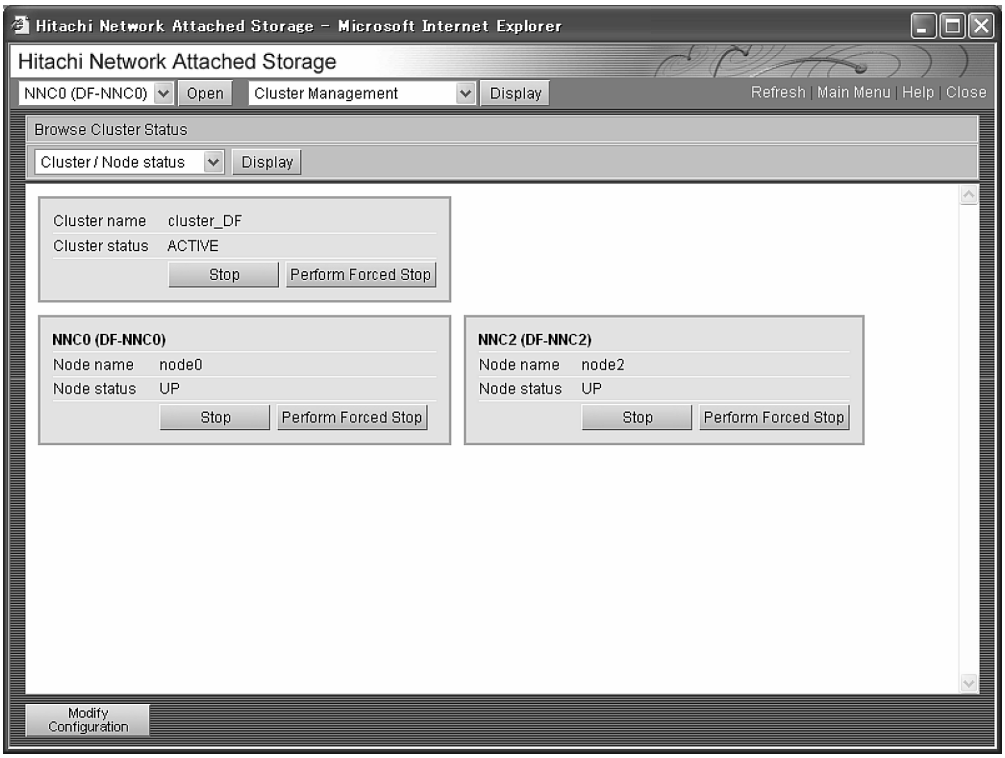



**Figure 4.18 Browse Cluster Status (Cluster / Node Status) Window**

The following table lists and describes the cluster and node information displayed in the **Browse Cluster Status** (Cluster / Node Status) window:

**Table 4.5 Contents of the Browse Cluster Status (Cluster / Node Status) Window**

| Item | Description |
|---|---|
| **Cluster name** | Name of the cluster. |
| **Cluster status** | Status of the cluster (see ***Note 1***):<br>`ACTIVE`<br>The cluster is running normally.<br>`INACTIVE`<br>The cluster stopped.<br>`UNKNOWN` (see ***Note 2***):<br>The status cannot be determined. |
| **Node name** | Names of the nodes in the cluster |
| **Node status** | Status of the nodes in the cluster(see ***Note 1***):<br>`UP` |

| Item | Description |
|---|---|
| | The node is running normally.<br>INACTIVE<br>The node stopped.<br>DOWN<br>The node ended abnormally and has shut down.<br>UNKNOWN (see ***Note 2***):<br>The status cannot be determined. |

***Note 1:*** If an error occurs in the system, the status of clusters and nodes may not be displayed. In this case, collect the error information and contact your HDS representative. For details on how to collect error information, see section 9.4.

***Note 2:*** After stopping a node or performing a forced stop of a node, if the **Browse Cluster Status** (Cluster / Node Status) window is displayed while you are logging into the stopped node, then UNKNOWN is displayed for the status of the cluster and the other node. In such a case, you cannot check the status of the cluster and the other node. To check the status of the cluster and the other node, log in to the running node (the other node), and then check the **Browse Cluster Status** (Cluster / Node Status) window.

To view the status of the cluster and its nodes:

1. In the **Main Menu** window, click the **Cluster Management** button.

   The **Browse Cluster Status** (Cluster / Node Status) window displays.

2. If the **Browse Cluster Status** (Resource Group Status) window is active, select **Cluster / Node status** from the drop-down list, then click the **Display** button.

### 4.5.4 Stopping and Starting a Cluster

In the initial status after installation, the cluster is stopped. A system administrator must set up network and interface information, and then start the cluster by using the **Browse Cluster Status** (Cluster/Node Status) window.

Also, a system administrator can stop and start a cluster during system maintenance or recovery after a failure. Stop a failed cluster when restoring it, and start the cluster when you finish the recovery task. You do not need to stop or start individual nodes when stopping or starting a cluster.

If a resource group was operating when a cluster was stopped, the system administrator needs to check whether a partial blockage has occurred in the resource group. For details on the partial blockage of the resource group, see section 4.1.3.

To stop or start a cluster:

1. In the **Main Menu** window, click the **Cluster Management** button.

   The **Browse Cluster Status** (Cluster / Node Status) window displays. If the **Browse Cluster Status** (Resource Group Status) window is active, select **Cluster / Node status** from the drop-down list, then click the **Display** button.

2. Click the **Stop** or **Start** button for the appropriate cluster.

   The **Stop** and **Perform Forced Stop** buttons appear if the cluster is active. The **Start** button appears if the cluster is inactive.

   Click the **Stop** button to stop all the nodes in the cluster and to stop all resource groups active on each node.

   Click the **Start** button to start all the nodes in the cluster. When a node starts, its resource groups can be activated.

3. In the **Browse Cluster Status** (Cluster / Node Status) window, in **Node status**, check for error information.

   Make sure that you finished the operation successfully. For details on how to check for error information in **Node status** in the **Browse Cluster Status** (Cluster / Node Status) window, see section 4.5.3.

   If any error information is displayed, a problem occurred during the operation. You must fix the problem. For details on how to remedy problems, see section 9.3.

### 4.5.5 Stopping and Starting a Node

During system maintenance or recovery after a failure, in the **Browse Cluster Status** (Cluster / Node Status) window, you can stop and start a node. Stop a failed node when you are restoring it after failover, and start the node when you finish the recovery task.

In normal operation, one resource group is active on one node. At failover, however, the resource group is switched to an alternate node. As a result, two resource groups will be active on the alternate node.

When a node is started after it is stopped, the system administrator needs to check whether a partial blockage has occurred in the resource group.

To stop or start a node:

1. In the **Main Menu** window, click the **Cluster Management** button.

   The **Browse Cluster Status** (Cluster / Node Status) window displays. If the **Browse Cluster Status** (Resource Group Status) window is active, select **Cluster / Node status** from the drop-down list, then click the **Display** button.

2. Click the **Stop** or **Start** button for the appropriate node.

   The **Stop** and **Perform Forced Stop** buttons appear if the node is active. The **Start** button appears if the node is inactive.

   Click the **Stop** button to stop the node and to switch the resource group active on that node to the alternate node. However, if two resource groups are active on the node you stopped, the resource group switched to the stopped node at failover becomes inactive, and the original resource group is moved to a different node. Depending on the usage status of the NAS Unit where the resource group that you want to perform failover is operating (for example, the number of file systems, usage status of the volume manager, or the number of NFS file shares), the processing time until failover finishes might vary between 10 minutes and 50 minutes.

   Click the **Start** button to start the node and to make the resource group available.

3. In the **Browse Cluster Status** (Cluster / Node Status) window, in **Node status**, check for error information.

   Make sure that you finished the operation successfully. If any error information is displayed, a problem occurred during the operation. You must fix the problem. For details on how to remedy problems, see section 9.3.

### 4.5.6 Performing a Forced Stop for a Cluster or Node

In the event of an error during stopping or starting of a cluster or node, in the **Browse Cluster Status** (Cluster / Node Status) window the system administrator can perform a forced stop for the failed cluster or node if processing cannot be continued.

Some services may remain running after a forced stop. This is because the system ignores any services affected by the error when completing the stop processing. If you start a resource group while some services remain running, two services with the same name may start. To prevent such a problem, do not start a resource group after a forced stop until the cluster or both nodes in the cluster have started. Performing a forced stop for a cluster may take an extended period of time.

When stop processing does not finish within 30 minutes, an uncorrectable error may have occurred. In this case, contact maintenance personnel.

You can recover from a temporary error by performing a forced stop for the cluster or node, and then restarting it. If you cannot recover from the error even after retrying this operation, you must determine the cause of the problem from the error information and take appropriate action. For details on the actions to take if an error occurs while stopping or starting a cluster or node, see section 9.3.

To perform a forced stop for a cluster or node:

1. In the **Main Menu** window, click the **Cluster Management** button.

   The **Browse Cluster Status** (Cluster / Node Status) window appears. For details on this window, see section 4.7.4. If the **Browse Cluster Status** (Resource Group Status) window is active, select **Cluster / Node status** from the drop-down list, and then click the **Display** button.

2. Click the **Perform Forced Stop** button for the cluster or node.

   When you click the **Perform Forced Stop** button for a cluster, the system ignores any errors that occurred during processing, and performs a forced stop for all the nodes in the cluster and all resource groups active on each node.

   When you click the **Perform Forced Stop** button for a node, the system ignores any errors that occurred during processing, performs a forced stop for the node and initiates failover for the resource groups active on the node. Depending on the usage status of the NAS Unit where the resource group that you want to perform failover is operating (for example, the number of file systems, usage status of the volume manager, or the number of NFS file shares), the processing time until failover finishes might vary between 10 minutes and 50 minutes.

### 4.5.7 Viewing Resource Group Status

In the **Browse Cluster Status** (Resource Group Status) window, shown below, you can view the status of the resource groups active on the node of the NAS Unit to which you are connected.

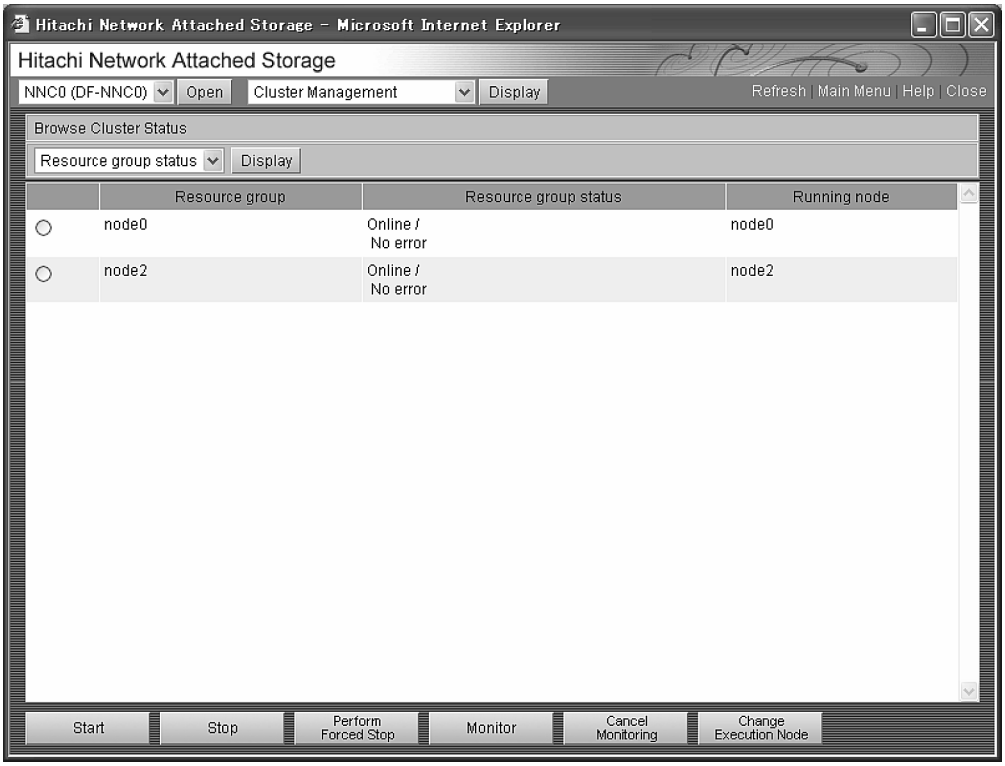



**Figure 4.19 Browse Cluster Status (Resource Group Status) Window**

The following table lists the resource group information displayed in the **Browse Cluster Status** (Resource Group Status) window:

**Table 4.6 Contents of the Browse Cluster Status (Resource Group Status) Window**

| Item | Description |
|---|---|
| **Resource group** | Name of a resource group.<br>Automatically allocated by the system. |
| **Resource group status** | Status and error information about a resource group, displayed in the following format:<br>*resource-group-status/error-information* |

| Item | Description | |
|---|---|---|
| | *resource-group-status* | `Online - Ready`<br>The resource group cannot start because the cluster is inactive, or an error was detected when the cluster was stopping.<br>`Initializing`<br>The resource group is initializing.<br>`Discovery (exclusivity)`<br>Online processing is being performed for the resource group before operations begin.<br>`Online - Pending`<br>The resource group is starting.<br>`Online`<br>The resource group is active.<br>`Online - Maintenance`<br>Automatic failover is impossible because monitoring is disabled.<br>`Offline - Pending`<br>The resource group is stopping.<br>`Offline`<br>The resource group is stopped.<br>`Internal Error`<br>An internal error was detected. Contact your HDS representative. |

| Item | Description | |
|---|---|---|
| Resource group status (continued) | *error-information* | `No error`<br>No errors occurred.<br>`Internal error - not recoverable`<br>An unrecoverable internal error occurred. Contact your HDS representative.<br>`Monitor activity unknown`<br>An error occurred during monitoring or while monitoring was being disabled. If you run the operation again and the error persists, perform a forced stop and fix the problem.<br>`No available nodes` or `No available nodes in failure domain after monitor failure`<br>An error occurred, but a failover could not be performed because it is already in a failover status. Perform a forced stop and remove the error that caused failover.<br>`Node not available (exclusivity)`<br>Failover is impossible because the **Node status** of the alternate node is not `ACTIVE`. Perform a forced stop and start the alternate node. If you cannot start the alternate node, perform a forced stop for the alternate node and fix the problem.<br>`Node unknown`<br>The resource group cannot be started because the **Node status** of the node is `UNKNOWN`. Perform a forced stop and start the node whose resource group you want to start. If you cannot start the node, perform a forced stop for the node and fix the problem.<br>`Split resource group (exclusivity)`<br>A duplicate resource group is active in the cluster. Perform a forced stop for the cluster, then request maintenance personnel to shut down and restart the NAS OS of the NAS Unit in the cluster.<br>`srmd executable error`<br>An error occurred during start or stop processing. Perform a forced stop and fix the problem. |
| **Running node** | Name of the node on which the resource group is running. | |

To view the status of a resource group active on the node of the NAS Unit to which you are connected:

1. In the **Main Menu** window, click the **Cluster Management** button.

   The **Browse Cluster Status** (Cluster / Node Status) window displays.

2. Select **Resource group status** from the drop-down list, then click the **Display** button.

   The **Browse Cluster Status** (Resource Group Status) window displays.

   If any error information is displayed in **Resource group status**, a problem occurred during the operation. You must fix the problem. For details on how to remedy problems, see section 9.3.

### 4.5.8 Stopping and Starting a Resource Group

In the initial status after installation, resource groups are stopped. After starting the cluster, a system administrator must use the **Browse Cluster Status** (Resource Group Status) window to start the resource groups.

Once operation starts, for each resource group the system administrator can start or stop an NFS share, a CIFS share, and other services provided by the resource group.

Before starting resource groups, make sure the data LAN ports are ready to communicate. For details on how to check the communication status for a data LAN port, see section 4.7.9.

After starting a resource group, check whether a partial blockage has occurred in the resource group. For details on the partial blockage of the resource group, see 4.1.3.

In normal operation, one resource group runs on one node. At failover, however, the resource group is switched to an alternate node. As a result, two resource groups will be active on the alternate node.

To stop or start a resource group:

1. In the **Main Menu** window, click the **Cluster Management** button.

   The **Browse Cluster Status** (Cluster / Node Status) window displays.

2. Select **Resource group status** from the drop-down list, then click the **Display** button.

   The **Browse Cluster Status** (Resource Group Status) window displays. For window details, see section 4.5.3.

3. Use a radio button to select a resource group, then click the **Stop** or **Start** button.

   Click the **Stop** button to stop the services provided by the selected resource group.

   Click the **Start** button to start the services provided by the selected resource group.

4. In **Resource group status**, check for error information.

   Make sure that you finished the operation successfully. For details on how to check for error information, see section 4.5.7.

   If any error information is displayed, a problem occurred during the operation. You must fix the problem. For details on how to remedy problems, see section 9.3.

### 4.5.9 Performing a Forced Stop for a Resource Group

In the event of an error when stopping or starting a resource group, in the **Browse Cluster Status** (Resource Group Status) window the system administrator can perform a forced stop for the affected resource group if processing cannot be continued.

Some services may remain running after a forced stop. This is because the system ignores any services affected by the error when completing the stop processing. If you start a resource group while some services remain running, two services with the same name may start. To prevent such a problem, do not start a resource group after a forced stop until the cluster or both nodes in the cluster have started.

You can recover from a temporary error by performing a forced stop for the resource group, and then restarting it. If you cannot recover from the error even after running this operation again, you must determine the cause of the problem from the error information and take appropriate action. For details on the actions to take if an error occurs while stopping or starting a resource group, see section 9.3.

To perform a forced stop for a resource group when an error occurs:

1. In the **Main Menu** window, click the **Cluster Management** button.

   The **Browse Cluster Status** (Cluster / Node Status) window displays.

2. Select **Resource group status** from the drop-down list, then click the **Display** button.

   The **Browse Cluster Status** (Resource Group Status) window displays. For window details, see section 4.5.4.

3. Click the **Perform Forced Stop** button for the resource group.

   When you click the **Perform Forced Stop** button, the system performs a forced stop for the resource group, ignoring any errors occurring during the process.

### 4.5.10 Disabling and Restarting Resource Group Monitoring

If your HDS representative or users incorrectly connect LAN cables during normal operation, the NAS Modular system will assume that an error occurred and initiate a failover. To perform a maintenance task on a service provided by a resource group, in the **Browse Cluster Status** (Resource Group Status) window the system administrator can temporarily disable resource group monitoring so as to avoid automatic failover.

To disable and restart resource group monitoring:

1. In the **Main Menu** window, click the **Cluster Management** button.

   The **Browse Cluster Status** (Cluster / Node Status) window displays.

2. Select **Resource group status** from the drop-down list, then click the **Display** button.

   The **Browse Cluster Status** (Resource Group Status) window displays. For window details, see section 4.5.4.

3. Use a radio button to select a resource group, then click the **Cancel Monitoring** or **Monitor** button.

   Click the **Cancel Monitoring** button to disable monitoring for the selected resource group.

   Click the **Monitor** button to restart monitoring for the selected resource group.

4. In **Resource group status**, check for error information.

   Make sure that you finished the operation successfully. For details on how to check for error information, see section 4.5.7.

   If any error information is displayed, a problem occurred during the operation. You must fix the problem. For details on how to remedy problems, see section 9.3.

### 4.5.11 Changing the Execution Node of a Resource Group

To carry out maintenance tasks or error recovery on a node, from the **Browse Cluster Status** (Resource Group Status) window, you can perform failover or failback by changing the execution node of a resource group.

When failover or failback occurs, the system administrator needs to check whether a partial blockage has occurred in the resource group.

To change the execution node of a resource group:

1. In the **Main Menu** window, click the **Cluster Management** button.

   The **Browse Cluster Status** (Cluster / Node Status) window displays.

2. Check the **Node status** of the destination node to which you are moving the resource group.

   Make sure that the **Node status** is `UP`. If it is not `UP`, you must start the destination node. For details on how to start a node, see section 4.5.5.

3. Select **Resource group status** from the drop-down list, then click the **Display** button.

   The **Browse Cluster Status** (Resource Group Status) window displays. For window details, see section 4.5.4.

4. Check the **Resource group status** of the resource group that you are moving.

   Make sure that the **Resource group status** is either `Online / No error` or `Online Maintenance / No error`. In any other status, you cannot change the execution node of the selected resource group.

5. Use a radio button to select the resource group that you want to move to another node, then click the **Change Execution Node** button.

   The selected resource group moves to the other node. Depending on the usage status of the NAS Unit where the resource group that you want to move is operating (for example, the number of file systems, usage status of the volume manager, or the number of NFS file shares), the processing time until failover finishes might vary between 10 minutes and 50 minutes.

6. In **Resource group status**, check for error information.

   Make sure that you finished the operation successfully. For details on how to check for error information, see section 4.5.7.

   If any error information is displayed, a problem occurred during the operation. You must fix the problem. For details on how to remedy problems, see section 9.3.

### 4.5.12 Rebooting the NAS OS

After any of the following operations, a system administrator can use the **Browse Cluster Status** (Cluster/Node Status) window to restart the NAS OS:

- Installing the NAS OS
- Installing an optional program that requires the NAS OS to be restarted

- Enabling or disabling use of the LDAP server for user authentication

The system administrator can also start, stop, or restart the NAS OS from Storage Navigator Modular, if necessary. For details on the NAS OS operations, see the manual *Storage Navigator Modular User's Guide*.

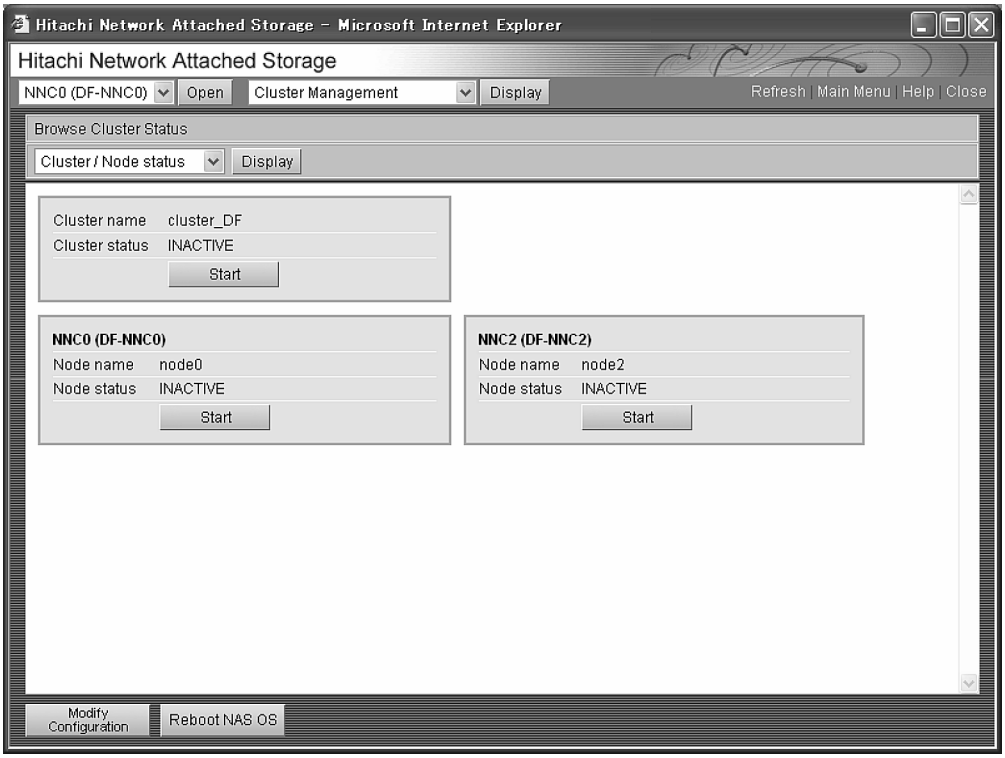



**Figure 4.20 Browse Cluster Status (Cluster / Node Status) Window**

***Note:*** Before the NAS OS is rebooted, the node must be stopped. Make sure that, in the **Browse Cluster Status** (Cluster / Node Status) window the system administrator confirms that the node at which the NAS OS is to be rebooted is inactive. For more information, see section 4.5.5.

To reboot the NAS OS:

1. In the **Main Menu** window, click the **Cluster Management** button.

   The **Browse Cluster Status** (Cluster / Node Status) window displays. If the **Node status** of the node you have logged on to is other than `UP`, the **Reboot NAS OS** button appears.

2. Click the **Reboot NAS OS** button.

   A dialog box confirms that you want to reboot the NAS OS.

3. Click the **OK** button.

   You are logged out of the connected NAS Unit, and a confirmation window displays.

4. Click the **Close** button.

   Close the Web browser. Wait for approximately five minutes, and log in again.

Then, start the node and perform failback.

For details on how to start a node, see section 4.5.5. For details on failback, see section 4.5.11.

### 4.5.13 Changing NNC Names

Before changing NNC names, the system administrator should:

- Notify the maintenance personnel and other administrators not to operate both the NAS Units in the cluster until the tasks finish.
- If you have already set up schedules for automatic operation, such as saving NAS system LUs, or automatic creation of a differential-data snapshot in NAS Sync Image, temporarily cancel all the schedules before changing the NNC names.

#### 4.5.13.1 General Tasks when Changing NNC Names

The general tasks required when changing an NNC name are as follows:

1. On each node in the cluster, stop the resource group.

   For details on how to stop a resource group, see section 4.5.8.

2. Stop the cluster.

   A details on how to stop a cluster, see section 4.5.4.

3. Change the NNC names.

   After you have changed the NNC names, the NAS OS in both NAS units in the cluster automatically restarts. Log out when you are prompted to log out.

   For details on how to change NNC names, see section 4.5.13.

4. Notify users that NNC names have been changed.

   The NetBIOS names set in the DNS server and domain controller must be changed to the new NNC names. For the CIFS clients that use an NNC name to access a file system, the NNC name must be changed.

5. Log in again.

   For details on how to log in, see section 4.2.1.

6. Start the cluster.

   For details on how to start a cluster, see section 4.5.4.

7. Start the resource groups in the cluster.

   For details on how to start a resource group, see section 4.5.8.

8. On each node in the cluster, manually save the NAS OS LU.

   For details on how to save a NAS OS LU manually, see section 4.17.2.1.

9. Manually, save the NAS Cluster Management LU.

   For details on how to save a NAS Cluster Management LU, see section 4.17.3.

### 4.5.13.2 Steps for Changing NNC Names

To change NNC Names:

1. In the **Main Menu** window, click the **Cluster Management** button.

   The **Browse Cluster Status** (Cluster / Node Status) window appears. For details on this window, see section 4.5.3.

2. Click the **Modify Configuration** button.

   The **Modify Cluster Configuration** window appears. For details on the this window, see section 4.5.2.

   After editing cluster configuration definitions in the **Modify Cluster Configuration** window, remember to click **OK**. If you do not click **OK**, the cluster configuration will not be changed.

3. Click the **Modify NNC Name** button.

   The **Modify NNC Name** window appears.

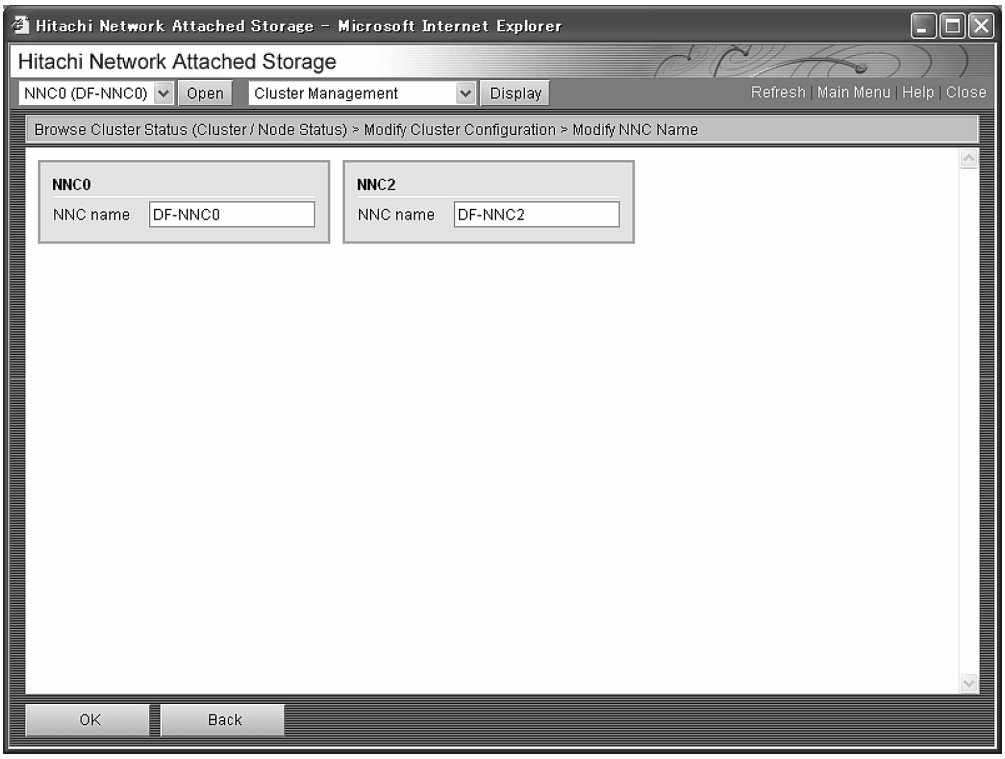



**Figure 4.21 Modify NNC Name Window**

4. Change information as required, and then click the **OK** button.

   A dialog box appears, asking you to confirm that you want to change the NNC names.

   The following table lists and describes the information to be specified in the Modify NNC Name window:

**Table 4.7 Information Specified in the Modify NNC Name Window**

| Item | Description |
|---|---|
| NNC **Name** | Specify an NNC name. The NNC name of each NAS Unit must be unique. Upper-case and lower-case letters are set exactly as specified, but names that differ only in case are assumed to be the same.<br>The NNC name can have a maximum of 10 characters.<br>You can use alphanumeric characters including hyphens (-). The NNC name must begin with an alphabetic letter, and must not end with a hyphen (-).<br>You cannot specify the words localhost, nasos, or system reserved words. They are not case-sensitive.<br>For details on system reserved words, see Appendix A, List of Reserved Words. |

5. Click the **OK** button.

   NNC names are changed.

   After the NNC names are changed, the NAS OS is automatically restarted on both NAS units in the cluster. When the window that prompts you to log out appears, click the **Close** button to log out.

   After clicking the **OK** button, do not perform any operation on the node that comprises the cluster (such as restarting a NAS OS or disconnecting a management LAN port cable) until the NAS OS has restarted and you have confirmed that you can log in to a NAS Unit again. If you perform such an operation before confirming that you can log in again, or if an error occurs while NNC names are being set, you must re-install the NAS OS and re-define the cluster configuration.

## 4.6 Managing Services

The NAS Modular system provides services such as NFS, CIFS, SSH, and FTP. The following table lists the services and management tasks that you can complete:

**Table 4.8 Services and Management Tasks**

| Service Type | Service Name | Change Configuration | Service Maintenance | Start, Stop, Restart |
|---|---|---|---|---|
| NFS service | NFS | Yes | No | Yes |
| CIFS service | CIFS | Yes | Yes | Yes |
| SSH service | SSH | Yes | No | No |
| FTP service | FTP | Yes | No | Yes |

This section contains information about checking the status of a service from the listed service information, changing a service configuration, performing maintenance for a service, and stopping, starting, and restarting services.

### 4.6.1 Viewing Service Information

In the **List of Services** window, shown below, you can view a list of information about the services running on each NAS Unit.

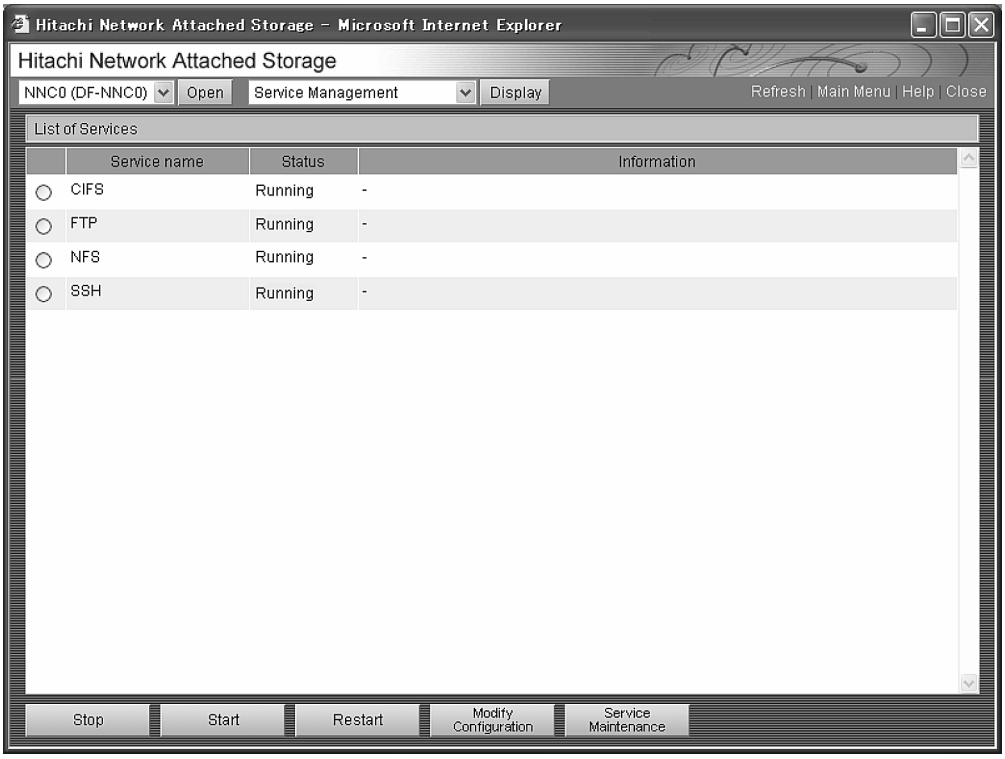



**Figure 4.22 List of Services Window**

The following table lists the information displayed in the **List of Services** window:

**Table 4.9 Contents of List of Services Window**

| Item | Description |
|---|---|
| **Service name** | Name of a service running on the NAS Unit. |
| **Status** | Operating status of the service as one of the following:<br>`running`<br>Displayed when the service is running normally.<br>`down`<br>Displayed when the service has terminated abnormally.<br>`failover`<br>Displayed when a failover has occurred for the resource group. |

| Item | Description |
|---|---|
| | `offline`<br>Displayed when the resource group is offline.<br>`stopped`<br>Displayed when the service has stopped. |
| **Information** | This item is displayed when the service needs to be restarted.<br>`The configuration was modified. Restart the service.`<br>This information is displayed when the service has not restarted since the configuration definition of the NFS service was modified. Restart the service.<br>`The configuration was modified. Start the service.`<br>This information is displayed when the service remains stopped since the configuration definition of the NFS service was modified. Start the service.<br>`The configuration was modified. Rebooting the NAS OS will not apply the modification.`<br>This information is displayed when the service has not restarted since the configuration definition of the CIFS service or FTP service was modified. Restart the service.<br>`The configuration was modified. Start the service. Rebooting the NAS OS will not apply the modification.`<br>This information is displayed when the service remains stopped since the configuration definition of the CIFS service or FTP service was modified. Start the service.<br>`Incomplete Service. Restart the service.`<br>This message appears if the service is operating in an incomplete state. The service running is incomplete. An error may have occurred. Collect the error information and contact your HDS representative, and then restart the service. For details on how to collect the error information, see section 9.3. |

To view a service information listing, click the **Service Management** button in the **Main Menu** window. The **List of Services** window displays.

### 4.6.2 Changing the NFS Service Configuration

You can use the **NFS Service Management** window, shown below, to change the configuration definitions of the NFS service.

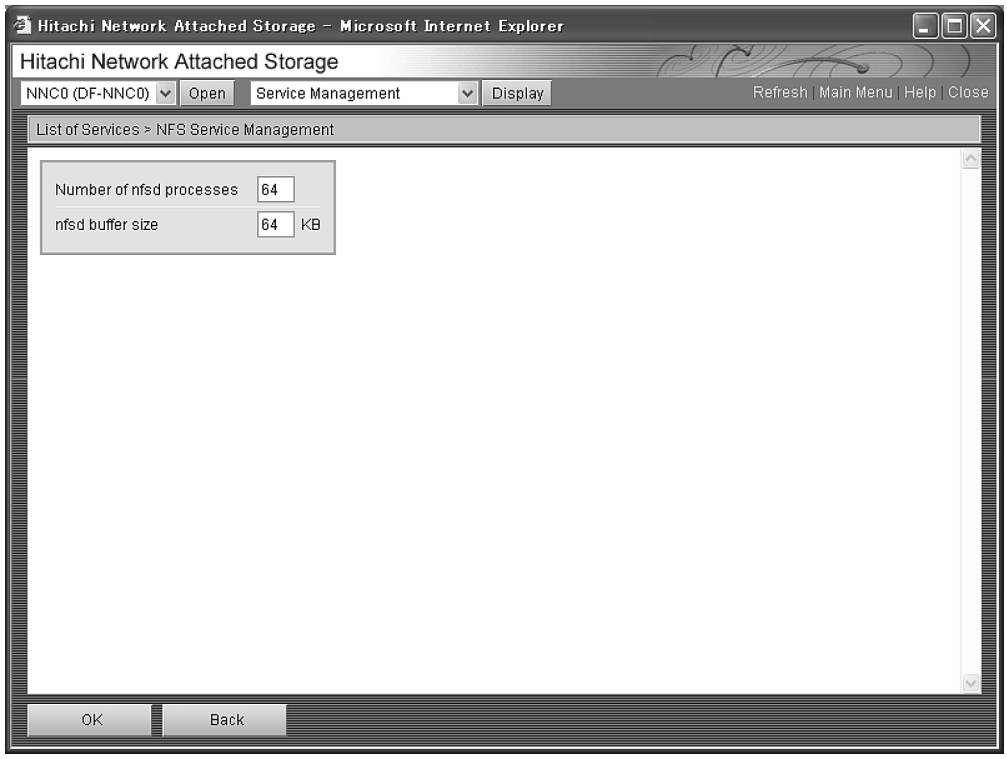



**Figure 4.23 NFS Service Management Window**

Before changing the configuration definitions of the NFS service, verify the following:

- In a NAS Modular system, the NFS service does not restart automatically after you modify its configuration definitions. When you modify the configuration definitions of the service, in the **List of Services** window click the **Start** button or the **Restart** button to restart the service.
- When the NAS OS is restarted after the configuration definitions of the NFS service was modified, the NFS service does not need to be restarted because the modified configuration definitions are applied.
- You must modify the service configuration definition of each NAS Unit equally to avoid any inconsistency among NAS Units in a cluster.
- You must request the NFS client host's administrator to unmount a file system from an NFS client before changing the **nfsd buffer size** (the maximum data size that can be transmitted) in the NFS service configuration definition. If you change the **nfsd buffer size** before the NFS client host's administrator unmounts the file system, access to the file system from the NFS client will be impossible after the NFS service is restarted. After modifying the configuration definition, you must request the NFS client host's administrator to mount the file system for the NFS client again.

By modifying configuration definitions, you can change the buffer size of data transmission or the number of NFS service daemons. For normal operation, however, there is no need to change the NFS service configuration. To change the NFS configuration definitions, call the Hitachi Data Systems Support Center.

To change the configuration of the NFS service:

1. In the **Main Menu** window, click the **Service Management** button.

   The **List of Services** window displays.

2. Use a radio button to select `nfs_service`, then click the **Modify Configuration** button.

   The **NFS Service Management** window displays.

3. Enter the required information, then click the **OK** button:

   - **Number of nfsd processes**

     Enter the number of nfsd processes that can be used. Specify a number from 1 to 256. The default value is 64.

   - **nfsd buffer size**

     Enter the maximum buffer size of data transmission. Request the NFS client host's administrator to unmount the file system from the NFS client before changing the maximum data size that can be transmitted.

     Specify a number from 8 to 64 (units: KB). The default value is 64. However, if NFS is mounted using the UDP protocol, the maximum data size that can be transmitted is 56 KB, even if 64 is specified for the value.

   The configuration definitions of the NFS service change and the **List of Services** window re-displays.

### 4.6.3 Before Changing the CIFS Service Configuration

Use the **NAS Manager** windows to change the configuration definitions of the CIFS service. Before changing definitions, verify the following:

- In a NAS Modular system, the CIFS service does not restart automatically after you modify its configuration definitions. When you modify the configuration definitions of the service, in the **List of Services** window click the **Start** button or the **Restart** button to restart the service.
- Even though the NAS OS is restarted after the configuration definitions of the CIFS service was modified, the modified configuration definitions are not applied. Restart the service.
- You must modify the service configuration definition of each NAS Unit equally to avoid any inconsistency among NAS Units in a cluster.
- If you modify the configuration definitions for the CIFS service while a change is being made to the file system from a CIFS client, the operation from the CIFS client may not finish normally. You must notify users before modifying the configuration definitions.

#### 4.6.3.1 Notes on Setting the Authentication Mode of the CIFS Service

The following provides notes on setting the Active Directory authentication mode for the CIFS service:

- After setting the Active Directory authentication mode, check the following:
  - The domain name used for the Active Directory domain has been set in **Default domain name** in the **DNS, NIS, LDAP Setup** window.
  - The DNS server used for the Active Directory domain has been set in **Primary DNS server** in the **DNS, NIS, LDAP Setup** window.
- Check the following conditions for the DNS server used for the Active Directory domain:
  - The service IP address and NNC name for the NAS Unit have been registered.
  - All the IP addresses registered for the host names of the domain controllers can communicate with the NAS Unit.
  - An IP address has not been dynamically added to the host name for the domain controller.
- When changing the Active Directory domain that the NAS Unit is to join, note the following:
  - After changing the Active Directory domain, if you immediately change the settings to rejoin the NAS Unit to its previous Active Directory domain, authentication of a CIFS client might result in an error even though the processing was successful. In this case, in the **CIFS Service Maintenance** window, click the **Rejoin Active Directory Domain** button to rejoin the NAS Units to the Active Directory domain.
  - After changing the Active Directory domain to a domain that has the same name as the previous one, if you join the NAS Unit to the new domain, an unnecessary computer account may remain in the previous Active Directory domain. Use the domain controller that is joined to the Active Directory domain to delete the unnecessary computer account.
- When a user registered in a domain attempts to access a file system of the NAS Modular system from a client machine that is not registered in the domain, user authentication may fail. In this case, use the **CIFS Service Maintenance** window to check whether the NetBIOS name of the Active Directory domain has been set correctly.

Note the following when you set the Active Directory authentication mode or the NT domain authentication mode for the CIFS service:

- If all the following conditions are satisfied, you must edit the `/etc/samba/lmhosts` file so that the NAS Unit can search for the domain controller of the domain with which a trust relationship has been established:
  - The domain to which the NAS Unit belongs has a trust relationship with another domain.
  - Either the domain to which the NAS Unit belongs, or the domain with which it has a trust relationship, is an NT domain.
  - The NAS Unit and the domain that has the trust relationship exist on different network segments.

  For details on how to edit the `/etc/samba/lmhosts` file, see section .

Note the following when you set the NT server authentication mode or the NT domain authentication mode for the CIFS service:

- When you set the NT server authentication mode or NT domain authentication mode, make sure that the network segment to which the NAS Unit is connected does not contain the following machines:

  When setting the NT server authentication:

  A machine that is not a server and whose name is the same as the NT server name specified in the NT Server Authentication window.

  When setting the NT domain authentication:

  A machine that is not a server and whose name is the same as the domain controller server name specified in the NT Domain Authentication window.

  When the NAS Unit is connected to multiple network segments (including VLANs), check the above condition for all the network segments to be connected.

#### 4.6.3.2 Notes on using user mapping

The following provides notes on using user mapping:

- To change the user mapping method from LDAP to RID or vice versa, you need to re-create the file systems.
- To share information about assigned user IDs and group IDs among multiple clusters, change the service configuration definitions so that the same user mapping settings are set on each node.
- Once a user ID or group ID is assigned, it can no longer be reused, even if you delete the user information from the domain controller.

The following notes are specific to each user mapping method.

Note the following when user mapping uses RIDs:

- Specify the range of user IDs and group IDs so that the range does not include user IDs and group IDs registered by NAS Manager, the NIS server, or the LDAP server for user authentication.

  Even if a user registered by the domain controller is registered with the same name for NAS Manager, the NIS server, or the LDAP server for user authentication, the user ID and group ID in the RID method are used when the user accesses a CIFS share.
- Considering the possibility that the range of user IDs and group IDs will be extended in the future, for NAS Manager, the NIS server, and the LDAP server for user authentication, we recommend that you do not use user IDs and group IDs beyond the range set by user mapping.

Note the following when user mapping uses LDAP:

- In the NAS Modular system, the LDAP server for user authentication and for user mapping cannot coexist. If information about the LDAP server for user authentication has been set in the **DNS, NIS, LDAP Setup** window, specifying user mapping information for LDAP in the **CIFS Service Management** window will result in an error.
- Information about assigned user IDs and group IDs is stored in the LDAP server as a database. You must create the tree for storing user IDs and group IDs on the LDAP server before restarting the CIFS server.
- If user mapping is used and the DNS server was set in the **DNS, NIS, LDAP Setup** window, configure the DNS server so that the NAS Unit can perform both forward and reverse lookup for the host name and IP address of the LDAP server used for user mapping.
- When you use a range specification to specify user IDs or group IDs, make sure that the range does not include a user ID or group ID registered by NAS Manager or the NIS server.
- If a user or group registered by NAS Manager or the NIS server accesses a CIFS share, the user is assumed to be a new user and a new user ID or group ID is assigned.
- Considering the possibility that the range of user IDs and group IDs will be extended in the future, for NAS Manager and the NIS server, we recommend that you do not use user IDs and group IDs beyond the range set by user mapping.

#### 4.6.3.3 Changing the CIFS Service Configuration

When using the **CIFS Service Management** window to change the CIFS service configuration definitions, you can specify whether or not to use user mapping, provided that the authentication mode assigned to the CIFS service is either NT domain authentication or Active Directory® authentication.

To change the configuration of the CIFS service:

1. In the **Main Menu** window, click the **Service Management** button.

   The **List of Services** window displays.

2. Use a radio button to select `cifs_service`, then click the **Modify Configuration** button.

   The **CIFS Service Management** window appears. The **CIFS Service Management** window always displays information based on the most recent configuration information. Therefore, if changes are made to the service configuration but the service has not been restarted or the service failed to restart, this window displays the configuration information to which the new configuration has not been applied to the service.

3. In **CIFS service setup** and **CIFS default setup**, specify the necessary information.

   The following table shows the information displayed in **CIFS service setup** in the **CIFS Service Management** window:

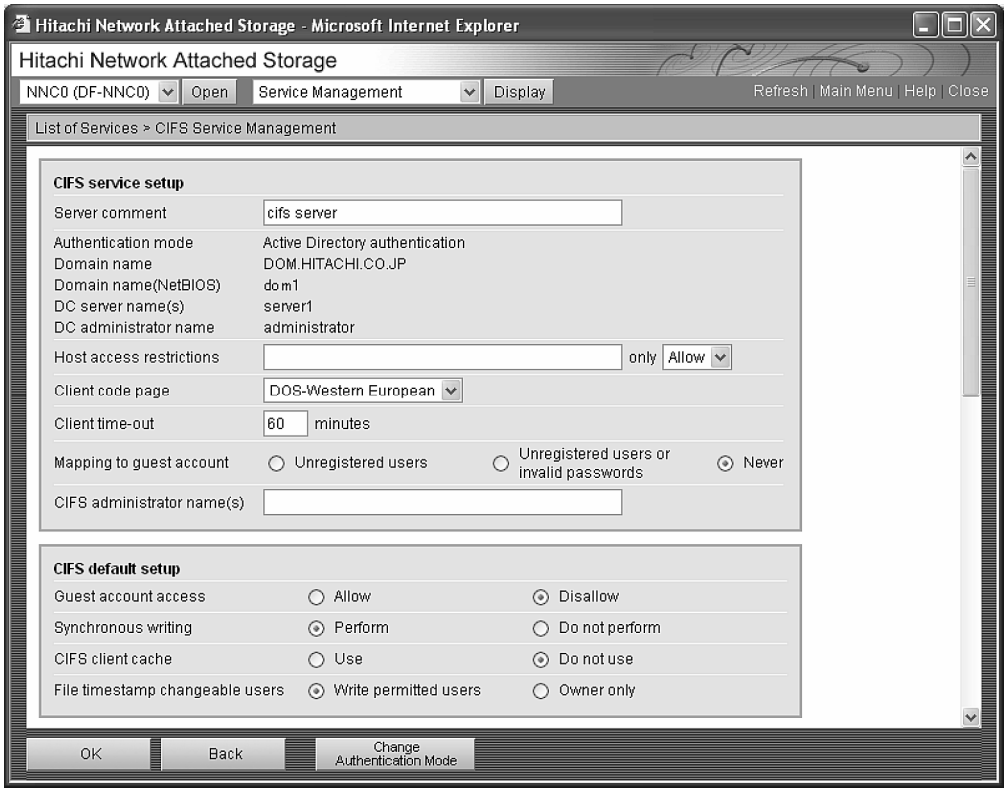



**Figure 4.24 CIFS service and default setup in the CIFS Service Management window**

The following table shows the information displayed in the **CIFS Service Management** window:

**Table 4.10 Contents of CIFS Service Management Window**

| Item | Description |
|---|---|
| **Authentication mode** | Displays the specified authentication mode, and the settings for user authentication used when a user logs on to the NAS Modular system from a CIFS client.<br>For details on the settings of the authentication mode, see section 4.8.3. |

The following table shows the information to be specified in **CIFS service setup** and **CIFS default setup** in the **CIFS Service Management** window.

**Table 4.11 Info Specified in CIFS Service and Default Setup Service Mgmt Window**

| Item | Description |
|---|---|
| **Server comment** | Enter a comment for the server name that appears on the CFS client.<br>Enter a maximum of 256 characters.<br>You can use any alphanumeric character, exclamation mark (!), number sign (#), dollar sign ($), ampersand (&), apostrophe ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), forward slash (/), colon (:), left angle bracket (<), right angle bracket (>), question mark (?), at mark (@), left bracket ([), backslash (\), right bracket (]), circumflex (^), underscore (_), grave accent (`), left brace ({), vertical bar (\|), right brace (}), and tilde (~). You can also specify spaces, but not at the beginning or end of the character string. A backslash (\) cannot be used at the end of the entry.<br>This item is optional. |
| **Host access restrictions**<br>(See ***Note 1, 2, 3,*** and ***4***) | Enter this item when you want to limit access by CIFS client hosts or networks to CIFS services. You can use a maximum of 1,023 characters. If this item is omitted, all hosts are allowed access to CIFS services.<br>If you want to limit access to CIFS services, enter the host name or network address in the text box and select whether to allow access to the CIFS services from the drop-down list. When specifying multiple hosts or networks, separate the specified host names and network addresses with commas (,).<br>**Allow**<br>Allow the specified hosts or networks to access CIFS services.<br>**Deny**<br>Do not allow the specified hosts or networks to access CIFS services. |
| **Client code page** | From the drop-down list, select the DOS code page used by the CIFS client accessing CIFS shared files.<br>**DOS-American**<br>United States.<br>**DOS-Western European**<br>Western European languages (Latin-1).<br>**DOS-Eastern European**<br>Eastern European languages (Latin-2).<br>**DOS-Japanese**<br>Japanese (SJIS). |
| **Client time-out** | Specify the maximum time to wait for a client response as the timeout value (units: minutes).<br>Specify from 0 to 1,440.<br>When 0 is specified, a client is not automatically disconnected by a timeout. |

| Item | Description |
|---|---|
| **Mapping to guest account**<br>(See ***Note 5*** and ***6***) | Specify the definition of guest account users.<br>If the authentication mode is NT server authentication, only **Never can be specified**.<br>**Unregistered users**<br>Select this if users unregistered in the system can be guest account users.<br>**Unregistered users or invalid passwords**<br>Select this if users unregistered in the system or users registered in the system who use an incorrect password can be guest account users.<br>***Note:*** If **Unregistered users or invalid passwords** is selected, users registered in the system can be guest account users even if the users enter an incorrect password.<br>**Never**<br>Select this if access to the CIFS service by guest account users is not permitted.<br>***Note:*** If **Never** is selected, access to all CIFS shares by guest account users is not permitted.<br>Even if **Allow** is selected in **Guest account** in the **Create CIFS File Share** or **Edit CIFS File Share** Windows, access is not permitted because the guest account setup for each CIFS share is disabled. |
| **CIFS administrator name(s)** | Specify a user name to be defined as a CIFS administrator. A CIFS administrator can perform operations such as deleting the unnecessary CIFS share files and changing permissions for all files and folders. When setting a CIFS administrator, consider the permissions to be given to the CIFS administrator.<br>If you want to specify multiple user names, separate them by commas ( **,** ).<br>When you are using user mapping, specify a domain name with the user name as follows:<br>*domain-name\user-name* |
| **Guest account access**<br>(See ***Note 5***) | Specify access permissions for guest account users on the CIFS service.<br>**Allow**<br>Select this to allow guest account users access to the CIFS service.<br>**Disallow**<br>Select this to disallow guest account users access to the CIFS service. |
| **Synchronous writing** | Specify whether to perform synchronous control for writing when a write request is issued from the CIFS client to the CIFS share folder.<br>If **Perform** is selected, data reliability improves when an error occurs in the network or the CIFS client, because a flush to disk is performed each time the CIFS client issues a write request. However, performance might deteriorate because a flush to disk occurs each time a write request is issued.<br>Regardless of the setting for this item, data can be saved to the disk when there is a flush to the file to be updated, or when the file is closed.<br>**Perform**<br>Select this to perform synchronous control when a write request is issued from a client.<br>**Do not perform**<br>Select this to not perform synchronous control when a write request is issued from a client. |

| Item | Description |
|---|---|
| **CIFS client cache** | Specify whether the updated data in the CIFS share file is to be cached on the client.<br>If **Use** is selected, performance improves when the updated data in the CIFS share file is cached on the client. However, when an error occurs in the network or CIFS client, data reliability might deteriorate.<br>**Use**<br>Select this if the updated data in the CIFS share file is to be cached on the client.<br>**Do not use**<br>Select this if the updated data in the CIFS share file is not to be cached on the client. |
| **File timestamp changeable users** | Select the users for whom you want to allow updating of CIFS share file timestamps. Select **Write permitted users** if the file is shared by the CIFS service only.<br>**Write permitted users**<br>Select this if you want to permit updating of the CIFS share file timestamp for all users who are permitted to write to this file.<br>**Owner only**<br>Select this if you want to restrict timestamp updating to the file owner. |

***Note 1:*** If you set **Host access restrictions** in the **CIFS Service Management** window, the settings in the **CIFS Service Management** window are applied to all CIFS shares regardless of the settings in the **Create CIFS File Share** window or **Edit CIFS File Share** window. If you want to set **Host access restrictions** for each CIFS share, set **Host access restrictions** in the **Create CIFS File Share** window or **Edit CIFS File Share** window, and do not set **Host access restrictions** in the **CIFS Service Management** window.

***Note 2:*** The user authentication of a CIFS client is performed even though access to CIFS services is permitted in **Host access restrictions**.

***Note 3:*** When you specify the host name in **Host access restrictions**, edit the `/etc/hosts` file in the **Edit System File** window to add the names and IP addresses of all hosts that are specified in **Host access restrictions**. If the host names are not added to the `/etc/hosts` file, the specified information might be invalid when access to the CIFS share is permitted or denied in **Host access restrictions**.

***Note 4:*** Specify the network in the following format:

- When specifying a network address:

  Specify an IP address (***example***: `10.203.15.0`).

- When specifying a network range by using a netmask, use the following format:

  *`network-address/netmask`* (***example***: `10.203.15.0/255.255.255.0`).

***Note 5:*** In **Guest account access** and **Mapping to guest account**, access permissions can be specified for the CIFS service for guest account users, also guest account user definitions can be specified. The guest account is regarded as `nobody` (user ID: `65534`) regardless of the CIFS service authentication mode. Therefore, allow access permissions in the CIFS share that guest account users can access as `nobody`. The guest account cannot be set for the ACL.

You can also specify access permissions for guest account users for each CIFS share in the CIFS service. When the CIFS service setup is changed, check the settings for each CIFS share, then change the settings if necessary. The settings for each CIFS share are specified in the **Create CIFS File Share** (see section 4.11.8) or **Edit CIFS File Share** windows. For details on the settings in the **Create CIFS File Share** window,. For details on the settings in the **Edit CIFS File Share** window, see section 4.11.11.

The guest account setup for each CIFS share is disabled when **Never** is specified in **Mapping to guest account**.

***Note 6:***

- When Local authentication is being used

  The users not registered by NAS Manager

- When NT server authentication is being used

  The users not registered in the Windows NT server

- When NT domain authentication is being used

  The users not registered in the domain controller in the domain

- When Active Directory authentication is being used

  The users not registered in the Active Directory domain controller

4. In **User mapping setup**, specify the necessary information.

   **User mapping setup** is displayed when the NT domain authentication mode or the Active Directory authentication mode has been set.

   Use a radio button to select whether to use user mapping, and specify information as required.

   – *When user mapping uses RIDs*

   – *When user mapping uses LDAP*

   – *When user mapping is not used*

   When user mapping uses RIDs

   The following table shows the information to be specified in **User mapping setup** in the **CIFS Service Management** window when user mapping uses RIDs.

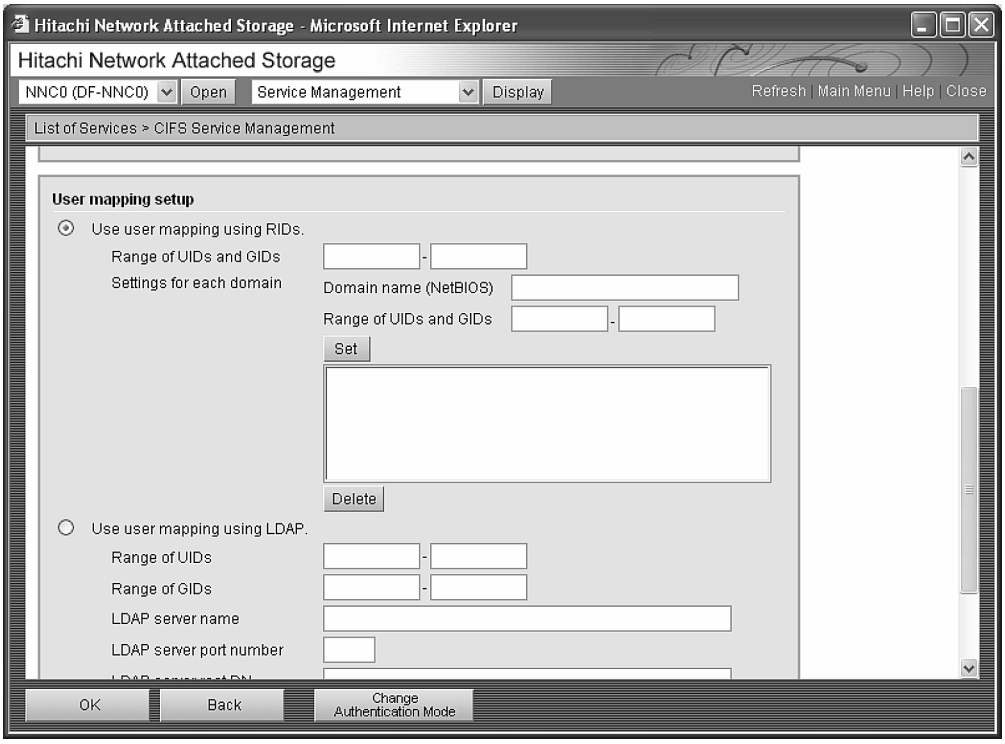



**Figure 4.25 User Mapping Setup in CIFS Service Mgmt Window (user mapping uses RIDs)**

**Table 4.12 User Mapping Setup in CIFS Service Mgmt Window (user mapping uses RIDs)**

| Item | Description |
|---|---|
| **Use user mapping using RIDs.** | Select this item when you want user mapping to use RIDs. When you select **Use user mapping using RIDs**, always specify **Range of UIDs and GIDs** and **Settings for each domain**. |
| **Range of UIDs and GIDs**#1 | Specify a range of user IDs and group IDs to be used for user mapping. You can specify a range of IDs within the range from 70,000 to 2,147,483,147.<br>Specify the minimum value in the left text box and the maximum value in the right text box. |

| Item | Description |
|---|---|
| **Settings for each domain** | Specify a range of user IDs and group IDs for each domain. You can specify a range for a maximum of six domains.<br>**Domain name (NetBIOS)**<br>Specify a domain name.<br>Specify the name of a domain that has a trust relationship with the domain set for the authentication mode.<br>**Range of UIDs and GIDs**#1<br>Specify a range of user IDs and group IDs for the specified domain. You can specify this range within the range of user IDs and group IDs set by user mapping. Specify the minimum value in the left text box and the maximum value in the right text box.<br>Make sure that the range for a domain does not overlap the range of another domain. The ranges for domains do not need to be consecutive.<br>After specifying the name of a domain and the range of user IDs and group IDs for the domain, when you click the **Set** button, the specified information is added to a list box.<br>To remove an entry from the list box, select the entry and then click the **Delete** button.<br>The entries in the list box are sorted in ascending order based on the ID range minimum value of each domain. |

***Note 1***: You cannot use the user IDs and group IDs that are being used by NAS Manager, the NIS server, the LDAP server for user authentication, or another domain. When you extend the range of user IDs and group IDs set for user mapping after applying the service, make sure the user IDs and group IDs that are being used by NAS Manager, the LDAP server for authentication, the NIS server, and another domain are not included in the new range, and then change the maximum value. If changing the maximum value would result in one or more of the currently used user IDs or group IDs being included in the new range, you need to re-create the file system, and then change the minimum value to extend the range. Set an adequate range of user IDs and group IDs after considering how long the operation will be performed and how much the number of users will increase.

**When user mapping uses LDAP**

The following figure and table show the information to be specified in **User mapping setup** in the **CIFS Service Management** window when user mapping uses LDAP.

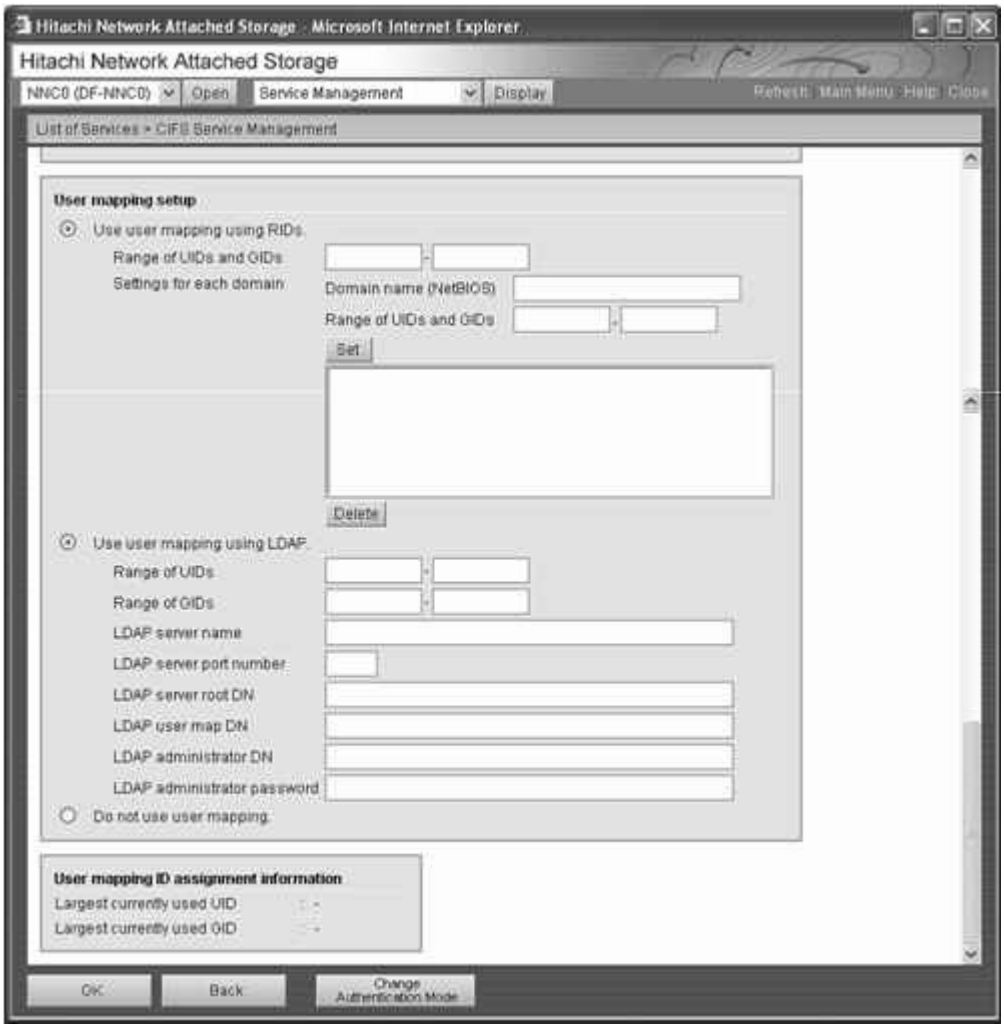



**Figure 4.26 Mapping Setup in CIFS Service Mgmt Window (when user mapping uses LDAP)**

**Table 4.13 Mapping Setup in CIFS Service Mgmt window (when user mapping uses LDAP)**

| Item | Description |
|---|---|
| **Use user mapping using LDAP.** | Select this radio button when you want user mapping to use LDAP. If you select this button, specify the items from **Range of UIDs** to **LDAP administrator password**. |
| **Range of UIDs**#1 | Specify a range of user IDs within the range from 70,000 to 2,147,483,147.<br>Specify the minimum value in the left text box and the maximum value in the right text box. |
| **Range of GIDs**#1 | Specify a range of group IDs within the range from 70,000 to 2,147,483,147.<br>Specify the minimum value in the left text box and the maximum value in the right text box. |
| **LDAP server name** | Specify the IP address or the host name of the LDAP server to be used for user mapping (the IP address is recommended). |

| Item | Description |
|---|---|
| **LDAP server port number** | Specify an LDAP server port number in the range from 1 to 65,535.<br>Specification of this item is optional.<br>The default value is `389`. |
| **LDAP server root DN** | Specify the identification name of the LDAP server root in DN format.<br>When OpenLDAP is used:<br>Specify the value specified in the suffix directive from the LDAP server definitions.<br>The following shows an example of specifying `dc=hitachi,dc=co,dc=jp` in the suffix directive:<br>`dc=hitachi,dc=co,dc=jp`<br>When Sun Java System Directory Server is used:<br>Select the **Directory** page to display the data tree. Specify the identification name starting from `dc=` displayed at the top level of the data tree. The following shows an example of specifying `dc=hitachi,dc=co,dc=jp`:<br>`dc=hitachi,dc=co,dc=jp`<br>When ADAM is used:<br>Specify the identification name that you specified in the **Application Directory Partition** page when creating the ADAM instance. |
| **LDAP user map DN** | Specify in DN format the identification name for which you want to add a user mapping account of the LDAP server.<br>Specify only the relative DN from **LDAP server root DN**.<br>The following shows an example of specifying **LDAP user map DN** when **LDAP server root DN** shows `dc=hitachi,dc=co,dc=jp` and the DN of the entry storing the user mapping account shows `ou=idmap,dc=hitachi,dc=co,dc=jp`:<br>`ou=idmap`<br>This item can be omitted. If you omit this item, the user mapping account is stored in the DN specified in **LDAP server root DN**. |
| **LDAP administrator DN** | Specify the identification name of the LDAP server administrator in DN format. Specify only the relative DN from **LDAP server root DN** for the DNs shown below.<br>When OpenLDAP is used:<br>The administrator DN specified in `rootdn`.<br>When the other LDAP server is used:<br>The DN for the user who is allowed the administrator permissions<br>The following shows an example of specifying **LDAP administrator DN** when **LDAP server root DN** shows `dc=hitachi,dc=co,dc=jp` and the name to identify the LDAP administrator shows `cn=Administrator,dc=hitachi,dc=co,dc=jp`:<br>`cn=Administrator` |

| Item | Description |
|---|---|
| **LDAP administrator password** | Specify the LDAP administrator password.<br>When OpenLDAP is used:<br>The value specified in `rootpw` from the LDAP server definitions.<br>When the other LDAP server is used:<br>The password for the user specified in **LDAP administrator DN**. |

***Note 1:*** If multiple CIFS clients attempt to open different CIFS shares on multiple nodes concurrently by using the same name for a new domain user, an ID might be missing from the range specified by **Range of UIDs** and **Range of GIDs**. The missing ID will not be reused.

When you extend the range of user IDs and group IDs set for user mapping after applying the service, make sure that user IDs and group IDs that are being used by NAS Manager, the NIS server, or another domain are not included in the new range, and then change the maximum value. If changing the maximum value would result in one or more of the currently used user IDs or group IDs being included in the new range, you need to re-create the file system, and then change the minimum value to extend the range. Set an adequate range of user IDs and group IDs after considering how long the operation will be performed and how much the number of users will increase.

When user mapping uses LDAP, you can check the largest value of the assigned user IDs and group IDs in **User mapping ID assignment information** in the **CIFS Service Management** window.

The following table shows the information to be displayed in **User mapping ID assignment information** in the **CIFS Service Management** window.

**Table 4.14 User Mapping Info ID Assignment in CIFS Service Maintenance window**

| Item | Description |
|---|---|
| **Largest currently used UID** | Displays the largest user ID within the range of user IDs that have already been assigned in the NAS Modular system.<br>Depending on the status of user mapping usage, the following information might be displayed:<br>`-`<br>Displayed when user mapping is not used.<br>`Not used, or less than the minimum UID used.`<br>Displayed when no user IDs have been assigned, or the smallest assigned user ID is smaller than the minimum value set in **Range of UIDs**.<br>`Cannot be got from LDAP server. Check the LDAP server settings and CIFS service configuration in service.`<br>Displayed when the largest user ID could not be acquired from the LDAP server for user mapping.<br>Check the user mapping settings and the operating status of the LDAP server. |

| Item | Description |
|---|---|
| **Largest currently used GID** | Displays the largest group ID within the range of group IDs that have already been assigned in the NAS Modular system.<br>Depending on the status of user mapping usage, the following information might be displayed:<br>-<br>Displayed when user mapping is not used.<br>`Not used, or less than the minimum GID used.`<br>Displayed when no group IDs have been assigned, or the smallest assigned group ID is smaller than the minimum value set in **Range of GIDs**.<br>`Cannot be got from LDAP server. Check the LDAP server settings and CIFS service configuration in service.`<br>Displayed when the largest group ID could not be acquired from the LDAP server for user mapping.<br>Check the user mapping settings and the operating status of the LDAP server. |

**When user mapping is not used**

The following table shows the information to be specified in **User mapping setup** in the **CIFS Service Management** window.

**Table 4.15 User Mapping Setup in CIFS Service Mgmt window (when mapping is not used)**

| Item | Description |
|---|---|
| **Do not use user mapping.** | Select this radio button if you do not want user mapping to be used. |

If you change the setting so that user mapping is not used, the range of user IDs and group IDs that was previously set is still displayed in **User mapping setup** in the **CIFS Service Management** window, even after the CIFS service is applied. If user mapping using RIDs was being used before the change, the domain-specific ranges of user IDs and group IDs are also displayed.

5. Click the **OK** button.

   The configuration definitions of the CIFS service change and the **List of Services** window reappears.

6. When you want user mapping to use LDAP, use the **List of RAS Information** (Batch-download) window to download the network information log group in a **Batch Operation**, and make sure that the LDAP server has been set up correctly.

   Use the log_interfaces_check file to check the status of the LDAP server.

   For details on how to download the log files in a **Batch Operation**, see 4.13.4.1. For details on the output of the log_interfaces_check file, see *D.3 Output content of the log_interfaces_check file*.

### 4.6.3.4 Setting up the Authentication Mode

To select and set up the authentication mode:

1. In the **Main Menu** window, click the **Service Management** button.

   The **List of Services** window displays.

2. Use a radio button to select `cifs_service`, then click the **Modify Configuration** button.

   The **CIFS Service Management** window displays. For window details, see section 4.6.3.1.

3. Click the **Change Authentication Mode** button.

   The Select Authentication Mode window displays.

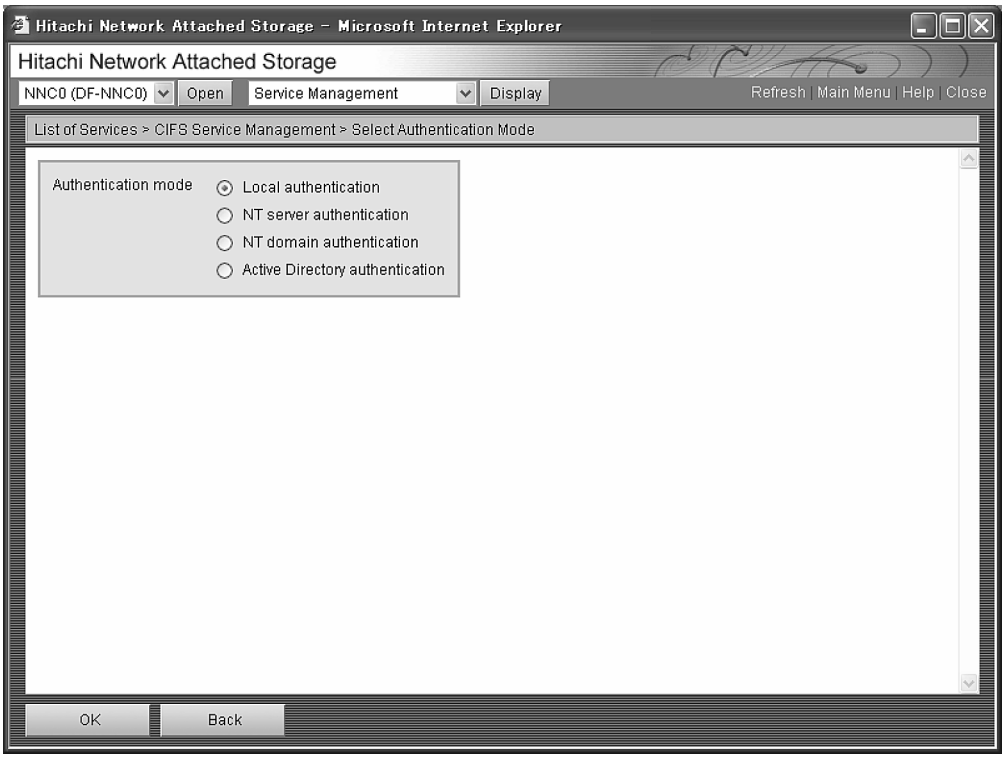



**Figure 4.27 Select Authentication Mode Window**

4. Use a radio button to select a desired authentication mode, then click the **OK** button.

   A relevant setup window for the selected authentication mode displays. Specify the following information in the Select Authentication Mode window:

   **Authentication mode**

   Using the following radio buttons, select a method for authenticating users logging on to the CIFS server from a CIFS client:

   - **Local authentication**

     Select this mode when the CIFS server authenticates users. Selecting this mode and then clicking the **OK** button displays the Local Authentication window.

   - **NT server authentication**

Select this mode when a Windows NT® server other than domain controller authenticates users. Users registered in the NAS Modular system cannot access CIFS shares, because users are managed by the specified Windows NT® server. Selecting this mode and then clicking the **OK** button displays the NT Server Authentication window.

- **NT domain authentication**

  Select this mode when the domain controller within the domain authenticates users. Users registered in the NAS Modular system cannot access CIFS shares, because users are managed by the corresponding domain controller. Selecting this mode and then clicking the **OK** button displays the NT Domain Authentication window.

- **Active Directory authentication**

  Select this mode when the Active Directory® domain controller authenticates users. Users registered in the NAS Modular system cannot access CIFS shares, because users are managed by the Active Directory® domain controller. Selecting this mode and then clicking the **OK** button displays the Active Directory Authentication window.

  ***Note:*** If user mapping is disabled when you select NT domain authentication or Active Directory authentication, user information registered in the domain controller must be registered by using NAS Manager, the NIS server, or the LDAP server for user authentication. Therefore, we recommend that you use user mapping when using NT domain authentication or Active Directory authentication to authenticate users. For details on how to enable user mapping, see 4.6.3.3.

5. In the setup window displayed according to the mode selected in step 4, enter required information, then click the **OK** button.

   The settings of the authentication mode take effect, and you return to the CIFS Services Management window.

   Figure 4.29 to Figure 4.35 show the setup windows to be displayed. Table 4.32 to Table 4.23 list the information to be specified in each window.

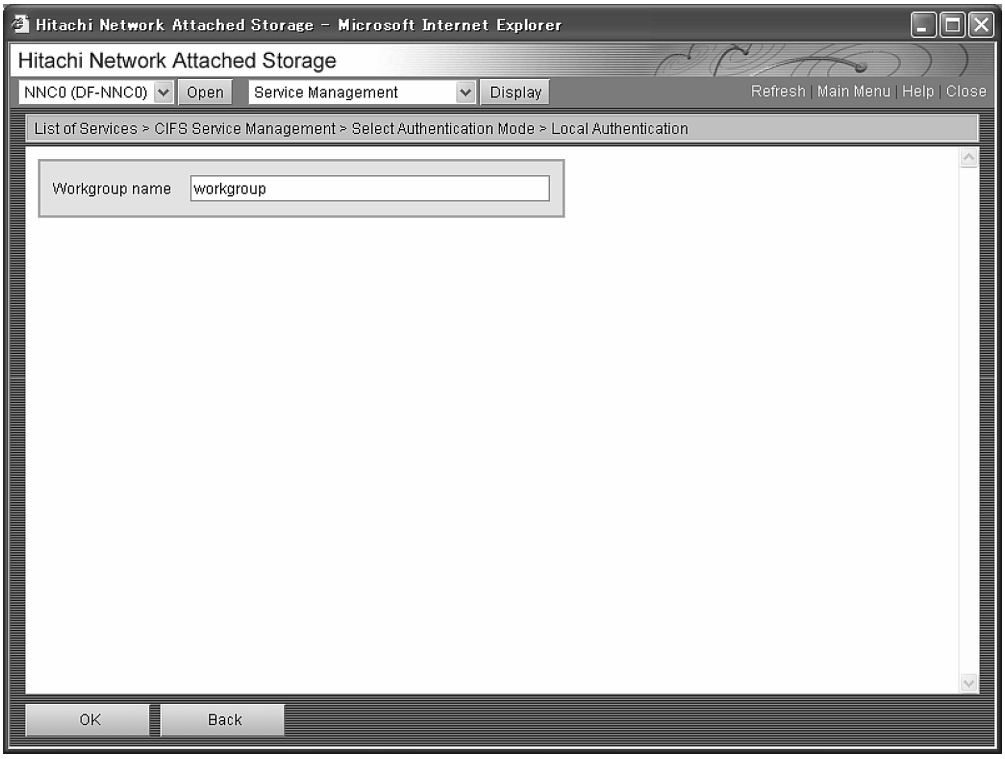



**Figure 4.28 Local Authentication Window**

Information specified in the Local Authentication window:

**Workgroup name**: The name of the work group to which the NAS unit server belongs. Use a name different from the NNC name. If you specify the same name, the group name may not be displayed correctly when you set an ACL.

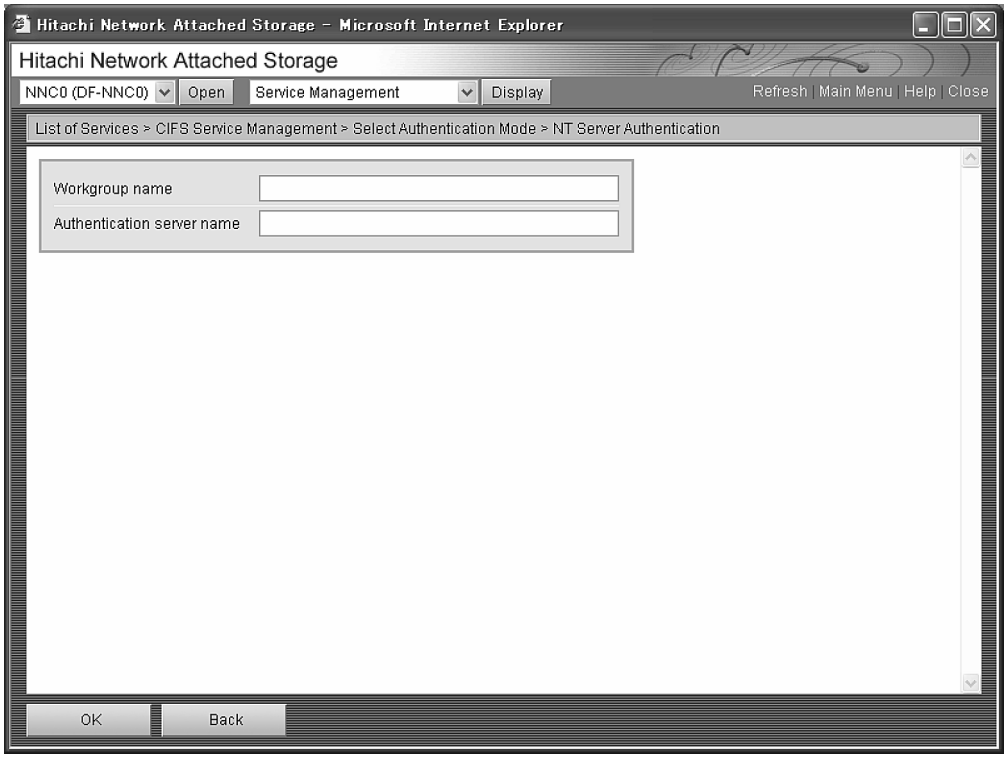



**Figure 4.29 NT Server Authentication Window**

**Table 4.16 Information Specified in NT Server Authentication Window**

| Item | Description |
|---|---|
| **Workgroup name** | Enter the name of the work group to which the NAS Unit server belongs.<br>Use a name different from the NNC name. If you specify the same name, the group name may not be displayed correctly when you set an ACL. |
| **Authentication server name** | Enter the name of the Windows NT® server that authenticates users. |

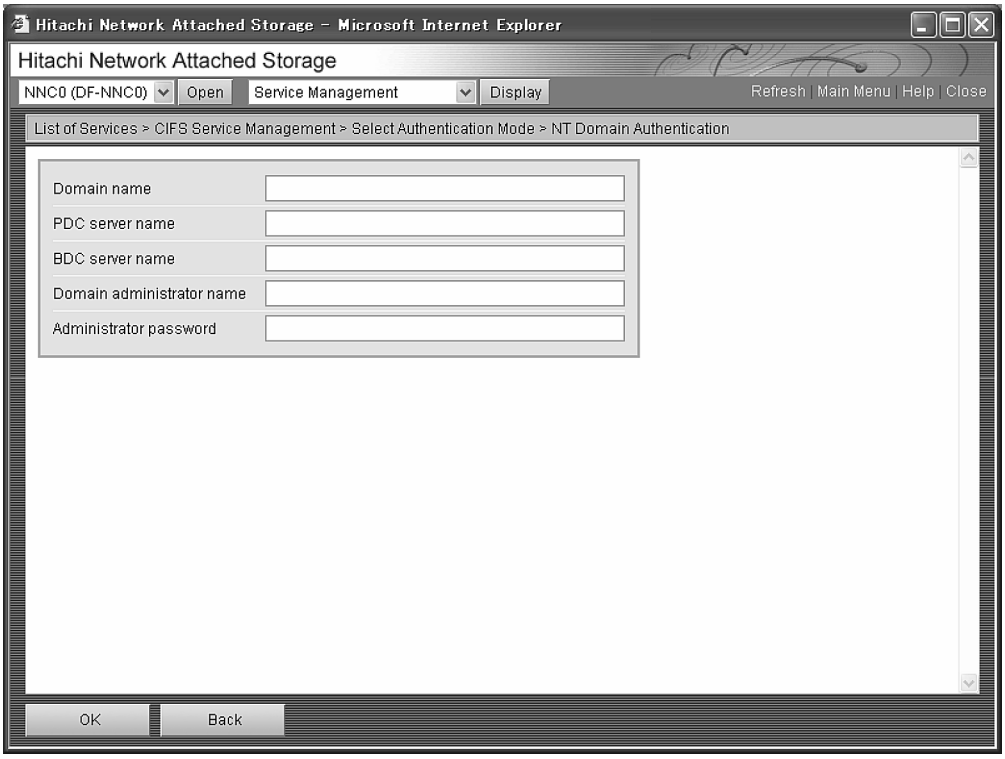



**Figure 4.30 NT Domain Authentication Window**

**Table 4.17 Information Specified in NT Domain Authentication Window**

| Item | Description |
|---|---|
| **Domain name** | Enter a domain name. |
| **PDC server name** | Enter the server name for the primary domain controller. |
| **BDC server name** | Enter the server name for the backup domain controller.<br>This item is optional. |
| **Domain administrator name** | Enter the user name of the domain administrator. |
| **Administrator password** | Enter the password of the domain administrator. |

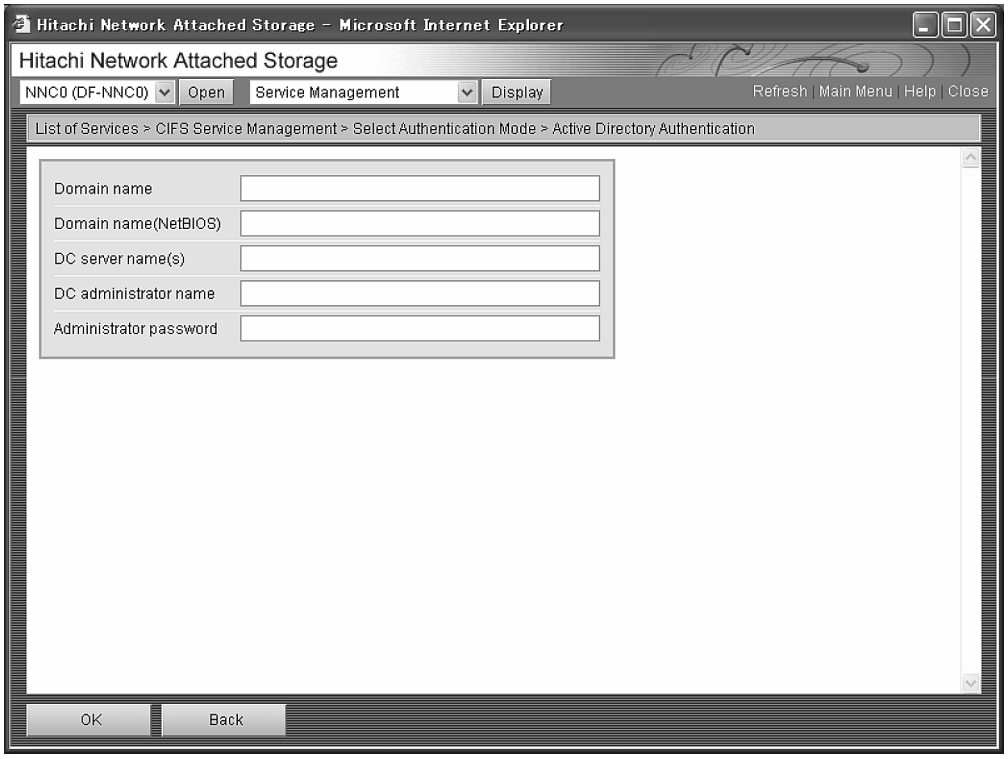



**Figure 4.31 Active Directory Authentication Window**

**Table 4.18 Information Specified in Active Directory Authentication Window**

| Item | Description |
|---|---|
| **Domain name** | Enter the DNS name of the Active Directory domain.<br>Any lower-case alphabetic characters are handled as upper-case alphabetic characters. |
| **Domain name (NetBIOS)** | Enter the NetBIOS name of the Active Directory domain (that is, the domain name used in Windows systems of Windows 2000 Professional or earlier). |
| **DC server name(s)** | Enter the server name for the Active Directory domain controller to which the NAS Unit belongs. Up to 5 server names can be specified. When specifying multiple names, separate each with a comma ( , ). |
| **DC administrator name** | Enter the user name of the domain administrator for the Active Directory domain controller. |
| **Administrator password** | Enter the password of the domain administrator for the Active Directory domain controller. |

### 4.6.4 Maintaining the CIFS Service

You can use the NAS Manager GUI to maintain the CIFS service. However, the following items must be verified beforehand:

- In an environment where user mapping is being used, when you delete the cached user mapping information from the CIFS service environment, the CIFS service automatically restarts. Make sure that no users are accessing CIFS shares, then delete the user mapping information.
- After you delete the user mapping information, a query about the user authentication information for an LDAP server occurs when a user first access the CIFS share, which in turn affects access performance. Therefore, delete the user mapping information only it is necessary to do so.
- When the CIFS service is rejoined to the Active Directory® domain, all the connected CIFS shares are disconnected, since a new computer account is registered in the domain. Make sure that no users are accessing the CIFS share, then rejoin the CIFS service to the Active Directory® domain.

#### 4.6.4.1 Viewing the CIFS service configuration that is being applied

In the **CIFS Service Maintenance** window, the system administrator can view the configuration definitions that are being applied to the CIFS service.

To view the configuration definitions that are being applied to the CIFS service:

1. Click the **Service Management** button in the **Main Menu** window.

   The **List of Services** window is displayed.

2. Use a radio button to select **CIFS**, and then click the **Service Maintenance** button.

   The **CIFS Service Maintenance** window appears. The information displayed in **User mapping information** in the **CIFS Service Maintenance** window differs depending on the user mapping method that is currently used.

   Figure 4.33 to Figure 4.35 show the **CIFS Service Maintenance** window, and Table 4.25 to Table 4.27 show the information to be displayed in the window.

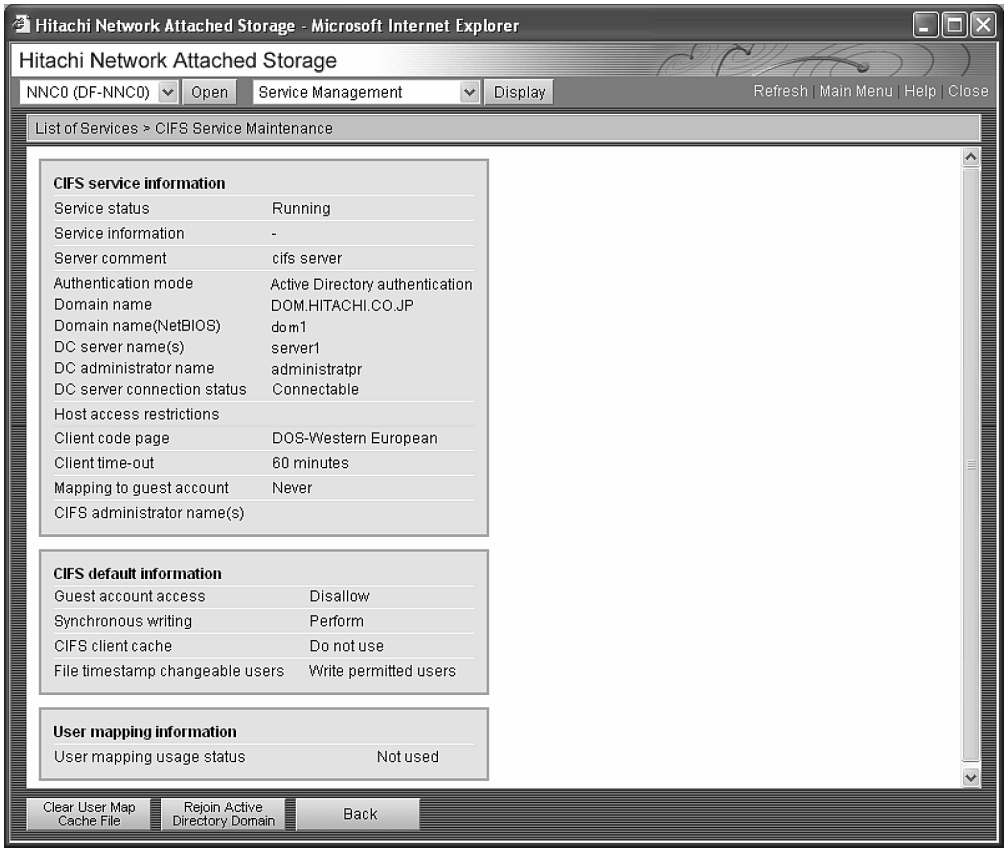



**Figure 4.32 CIFS Service Maintenance window**

**Table 4.19 Information displayed in the CIFS Service Maintenance window**

| Item | Description |
|---|---|
| **Service status** | Displays the status of the CIFS service.<br>`Running`<br>Displayed when the CIFS service is operating normally.<br>`Down`<br>Displayed when the CIFS service has terminated abnormally.<br>`Failover`<br>Displayed when the resource group has failed over to the other node.<br>`Offline`<br>Displayed when the resource group is stopped.<br>`Stopped`<br>Displayed when the CIFS service is stopped. |

| Item | Description |
|---|---|
| **Service information** | The information about the CIFS service operating status is displayed.<br>`The configuration was modified. Restart the service. Rebooting the NAS OS will not apply the modification.`<br>Displayed after the service configuration is changed. If this information appears, restart the CIFS service. The change is not applied by simply restarting the NAS OS.<br>`The configuration was modified. Start the service. Rebooting the NAS OS will not apply the modification.`<br>This information is displayed when the service remains stopped since the configuration definition of the CIFS service or FTP service was modified. Start the service.<br>`Incomplete Service. Restart the service.`<br>Displayed if a service has terminated abnormally. If this information appears, restart the service. |
| **Server comment** | Displays a comment on the server name displayed on the CIFS client. |

| Item | Description |
|---|---|
| **Authentication mode** | Displays information about the authentication mode and authentication server.<br>`Local authentication`<br>Displayed when local authentication is being used.<br>**Workgroup name**<br>Displays the work group name.<br>`NT server authentication`<br>Displayed when NT server authentication is used.<br>**Workgroup name**<br>Displays the work group name.<br>**Authentication server name**<br>Displays the name of the Windows NT server that is used as an authentication server.<br>`NT domain authentication`<br>Displayed when NT domain authentication is being used.<br>**Domain name**<br>Displays the domain name.<br>**PDC server name**<br>Displays the server name of the primary domain controller.<br>**BDC server name**<br>Displays the server name of the backup domain controller.<br>**Domain administrator name**<br>Displays the user name of the domain administrator.<br>`Active Directory authentication`<br>Displayed when Active Directory authentication is being used.<br>**Domain name**<br>Displays the domain name of the Active Directory domain.<br>**Domain name(NetBIOS)**<br>Displays the NetBIOS name of the Active Directory domain (the domain name used by a Windows machine that runs a Windows OS earlier than Windows 2000 Professional).<br>**DC server name(s)**<br>Displays the server name of the Active Directory domain controller.<br>**DC administrator name**<br>Displays the user name of the domain administrator for the Active Directory domain controller. |
| **DC server connection status**[#1] | Displays the connection status of the user authentication server. When there is at least one domain controller server to which you can connect, `Connectable` is displayed. |
| **Host access restrictions** | When only specific CIFS clients are allowed to access the CIFS service, the names of CIFS client hosts or the addresses of networks are displayed after `Allow`. When only specific CIFS clients are denied to access the CIFS service, the name of CIFS client hosts or the addresses of networks are displayed after `Deny`.<br>When all hosts are permitted to access the CIFS service, nothing is displayed. |

| Item | Description |
|---|---|
| **Client code page** | Displays the DOS code page used by the CIFS client.<br>`DOS-American`<br>Displayed when the American code page is used.<br>`DOS-Western European`<br>Displayed when the Western European (Latin-1) code page is used.<br>`DOS-Eastern European`<br>Displayed when the Eastern European (Latin-2) code page is used.<br>`DOS-Japanese`<br>Displayed when the Japanese (SJIS) code page is used. |
| **Client time-out** | Displays the client timeout value (in minutes). If `0` is displayed, automatic disconnection due to a timeout is not performed. |
| **Mapping to guest account** | Displays what kind of users will be treated as guests.<br>`Unregistered users`<br>Displayed when users who have not been registered in the system will be treated as guests.#2<br>`Unregistered users or invalid passwords`<br>Displayed when users who have not been registered in the system or who have been registered in the system but have an invalid password will be treated as guests.<br>`Never`<br>Displayed when guest access to the CIFS service is not permitted. |
| **CIFS administrator name(s)** | When one or more users have been set as CIFS administrators, this item displays their user names. |
| **Guest account access** | Displays whether to allow users to access the CIFS service as guests.<br>`Allow`<br>Displayed when guest access is allowed.<br>`Disallow`<br>Displayed when guest access is not allowed. |
| **Synchronous writing** | Displays whether to synchronize write operations when CIFS clients make requests to write to CIFS shared folders.<br>`Perform`<br>Displayed when synchronous writing is performed.<br>`Do not perform`<br>Displayed when synchronous writing is not performed. |
| **CIFS client cache** | Displays whether updates to the files in CIFS shares are to be cached on the client.<br>`Use`<br>Displayed when updates are cached on the client.<br>`Do not use`<br>Displayed when updates are not cached on the client. |

| Item | Description |
|---|---|
| **File timestamp changeable users** | Displays the users who can update the timestamps of files in CIFS shares.<br>`Write permitted users`<br>Displayed when all users able to write to the files are permitted to update the timestamps.<br>`Owner only`<br>Displayed when only file owners are allowed to update the timestamps. |
| **User mapping usage status** | Displays whether user mapping is used.<br>`In use`<br>Displayed when user mapping is used.<br>`Not used`<br>Displayed when user mapping is not used. |

***Note 1***: The label of this item **DC server connection status** differs depending on the authentication mode for the CIFS service. **DC server connection status** is displayed when NT domain authentication or Active Directory authentication is used, and **Authentication server connection status** is displayed when NT server authentication is used.

***Note 2***: The users to be treated as guests differ depending on the authentication mode that is currently used (the mode displayed in **Authentication mode**):

- When Local authentication is being used

  Users who are not registered by NAS Manager are treated as guests.

- When NT server authentication is being used

  Users who are not registered on the Windows NT server are treated as guests.

- When NT domain authentication is being used

  Users who are not registered in the domain controller in the domain are treated as guests.

- When Active Directory authentication is being used

  Users who are not registered in the Active Directory domain controller are treated as guests.

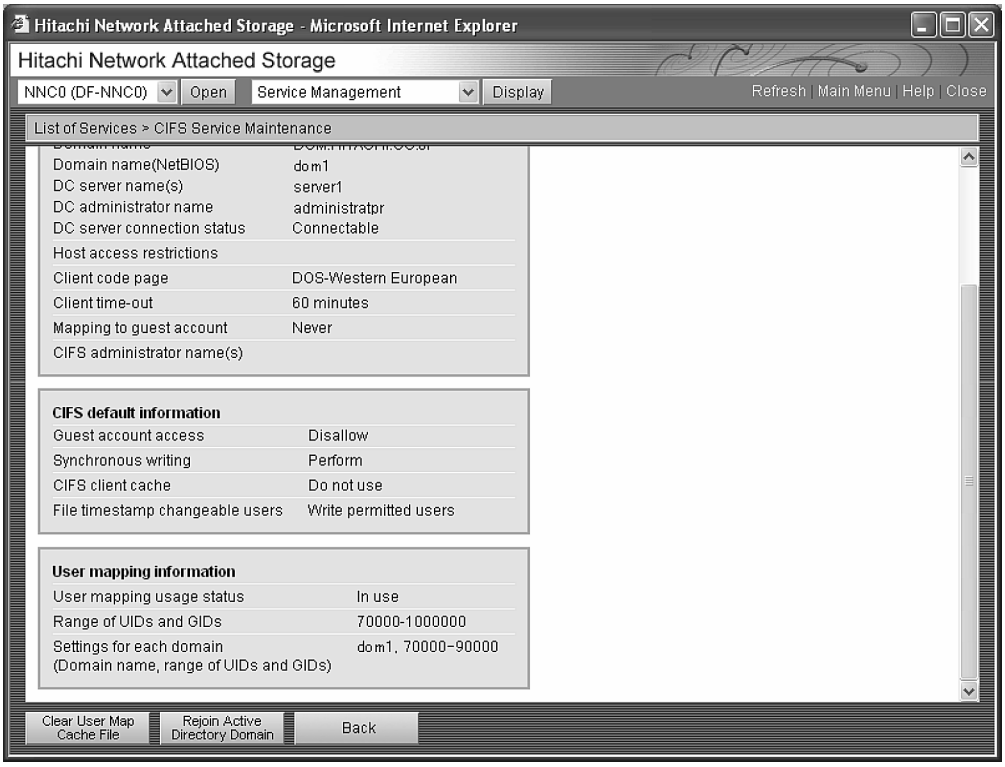



**Figure 4.33 CIFS Service Maintenance window (when user mapping uses RIDs)**

**Table 4.20 User Mapping in CIFS Service Maintenance window (when mapping uses RIDs)**

| Item | Description |
|---|---|
| **Range of UIDs and GIDs** | Displays the range of user IDs and group IDs mapped by using RIDs. |
| **Settings for each domain** | Displays the range of user IDs and group IDs set for each domain.<br>When two or more ranges have been set, they are displayed in ascending order of the minimum value for the range of user IDs and group IDs. |

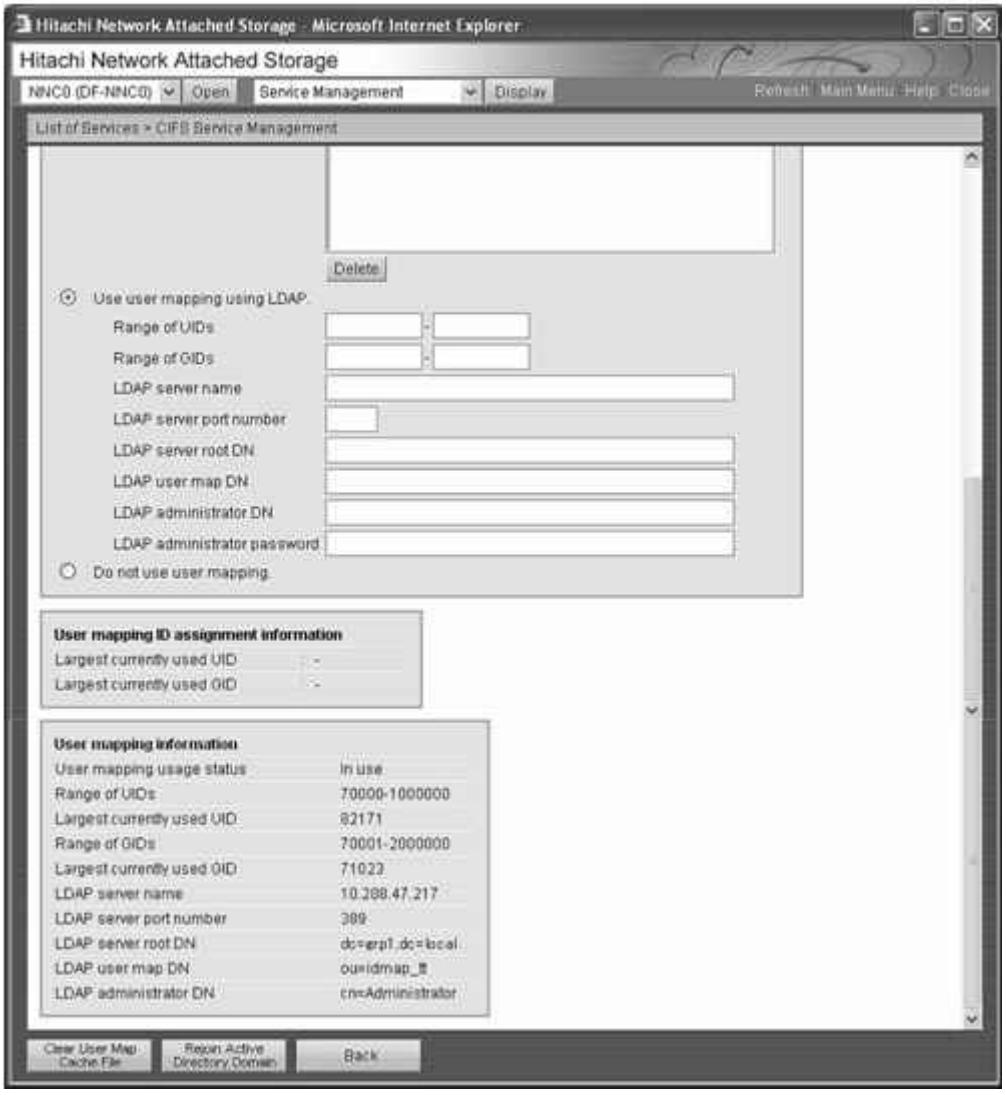



**Figure 4.34 CIFS Service Maintenance window (when user mapping uses LDAP)**

**Table 4.21 User Mapping in CIFS Service Maintenance window (when mapping uses LDAP)**

| Item | Description |
|---|---|
| **Range of UIDs** | Displays the range of user IDs mapped by using LDAP. |
| **Largest currently used UID** | Displays the largest user ID within the range of user IDs that have already been assigned in the NAS Modular system.<br>Depending on the status of user mapping usage, the following information might be displayed:<br>`Not used, or less than the minimum UID used.`<br>Displayed when no user IDs have been assigned, or the smallest assigned user ID is smaller than the minimum value set in **Range of UIDs**.<br>`Cannot be got from LDAP server. Check the LDAP server settings and CIFS service configuration in service.`<br>Displayed when the largest ID could not be acquired from the LDAP server for user mapping. Check the user mapping settings and the operating status of the LDAP server. |
| **Range of GIDs** | Displays the range of group IDs mapped by using LDAP. |
| **Largest currently used GID** | Displays the largest group ID within the range of group IDs that have already been assigned in the NAS Modular system.<br>Depending on the status of user mapping usage, the following information might be displayed:<br>`Not used, or less than the minimum GID used.`<br>Displayed when no group IDs have been assigned, or the smallest assigned group ID is smaller than the minimum value set in **Range of GIDs**.<br>`Cannot be got from LDAP server. Check the LDAP server settings and CIFS service configuration in service.`<br>Displayed when the largest ID could not be acquired from the LDAP server for user mapping. Check the user mapping settings and the operating status of the LDAP server. |
| **LDAP server name** | Displays the host name or IP address of the LDAP server. |
| **LDAP server port number** | Displays the port number of the LDAP server. |
| **LDAP server root DN** | Displays the identification name of the LDAP server root in DN format. |
| **LDAP user map DN** | Displays the identification name for which you added the user mapping account of the LDAP server in DN format. |
| **LDAP administrator DN** | Displays the identification name of the LDAP server administrator in DN format. |

### 4.6.4.2 Deleting Cached User Mapping Information from the CIFS Service Environment

Using the **CIFS Service Maintenance** window, shown below, you must delete the cached user mapping information from the CIFS service environment when one of the following conditions applies:

- Space on the system disk is depleted when the amount of information about the deleted users increases, and a large amount of unnecessary user information remains on the NAS Modular system (in an environment where user mapping is used).
- You reconfigure the user mapping environment for the LDAP server that is managing user information.

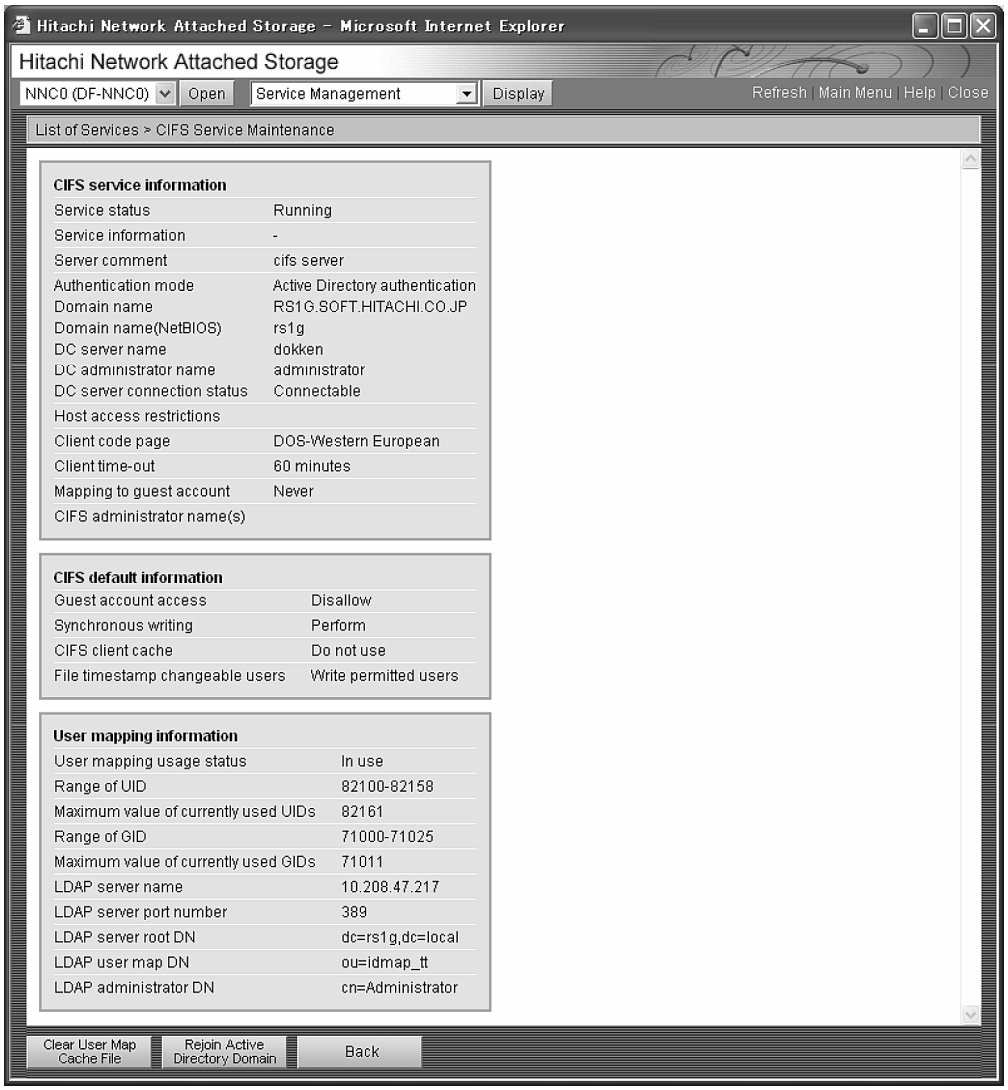



**Figure 4.35 CIFS Service Maintenance Window**

To delete the cached user mapping information from the CIFS service environment:

1. Click the **Service Management** button in the **Main Menu** window.

   The **List of Services** window displays. For window details, see section 4.6.1.

2. Select the **cifs_service** radio button and then click the **Service Maintenance** button. The **CIFS Service Maintenance** window displays and displays the following information:
   - In **DC server connection status**, the connection status for the server authenticating users is displayed. If a connection can be made, **connectable** is displayed.
   - The item name for DC server connection status varies depending on the authentication mode of the CIFS service. If NT domain authentication or Active Directory® authentication is used, the item name is **DC server connection status**. If NT server authentication is used, the item name is **Authentication server connection status**.

3. Click the **Clear User Map Cache File** button. The cached user mapping information is deleted.

#### 4.6.4.3 Rejoining the CIFS Service to the Active Directory Domain

When the Active Directory authentication for the CIFS service authentication mode is selected, if an error occurs in the domain controller or the domain configuration has been changed, you might not be able to connect a CIFS share. In such a case, rejoin the NAS Unit to the Active Directory® domain to recover the CIFS connection.

To rejoin the CIFS service to the Active Directory® domain:

1. Click the **Service Management** button in the **Main Menu** window.

   The **List of Services** window displays. For window details, see section 4.6.1.

2. Select the **cifs_service** radio button and then click the **Service Maintenance** button.

   The **CIFS Service Maintenance** window displays. For window details, see section 4.6.4.1.

3. Click the **Rejoin Active Directory Domain** button.

   The selected CIFS service is rejoined to the Active Directory® domain.

   If the selected CIFS service cannot be rejoined to the Active Directory® domain, manually delete the computer account left on the Active Directory® domain, then rejoin the CIFS service to the Active Directory® domain.

### 4.6.5 Changing the SSH Service Configuration (Registering a Public Key)

You can use the NAS Manager to change the configuration definitions of the SSH service: for example, the registration and deletion of a public key. Before modifying the configuration definitions of the SSH service, you must modify the service configuration definition of each NAS Unit equally to avoid any inconsistency among NAS Units in a cluster.

Before registering a public key, review the following items:

- Use a key creation tool to create the keys (private key and public key) that are used in the SSH authentication. For details on how to install the relevant software and create those keys, see the documentation provided with the software.
- The passphrase specified when creating the keys is used as the SSH **Login** password. Although you can skip specifying a passphrase, we recommend that you specify the passphrase for security purposes.
- If a public key is created in the machine where the NAS Manager is not available, prepare the public key in the machine where you can use the NAS Manager by, for example, transferring it with FTP, or copying it to another record medium.

When registering a public key, use the **NAS Manager** (Add Public Key window). The public key is registered for the SSH account `nasroot`.

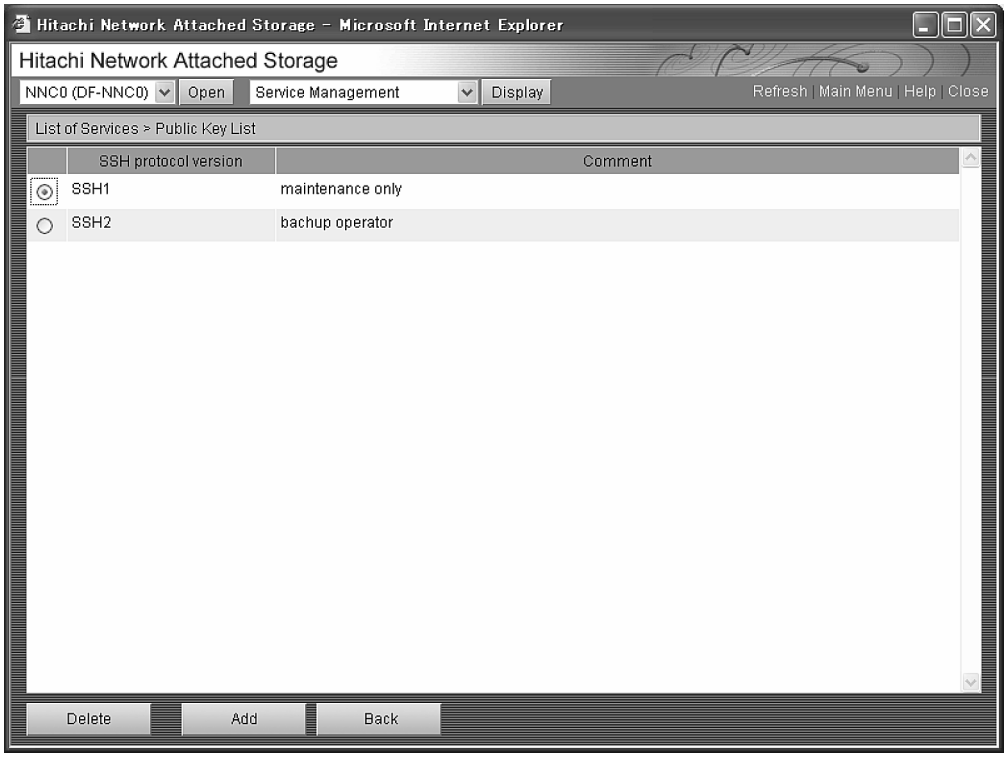



**Figure 4.36 Public Key List Window**

Make sure that there are no more than 128 public keys per node for the protocol (SSH1 and SSH2).

### 4.6.5.1 Registering a Public Key

To register a public key:

1. In the **Main Menu** window, click the **Service Management** button.

   The **List of Services** window displays.

2. Use a radio button to select `ssh_service`, and then click the **Modify Configuration** button.

   The **Public Key List** window displays. Following is a description of the information that is displayed in the **Public Key List** window:

   - **SSH protocol version** of the SSH protocol.
   - **Comment** Notes about the public key.

3. Click the **Add** button.

   The **Add Public Key** window displays.

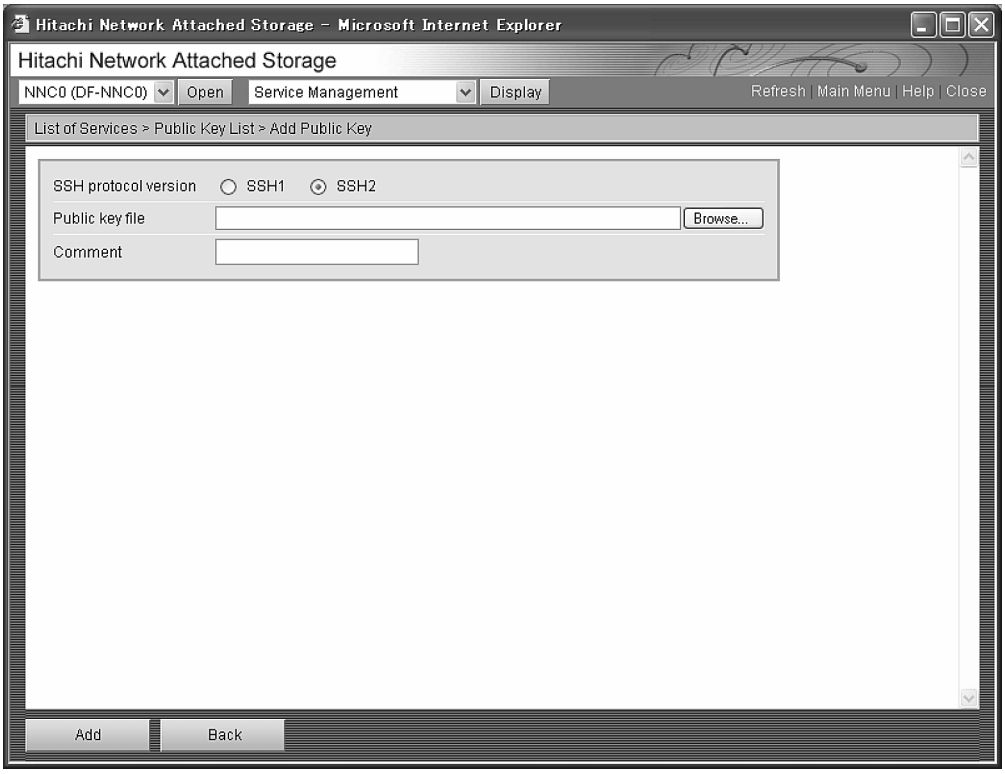



**Figure 4.37 Add Public Key Window**

4. Enter the required information as described in Table 4.22, then click the **Add** button.

   The configuration definitions for the SSH service change and the **Public Key List** window re-displays.

   The following table lists and describes the information to be specified in the **Add Public Key** window:

**Table 4.22 Information Specified in Add Public Key Window**

| Item | Description |
|---|---|
| **SSH protocol version** | Use a radio button to select the SSH protocol version:<br>**SSH1**<br>Select this to set SSH1. |

| Item | Description |
|---|---|
| | The authentication method is RSA.<br>**SSH2**<br>Select this to set SSH2.<br>The authentication methods are RSA and DSA. |
| **Public key file** | Specify the path to the public key file.<br>The maximum size of the public key file is 1 KB.<br>To select a file name through browsing, click the **Browse** button. |
| **Comment** | Enter a comment about the public key.<br>Enter a maximum of 32 characters.<br>You can use alphanumeric characters and hyphens (-).<br>You can also specify spaces, but not at the beginning or end of the character string. |

### 4.6.5.2 Deleting a Public Key

To delete a public key:

1. In the **Main Menu** window, click the **Service Management** button.
   The **List of Services** window displays. For window details, see section 4.6.1.
2. Use a radio button to select `ssh_service`, then click the **Modify Configuration** button.
   The **Public Key List** window displays. For window details, see section 4.6.5.
3. Use a radio button to select the public key to be deleted, then click the **Delete** button.
   A dialog box confirms that you want to delete the public key.
4. Click the **OK** button.
   The selected public key is deleted.

### 4.6.6 Changing the FTP Service Configuration

You can use the **FTP Service Management** window (shown below) to change the configuration definitions of the FTP service. If the FTP service is used from the client, the service IP address is used for connection.

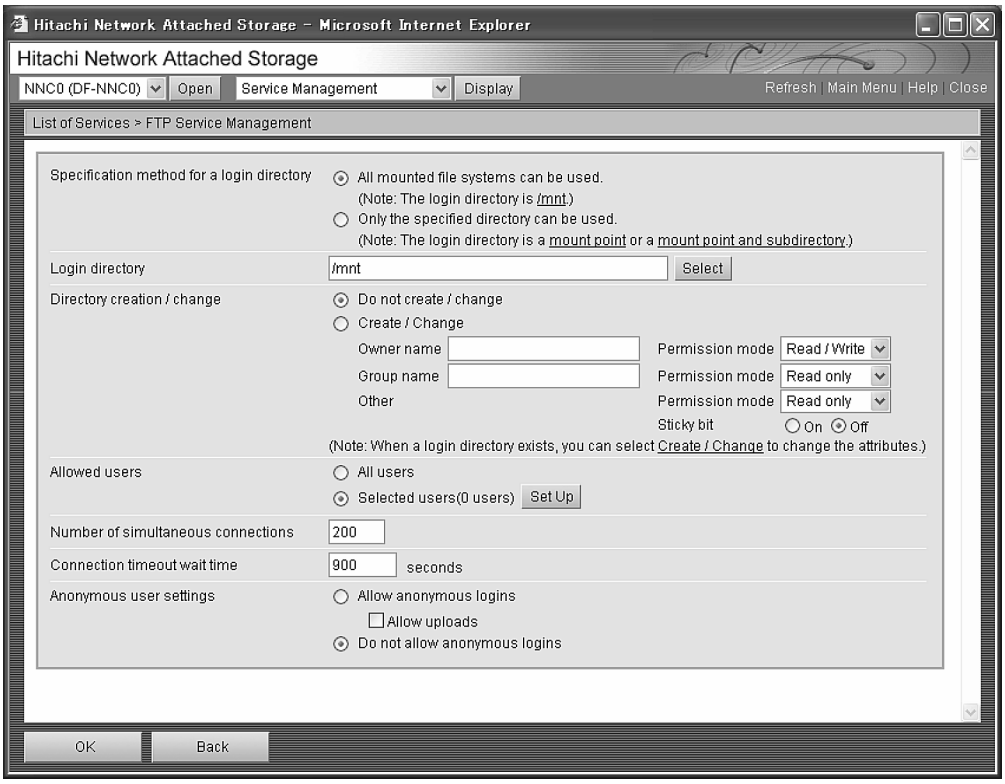



**Figure 4.38 FTP Service Management Window**

Before you change the FTP service configuration, complete the following items:

- When you change the configuration definitions of the FTP service, anonymous users are allowed to log in by using the FTP service. If an anonymous user logs in to the FTP service, the name ftp is used for the user name and group name.

  If an update installation is performed for NAS OS or NAS Manager, and a user with the name ftp used NAS Manager to register, the service might then be used by an anonymous FTP-service user. To give an anonymous user permission to log in to the FTP service, change or delete the user name and group name registered as ftp in the NAS Modular system before updating NAS OS or NAS Manager, and then perform the update installation. If the names are changed or deleted after performing an update installation of NAS OS or NAS Manager, the NAS Modular system must be restarted.

- In the NAS Modular system, the service does not automatically restart even when the configuration definitions of the FTP service have been changed. If the configuration definitions of the FTP service have been changed, restart the service by clicking the **Start** or **Restart** button in the **List of Services** window.

- Even if NAS OS is restarted after the configuration definitions of the FTP service are changed, the changed configuration definitions are not applied. Restart the service.
- If you change the configuration definitions of the FTP service while a client is updating the file system, the client operation might not finish normally. Therefore, contact users beforehand.
- When the `chmod` command is executed on an FTP client for a file or directory for which an ACL is set, the ACL settings might become invalid. In this case, set the ACL again.

### 4.6.6.1 Changing the FTP Service Configuration

To change the configuration of the FTP service:

1. In the **Main Menu** window, click the **Service Management** button.

   The **List of Services** window displays. For window details, see section 4.6.1.

2. Use a radio button to select `ftp_service`, and then click the **Modify Configuration** button.

   The **FTP Service Management** window displays.

3. Enter the required information, then click the **OK** button. The configuration definitions of the FTP service change and the **List of Services** window re-displays.

   The following table displays the information to be specified in the **FTP Service Management** window:

**Table 4.23 Contents of FTP Service Management Window**

| Item | Description |
|---|---|
| **Specification method for a login directory** | Select the method of setting a directory to which the users can log in by using the FTP service.<br>**All mounted file systems can be used.**<br>Log in to the `/mnt` directory. This setting allows use of all file systems mounted on each node. In this case, both nodes can use the FTP service.<br>**Only the specified directory can be used.**<br>Log in to a specified file system or directory. This setting limits the accessible range to the specified file system or node. In this case, only one node can use the FTP service. |

| Item | Description |
|---|---|
| **Login directory** | Specify the directory to which the users can log in by using the FTP service.<br>The system assumes `/mnt` if you select **All mounted file systems can be used** for **Specification method for a login directory**. If you select **Only the specified directory can be used**, specify the path name of any file system or directory you want to use as the **Login** directory.<br>Clicking the **Select** button displays the **List of Mounted File Systems** window. In this window, select the directory to be accessed using the FTP service, or enter its name directly in the text box. When you select a directory in the **List of Mounted File Systems** window, see 4.6.6.2.<br>When you create a **Login** directory for the FTP service, the directory name must be unique within the cluster. Make sure that you use an absolute path to specify the directory. You cannot specify a path including a symbolic link.<br>You can use any alphanumeric character, hyphen (`-`), period (`.`), forward slash (`/`), and underscore (`_`).**Login directory** is case-sensitive.<br>▪ When sharing a directory of the file system:<br>`/mnt/`*`name-of-mounted-file-system/path-name`*<br>***Example***: `/mnt/filesystem01/ftp1`<br>▪ When sharing the whole of each file system:<br>`/mnt/`*`name-of-mounted-file-system`*<br>***Example***: `/mnt/filesystem02` |

| Item | Description |
|---|---|
| **Directory creation/change** | Use a radio button to select whether to create a new directory if the directory specified in **Login directory** does not exist. If the directory has been created, you can change the properties for the specified directory.<br>If the directory specified in **Login directory** has already been created, and you want to use the directory without change, select **Do not create/change**. The system assumes **Do not create/change** if the specification of **Login directory** is `/mnt`.<br>To create a new directory, or to change the attributes of a directory already created, select **Create/Change**. When you select **Create/Change**, select or enter the following items:<br>**Owner**<br>Specify the user name or user ID of the directory owner.<br>**Group**<br>Specify the group name or group ID of the owner's group.<br>**Permission mode**<br>From the drop-down list, select the access permission for the directory owner, owner's group, and others.<br>**Read/Write**<br>Select this mode to grant both read and write permissions. The directory execution permission is granted.<br>**Read only**<br>Select this mode to grant read permission only. The directory execution permission is granted.<br>**None**<br>Select this mode when neither the read and write permissions nor the directory execution permission is granted. This mode is available for **Group** and **Other**.<br>**Sticky bit**<br>Permit only the owner of the directory to delete or rename the files or directories under that directory.<br>Use a radio button to select whether to set a sticky bit for the directory.<br>**On**<br>Set a sticky bit.<br>**Off**<br>Do not set a sticky bit. |
| **Allowed users** | Specify the users to log in by using the FTP service.<br>**All users**<br>Allow all users to log in by using the FTP service.<br>Select this item if you want to allow the users registered by user mapping to log in to the FTP service.<br>**Selected users**<br>Allow the specified users to log in by using the FTP service. Clicking the **Set Up** button displays the **Select FTP Users** window. In this window, select the users to log in by using the FTP service. You can select a maximum of 2,000 users.<br>For details on how to select the users in the **Select FTP Users** window, see section 4.6.6.3.<br>This item name is followed by the number of users currently allowed to log in, using the **Selected users(***number-of-users* **users)** format. |
| **Number of simultaneous connections** | Specify the number of uses who can concurrently log in to the FTP service.<br>Specify a number in the range from 10 to 500. The default is `200`. |

| Item | Description |
|---|---|
| **Connection timeout wait time** | Specify the timeout for an automatic logout (unit: seconds). If no operation is performed within the timeout period after an FTP client logged in to the NAS Modular system, the FTP client is logged out automatically.<br>Specify a number in the range from 30 to 43,200. The default is 900. |
| **Anonymous user settings** | Use a radio button to select whether to allow anonymous users to log by using the FTP service.<br>**Allow anonymous logins**<br>Select this to grant anonymous users permission to log by using the FTP service. Anonymous users can use the FTP service with the ftp user (UID=97) and ftp group (GID=97) permissions.<br>**Allow uploads**<br>When you select **Allow anonymous logins**, use a check box to specify whether or not to allow anonymous users to upload data.<br>**Do not allow anonymous logins**<br>Do not allow anonymous users to log in by using the FTP service. |

Check the following when you set a directory to which users log in by using the FTP service:

- You should select All mounted file systems can be used for Specification method for a **Login** directory, so that the file systems in both nodes are available. Select Only the specified directory can be used if you want to limit the file system or directory to be used.
- To continue the service if a failover occurs, you must make sure that the FTP service settings are the same for both nodes and that the FTP services are running on both nodes If you select Only the specified directory can be used, the FTP service can only be used on the node where the file system is mounted, because the file system or directory to be specified for the **Login** directory exists only in that node.

  The **List of Mounted File Systems** window only displays the file system contained in the node to which you have logged in. With Only the specified directory can be used selected, you can click the Select button for **Login** directory to display the **List of Mounted File Systems** window. In this window, you select the **Login** file system for the FTP service. In this case, you must also directly enter a path for **Login** directory for the other node.

  You cannot create a file system or directory having the same path in both nodes. This means that even if you specify a directory for **Login** directory for either node and then create or change a directory with Create/Change selected for Directory creation/change, you must select Do not create/change for the other node.
- If you log in by using the FTP service and use a command, the directory specified in **Login** directory is used as the root directory.

### 4.6.6.2 Selecting a File System for Login by using the FTP Service

In the **List of Mounted File Systems** window, shown below, you can select a file system to which users can log in by using the FTP service.

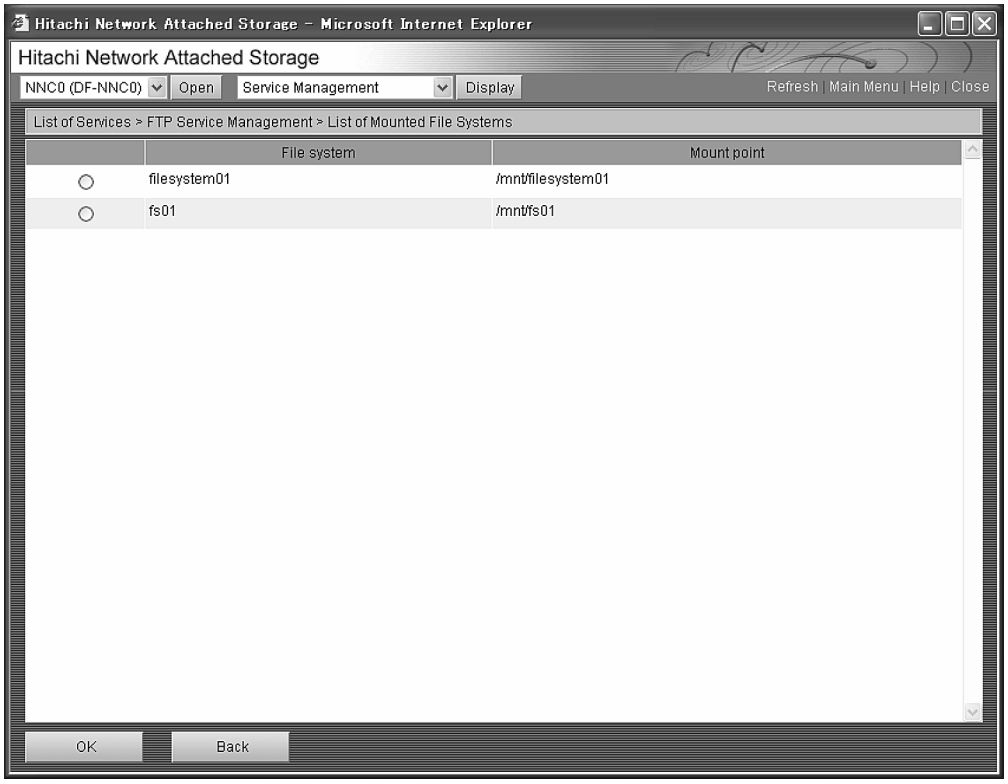



**Figure 4.39 List of Mounted File Systems Window**

The above **List of Mounted File System** window is used when file system is selected for **Login** by using the FTP service.

To select a file system to which the users can log in to the FTP service:

1. In the **Main Menu** window, click the **Service Management** button.

   The **List of Services** window displays. For window details, see section 4.6.6.

2. Use a radio button to select ftp_service, and then click the **Modify Configuration** button.

   The **FTP Service Management** window displays. For window details, see section 4.6.6.

3. To select a mount point for a **Login** directory for the FTP service (mount point or subdirectories), click the Select button for **Login** directory.

   The **List of Mounted File Systems** window displays.

4. From the list of the mounted file systems, use a radio button to select the file system allowed for **Login** to the FTP service, and then click the **OK** button.

The **FTP Service Management** window re-displays. In **Login** directory of the **FTP Service Management** window, the mount point of the selected file system appears. To allow access to directories under the file system, enter the directories following the displayed mount point.

### 4.6.6.3 Allowing Users to Log into the FTP Service

In the **Select FTP Users** window, shown below, you can select users to be allowed to log into the FTP service.

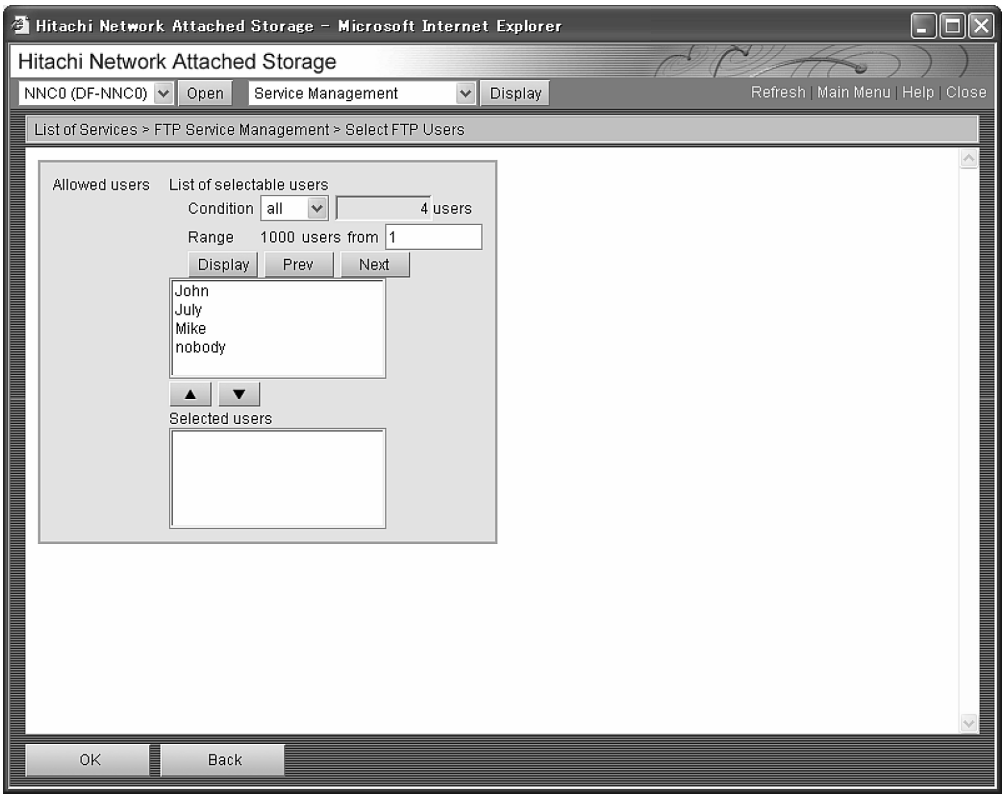



**Figure 4.40 Select FTP Users Window**

To select users to be allowed to log in to the FTP service:

1. In the **Main Menu** window, click the **Service Management** button.

   The **List of Services** window displays. For window details, see section 4.6.6.

2. Use a radio button to select ftp_service, and then click the **Modify Configuration** button.

   The **FTP Service Management** window displays. For window details, see section 4.6.6.

3. To select, from a list of users, the users to be allowed to log in to the FTP service, click the **Setup** button for **Allowed users**.

   The **Select FTP Users** window displays. Following is a description of the window's contents:

**List of selectable users**: From the List of selectable users list box, select the users who will use the FTP service. To narrow down the users to be displayed, select the users from the Condition drop-down list, and then click the **Display** button:

- **all** Displays all user names.
- **a** to **z**, **A** to **Z**, or **0** to **9** Displays user names that begin with the selected alphanumeric character.
- **other** Displays user names that begin with a character other than an alphanumeric.

  The total number of filtered users is shown on the right side of the **Condition** drop-down list. A maximum of 1,000 users can be displayed at the same time in the **List of selectable users** list box. If the number of users exceeds 1,000, you can use the following methods to specify the users to be displayed.
- **Range** text box. Displays initially the sequence number of the user who is displayed at the beginning of the **List of selectable users** list box.

  Specify a value equal to or less than the total number of filtered users, and then click the **Display** button. This displays 1,000 users, beginning with the user whose sequence number you specified.

  If you then select a different filter from the **Condition** drop-down list and click the **Display** button, the value specified in the **Range** text box is ignored and users are displayed beginning with the first user.
- **Prev** button. Clicking this button displays in sequential order the users preceding the user displayed at the beginning of the **List of selected users** list box. If the user displayed at the beginning of the **List of selected users** list box is the first user, or if the total number of filtered users is 0, an error message appears when you click the **Prev** button.
- **Next** button. Clicking this button displays in sequential order the users following the user displayed at the end of the **List of selected users** list box. If the user displayed at the end of the **List of selected users** list box is the last user, or if the total number of filtered users is 0, an error message appears when you click the **Next** button.
- Select a user, and then click the ▼ button to add that user to the **Selected users** list box. Only users listed in the **Selected users** list box are set as users with the designated access permission.
- To delete a user from the **Selected users** list box, select the user and click the ▲ button.

4. Specify the required information, and then click the **OK** button.

   The users are added, and the **FTP Service Management** window re-displays.

### 4.6.7 Starting, Stopping, or Restarting a Service

In the **List of Services** window, you can stop, start, and restart services. ***Note:*** Start control is not possible for the SSH service.

To start, stop, or restart a service:

1. In the **Main Menu** window, click the **Service Management** button.

   The **List of Services** window displays. For window details, see section 4.6.1.

2. Use a radio button to select the service, then click the appropriate button:
   - Start
   - Stop
   - Restart

   A dialog box confirms your selection.

3. Click the **OK** button.
   - If you clicked Start, the service starts and **Status** changes to `Running`.
   - If you clicked Stop, the service stops and **Status** changes to `stopped`.
   - If you clicked Restart, the service restarts and **Status** changes to `Running`.

## 4.7 System Setup

From the **System Setup Menu** window, shown below, you must set or change the interface information, the network information, and the server information to be viewed on each NAS Unit as required.

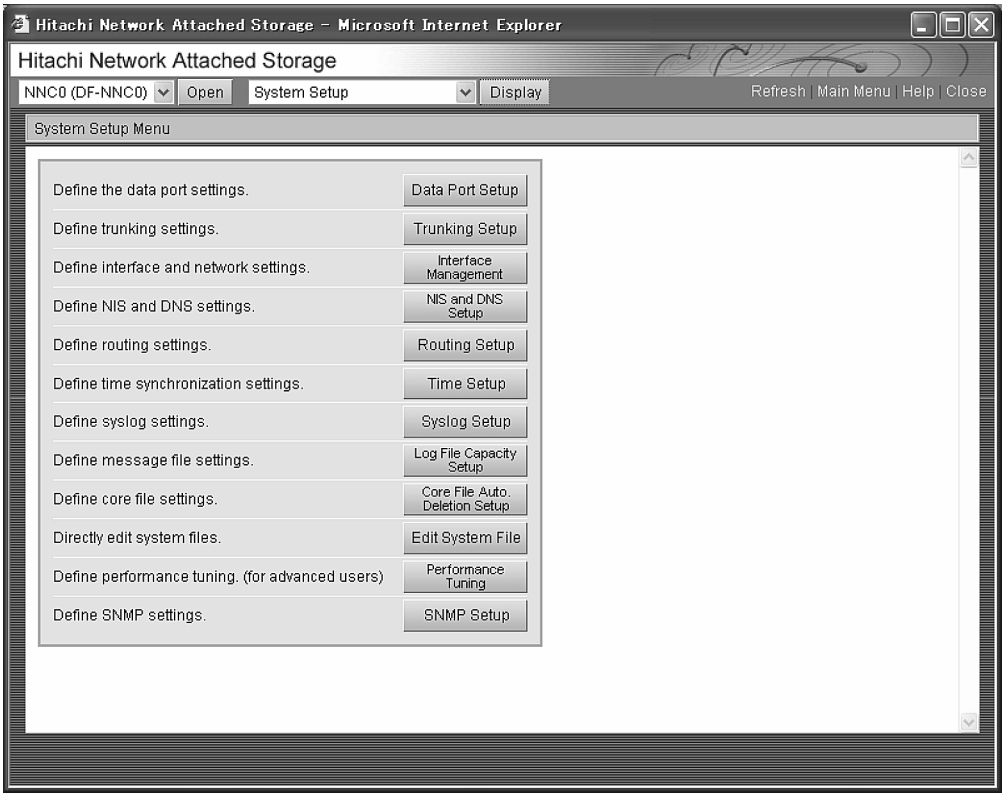



**Figure 4.41 System Setup Menu Window**

You can set the following information from the **System Setup Menu** window:

- Data LAN Port Settings
- Trunking Settings
- Interface and Network Information[#1]
- DNS server, NIS server, and LDAP server for user authentication settings[#2]
- Routing Information[#1]
- Time Settings
- Syslog Transfer Destinations
- Log File Size
- Core File Storage Period
- System File Editing
- File System **Performance Tuning**
- SNMP Settings
- User interface mode

#1:

Interface, network, and routing information needs to be set while taking the association with one another into consideration.

#2:

When use of the LDAP server for user authentication is started or stopped, the NAS OS must be restarted on both NAS Units in the cluster (either immediately or later).

The following describes how to perform system setup by using an example of setting interface, network, and routing information for gbe4. This example does not use a tagged VLAN.

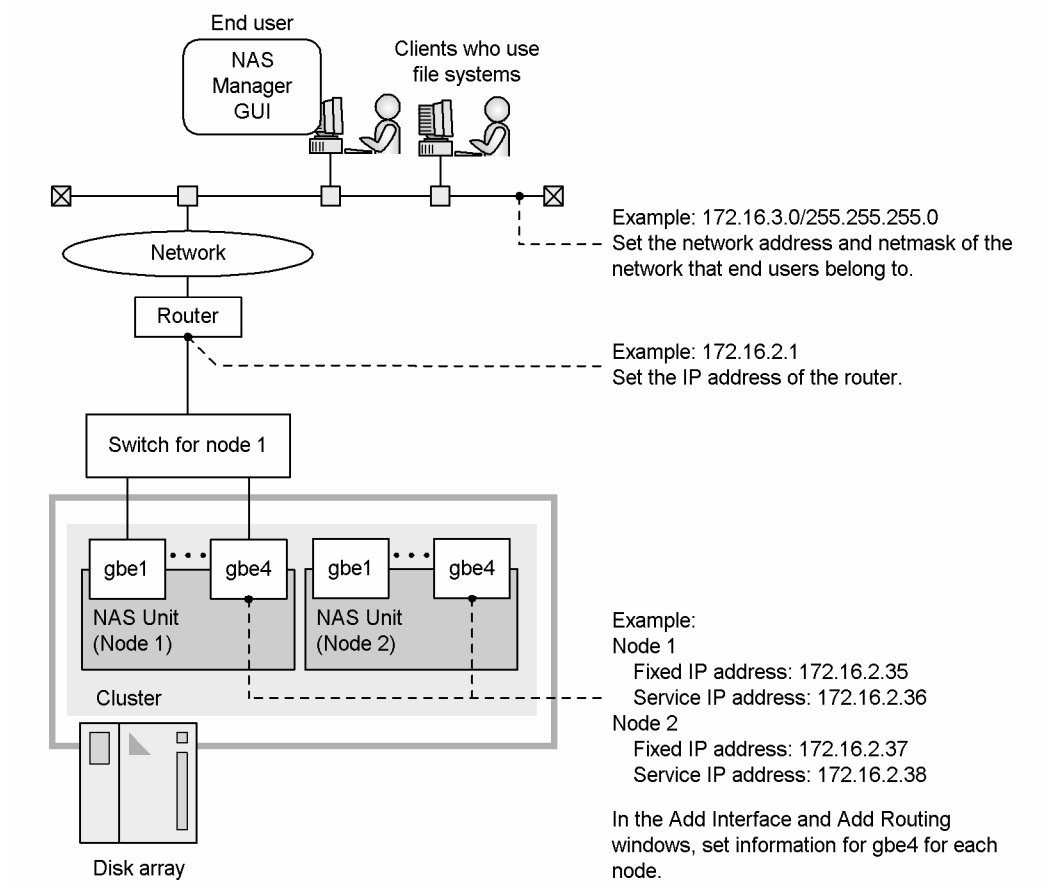



**Figure 4.42 Setting Interface, Network, and Routing Information for gbe4**

The information to be set in the **Add Interface** and Add Routing windows is described in the following table.

**Table 4.24 Add Interface and Add Routing Windows Information**

| Window | Item | Example of Specified Information |
|---|---|---|
| **Add Interface window** | **Port** | Select **gbe4** from the drop-down list. |
| | **Tagged VLAN** | Select the radio button for **Do not use**, because a tagged VLAN is not used. |
| | **Fixed IP address** | For Node 1:<br>Specify `172.16.2.35`.<br>For Node 2:<br>Specify `172.16.2.37`. |
| | **Service IP address** | For Node 1:<br>Specify `172.16.2.36`.<br>For Node 2:<br>Specify `172.16.2.38`. |
| | **Netmask** | Specify `255.255.255.0`. |
| | **MTU** | Specify `1500`. |

| Window | Item | Example of Specified Information |
|---|---|---|
| **Add Routing window** | **Interface** | Select **gbe4** from the drop-down list. |
| | **How to specify target** | Select the **Network** radio button. |
| | **Target** | Specify `172.16.3.0` (the address of the network that end users belong to). |
| | **Netmask** | Specify `255.255.255.0` (the netmask for the address of the network that end users belong to). |
| | **Gateway** | Specify `172.16.2.1` (the IP address of the router). |
| | **Method of specifying route** | Select the **Allow** radio button. |
| | **MSS** | Do not specify. |

For details about information specified in the **Add Interface** window, see section 4.7.4.3. For details about information specified in the Add Routing window, see section 4.7.6.2.

The following subsections explain how to set system information.

## 4.7.1 Setting Data LAN Ports

You can check the communication status and can change the data port negotiation mode for a data LAN port.

### 4.7.1.1 Before Changing the Negotiation Mode

Before changing the negotiation mode for a data LAN port, you must stop the node for the port. For details on how to do this, see section 4.5.5.

Also, before changing the negotiation mode for a data LAN port, the negotiation mode for the connected switch must be checked. If a negotiation mode different from the negotiation mode for the switch is set, a linkage error that prevents communication may occur. The following table describes the network communication status when the negotiation modes for a data LAN port and the connected switch are different:

**Table 4.25 Checking Negotiation Modes**

| Negotiation mode for a data LAN port | Negotiation mode for the connected switch | Resulting network communication status |
|---|---|---|
| Auto | Auto:<br>▪ 100Base half duplex<br>▪ 100Base full duplex | 100Base full duplex#1 |
| | Auto:<br>▪ 1000Base half duplex<br>▪ 1000Base full duplex | 1000Base full duplex#1 |

| Negotiation mode for a data LAN port | Negotiation mode for the connected switch | Resulting network communication status |
|---|---|---|
| | Auto:<br>▪ 100Base half duplex<br>▪ 1000Base half duplex | 1000Base half duplex[1] |
| | Auto:<br>▪ 100Base full duplex<br>▪ 1000Base full duplex | 1000Base full duplex[1] |
| | Auto negotiation mode<br>▪ 100Base half duplex<br>▪ 100Base full duplex<br>▪ 1000Base half duplex<br>▪ 1000Base full duplex | 1000Base full duplex[1] |
| | 100Base half duplex | 100Base half duplex |
| | 1000Base half duplex | 1000Base half duplex |
| | 100Base full duplex | Communication impossible[2] |
| | 1000Base full duplex | Communication impossible[2] |
| 100Base half duplex | 100Base half duplex | 100Base half duplex |
| 100Base full duplex | 100Base full duplex | 100Base full duplex |
| 1000Base full duplex | 1000Base full duplex | 1000Base full duplex |
| 100Base half duplex | Auto | Communication is impossible if the port and switch do not use the same communication rate and method[#2] |
| 100Base full duplex | | |
| 1000Base full duplex | | |

***Note 1:*** Depending on the switch type, a problem with communication may occur even though the auto negotiation mode is set for both the port and switch.

***Note 2:*** When one of the connected devices uses auto negotiation mode and the other uses the half duplex or full duplex method, the device in auto negotiation mode uses the half duplex method. At this time, if the other device uses the full duplex method, communication between the devices may be impossible because the negotiation modes do not match. Even if communication is possible, the throughput and response may degrade.

If communication is impossible because the negotiation modes do not match, check whether the negotiation modes for the data LAN port and the connected switch are the same. For details on how to check the negotiation mode of the data LAN port, see section 4.7.1.2.

If the negotiation modes are the same, the problem may pertain to a hardware error. Contact your HDS representative if necessary.

### 4.7.1.2 Checking the Communication Status for a Data LAN Port

To check the communication status for a data LAN port:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window appears. For details on this window, see section 4.7.

2. Click the **Data Port Setup** button.

   The **List of Data Ports** window appears.

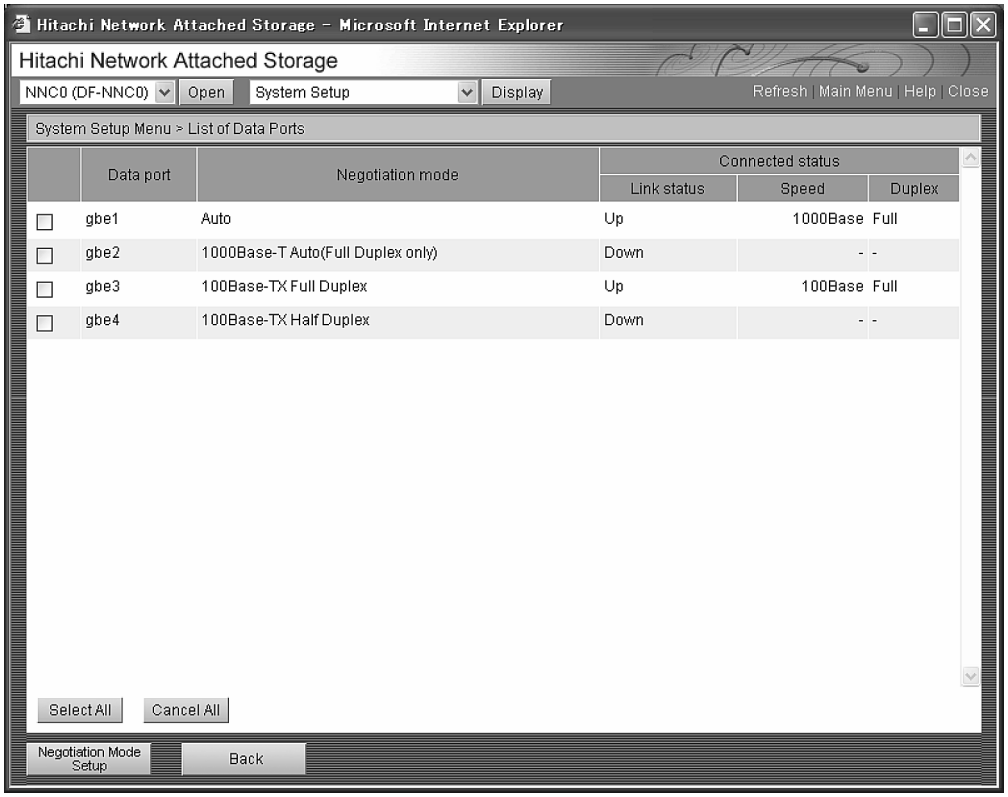



**Figure 4.43 List of Data Ports window**

The following table lists and describes the information displayed in the **List of Data Ports** window:

**Table 4.26 Information Displayed in the List of Data Ports Window**

| Item | Description |
|---|---|
| **Data port** | Displays data LAN port names (`gbe1` to `gbe4`). |
| **Negotiation mode** | Displays the negotiation mode for a specific data LAN port:<br>`Auto`<br>This is displayed when the auto negotiation mode is used for communication.<br>`1000Base-T Auto (Full Duplex only)`<br>This is displayed when 1000Base-T full duplex communication is used.<br>`100Base-TX Full Duplex`<br>This is displayed when 100Base-TX full duplex communication is used.<br>`100Base-TX Half Duplex`<br>This is displayed when 100Base-TX half duplex communication is used. |
| **Connected status** | Displays the communication status for a data LAN port:<br>**Link status**<br>Displays the link status.<br>`Up`<br>This is displayed when the link is connected normally.<br>`Down`<br>This is displayed when the link is disconnected. Check the negotiation mode of the switch connected to the data LAN port, and then re-set the negotiation mode.<br>`Error`<br>This is displayed when the link cannot be recognized. If this is displayed, an error may have occurred in the NAS Modular system. Download all log files for operation management, and contact your HDS representative. For details on how to download log files, see 4.13.10.<br>**Speed**<br>Displays the current communication rate:<br>`1000Base`<br>This is displayed when communication is being performed with 1000Base.<br>`100Base`<br>This is displayed when communication is being performed with 100Base.<br>`10Base`<br>This is displayed when communication is being performed with 10Base. The 10Base is not a recommended communication rate. Check and, if necessary, correct the setting of the connected switch so that the communication rate is 100Base or greater.<br>`-`<br>This is displayed when communication is not being performed (**Link status** is `Down`).<br>**Duplex**<br>Displays the current communication method.<br>`Full`<br>This is displayed when full duplex communication is used.<br>`Half`<br>This is displayed when half duplex communication is used.<br>`-`<br>This is displayed when communication is not being performed (**Link status** is `Down`). |

### 4.7.1.3 Changing the Negotiation Mode for a Data LAN Port

To change the negotiation mode for a data LAN port:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window appears. For details on this window, see Figure 4.41.

2. Click the **Data Port Setup** button.

   The **List of Data Ports** window appears. For details on this window, see 4.7.1.2.

3. Select the check box for the data LAN port for which you want to change the negotiation mode, and then click the **Negotiation Mode Setup** button.

   The **Negotiation Mode Setup** window for the selected data LAN port appears.

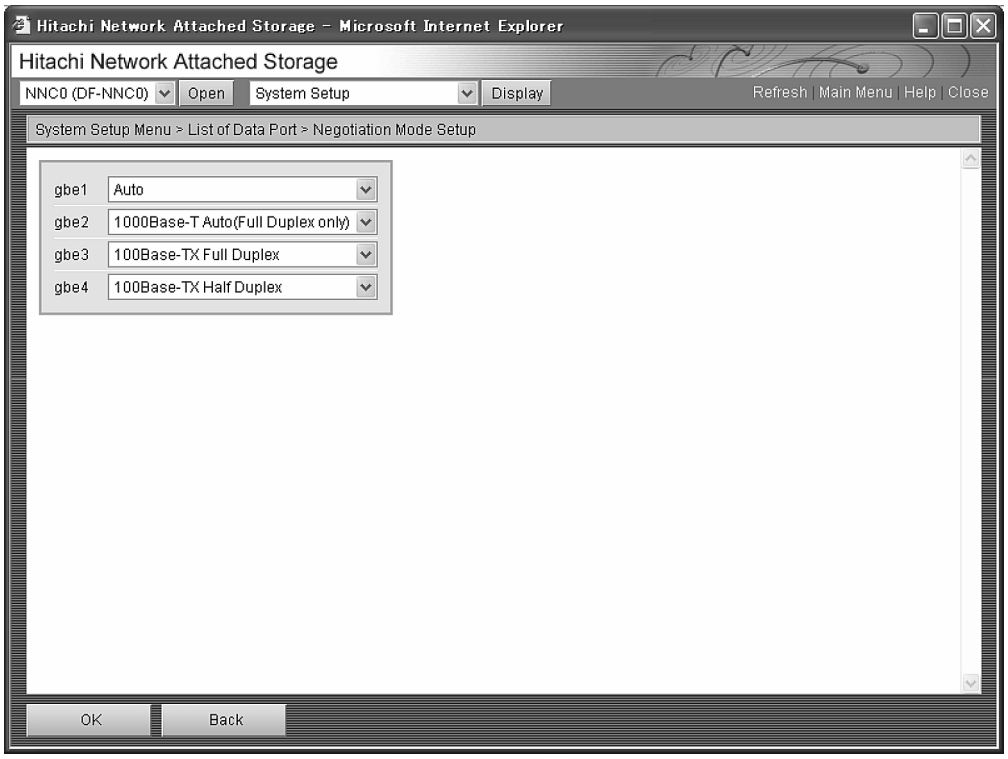



**Figure 4.44 Negotiation Mode Setup Window**

4. Specify information as required, and then click the **OK** button.

   The negotiation mode is set and the **List of Data Ports** window appears again.

**Table 4.27 Information to be specified in the Negotiation Mode Setup window**

| Item | Description |
|---|---|
| **gbe1**, **gbe2**, **gbe3**, and **gbe4** | Select the negotiation mode for each data LAN port from the drop-down list for the port:<br>**Auto**<br>Select this to use the auto negotiation mode for communication.<br>**1000Base-T Auto (Full Duplex only)** |

| Item | Description |
|---|---|
| | Select this to use 1000Base-T full duplex communication.<br>**100Base-TX Full Duplex**<br>Select this to use 100Base-TX full duplex communication.<br>**100Base-TX Half Duplex**<br>Select this to use 100Base-TX half duplex communication. |

### 4.7.2 Setting Up Trunking

You can set or release trunking.

We recommend that cascaded trunking be used for NAS Modular systems. When you set cascaded trunking, set link aggregation in the **Link Aggregation Setup** window first. Then, set link alternation by using the port for which link aggregation was set in the **Link Alternation Setup** window and a port for which trunking has not been set. For details on trunking configuration, see section 2.3.1.

You must stop stop the cluster as well as the resource groups on both nodes before performing any of the following trunking operations during operation of the NAS Modular system:

- Specifying the settings for link aggregation, or editing information on link aggregation
- Specifying the settings for link alternation, or editing information on link alternation
- Specifying the settings for cascaded trunking, or editing information on cascaded trunking
- Releasing trunking

For details on how to stop a resource group, see section 4.5.8. For details on how to stop a cluster, see section 4.5.4.

After you finish the operation, start the cluster as well as the resource groups on both nodes.

If trunking is set during operation of the NAS Modular system, the system automatically deletes the interface information (including VLAN settings) and routing information set for the data LAN port selected as the trunking target. If trunking is released, the system automatically deletes the interface information (including VLAN settings) and routing information set for the port for which trunking is to be released. If you have changed trunking settings, review the interface information, routing information, and VLAN settings.

### 4.7.3 Viewing Trunking Information

You can view trunking information in the **List of Trunking Configurations** window. When you have restarted a resource group, remember to check the trunking status in this window.

To view trunking information:

1. In the **Main Menu** window, click the System Setup button.

   The **System Setup Menu** window appears. For details on this window, see section 4.7.

2. Click the **Trunking Setup** button.

   The **List of Trunking Configurations** window appears.

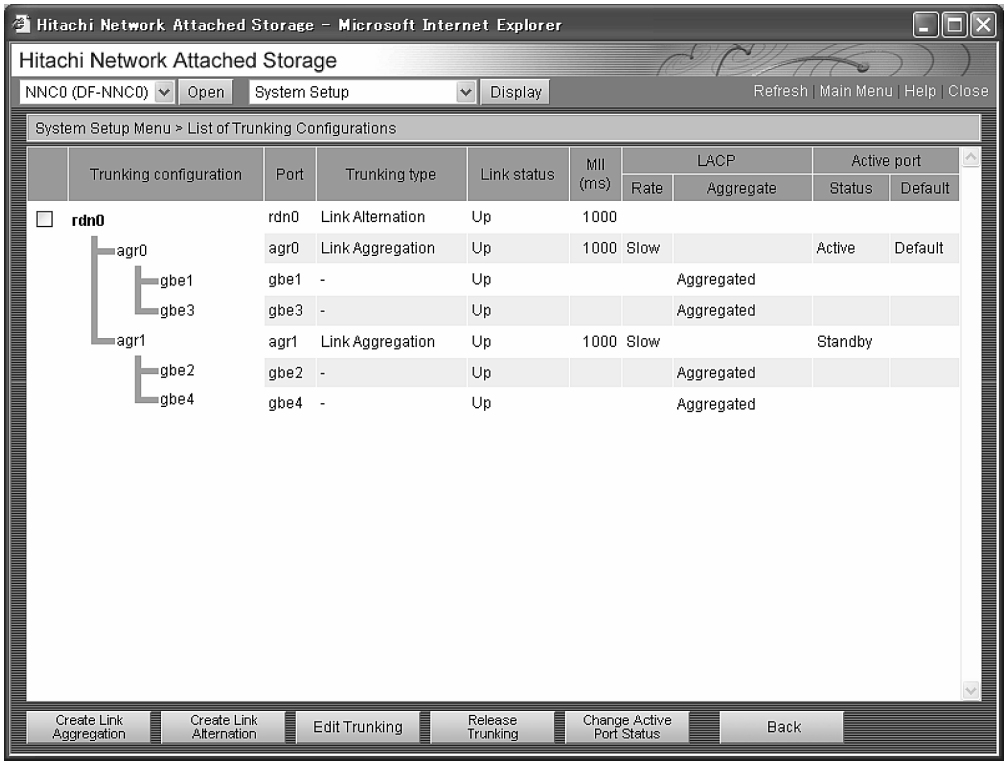



**Figure 4.45 List of Trunking Configurations Window**

The following table lists and describes the information displayed in this window:

**Table 4.28 Information Displayed in the List of Trunking Configurations Window**

| Item | Description |
|---|---|
| **Trunking Configuration** | Displays trunking configuration. |
| **Port** | Displays a port name.<br>`agr0, agr1`<br>This is displayed for a link aggregation port.<br>`rdn0, rdn1`<br>This is displayed for a link alternation port or a cascaded trunking port.<br>`gbe1`, `gbe2`, `gbe3`, or `gbe4`<br>For a port for which trunking is not set, port name `gbe1`, `gbe2`, `gbe3`, or `gbe4` is displayed.<br>When trunking is set, the names of the ports that comprise a trunking configuration are displayed. |

| Item | Description |
|---|---|
| **Trunking Type** | Displays the type of trunking being used.<br>`Link Aggregation`<br>This is displayed for a link aggregation port.<br>`Link Alternation`<br>This is displayed for a link alternation port or a cascaded trunking port.<br>`-`<br>This is displayed for ports for which trunking is not set. This is also displayed for ports that comprise a trunking configuration. |
| **Link Status** | Displays the link status of each port.<br>`Up`<br>This is displayed when the link is normal.<br>`Down`<br>This is displayed when the link is disconnected.<br>Immediately after link trunking settings are changed, `Down` might be displayed for the port that comprises link trunking even if `Up` is displayed for the link trunking port. In this case, wait a while and then click `Refresh` to update information displayed in the window. |
| **MII (ms)** | Displays the MII (link status monitoring interval) set in the link aggregation port or the link alternation port. |
| **LACP** | Displays the LACP interval (checking interval for the status of aggregated ports) set in the link aggregation port, and displays whether each port is currently aggregated.<br>`Rate`<br>Displays `Slow` or `Fast` as the LACP interval.<br>`Slow`<br>Displayed when the LACP interval is set to 30 seconds.<br>`Fast`<br>Displayed when the LACP interval is set to 1 second.<br>`Aggregate`<br>Displays whether each port is currently aggregated.<br>If `Aggregated` is displayed for all ports that comprise the link aggregation port, all the ports have been aggregated.<br>`Aggregated`<br>The port is currently aggregated.<br>`Not aggregated`<br>The port has not participated in aggregation.<br>`Not aggregated` may be displayed for a port that has normally participated in aggregation, for example, immediately after trunking settings are changed. In such a case, wait for a while, and click `Refresh` to refresh the information displayed in the window. |

| Item | Description |
|---|---|
| **Active Port** | Displays the status of the ports for which link alternation is set.<br>`Status`<br>`Active`<br>The port is operating.<br>`Standby`<br>The port is standing by.<br>`Default`<br>This is displayed for the port that is set to operate during normal operation. |

#### 4.7.3.1 Setting Link Aggregation

You can set link aggregation in the **Link Aggregation Setup** window.

To set link aggregation:

1. In the **Main Menu** window, click the System Setup button.

   The **System Setup Menu** window appears. For details on this window, see section 4.7.

2. Click the **Trunking Setup** button.

   The **List of Trunking Configurations** window appears. For details on this window, see section 4.7.2.

3. Select the ports for which you want to set link aggregation, and then click the **Create Link Aggregation** button.

   The **Link Aggregation Setup** window appears.

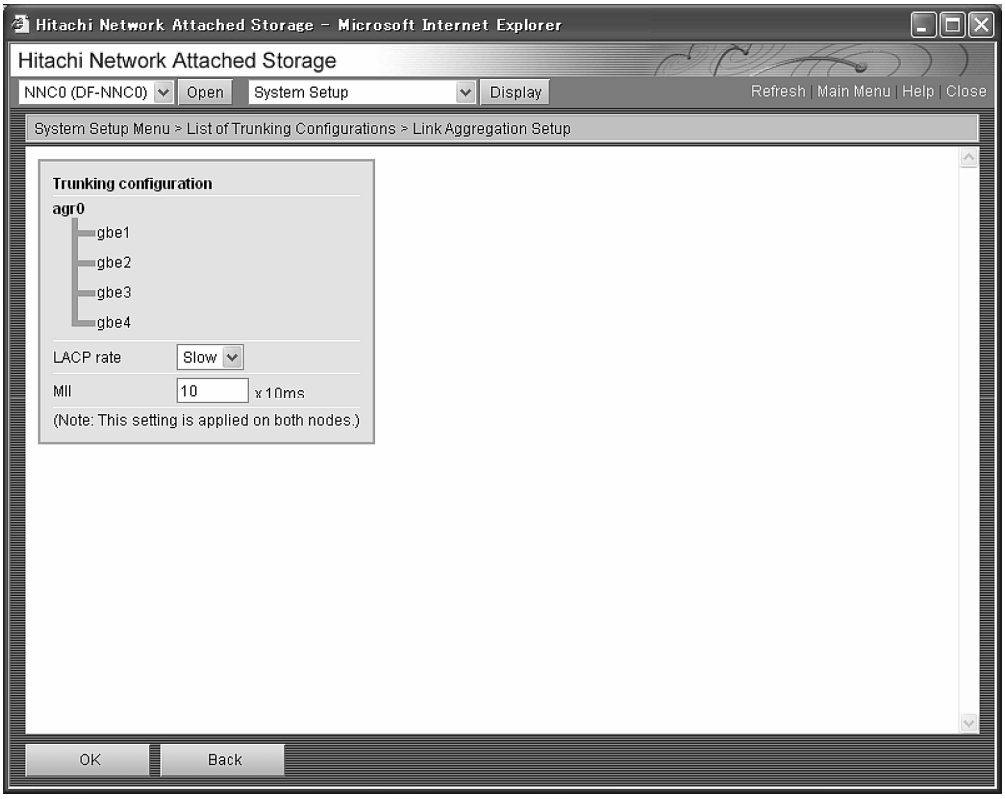



**Figure 4.46 Link Aggregation Setup Window**

4. Enter the required information, and then click the **OK** button.

   Link aggregation is set and the **List of Trunking Configurations** window appears again.

   The following table lists and describes the information to be specified in the **Link Aggregation Setup** window:

**Table 4.29 Information to be Specified in the Link Aggregation Setup Window**

| Item | Description |
|---|---|
| **LACP Rate** | This is a drop-down list that lets you select the interval for checking the status of ports that comprise a link aggregation port.<br>**Slow**<br>Select this to conduct a status check every 30 seconds.<br>**Fast**<br>Select this to conduct a status check every second. |
| **MII** | Specify the interval for checking the link status.<br>You can specify a value from 1 to 100 in units of 10 milliseconds. |

### 4.7.3.2 Editing Information on Link Aggregation

You can edit information on link aggregation in the **Link Aggregation Setup** window.

To edit information on link aggregation:

1. In the **Main Menu** window, click the System Setup button.

   The **System Setup Menu** window appears. For details on this window, see section 4.7.

2. Click the **Trunking Setup** button.

   The List of **Trunking Configurations** window appears. For details on this window, see section 4.7.2.

3. Select the link aggregation ports for which you want to change the settings. Then, click the **Edit Trunking** button.

   The **Link Aggregation Setup** window appears. For details on this window, see section 4.7.2.

4. Enter the required information, and then click the **OK** button.

   The link aggregation settings are changed, and the **List of Trunking Configurations** window appears again.

### 4.7.3.3 Setting Link Alternation

You can set link alternation in the **Link Alternation Setup** window.

To set link alternation:

1. In the **Main Menu** window, click the System Setup button.

   The **System Setup Menu** window appears. For details on this window, see section 4.7.

2. Click the **Trunking Setup** button.

   The **List of Trunking Configurations** window appears. For details on this window, see section 4.7.2.

3. Select two ports for which you want to set link alternation, and then click the **Create Link Alternation** button.

   The **Link Alternation Setup** window appears.

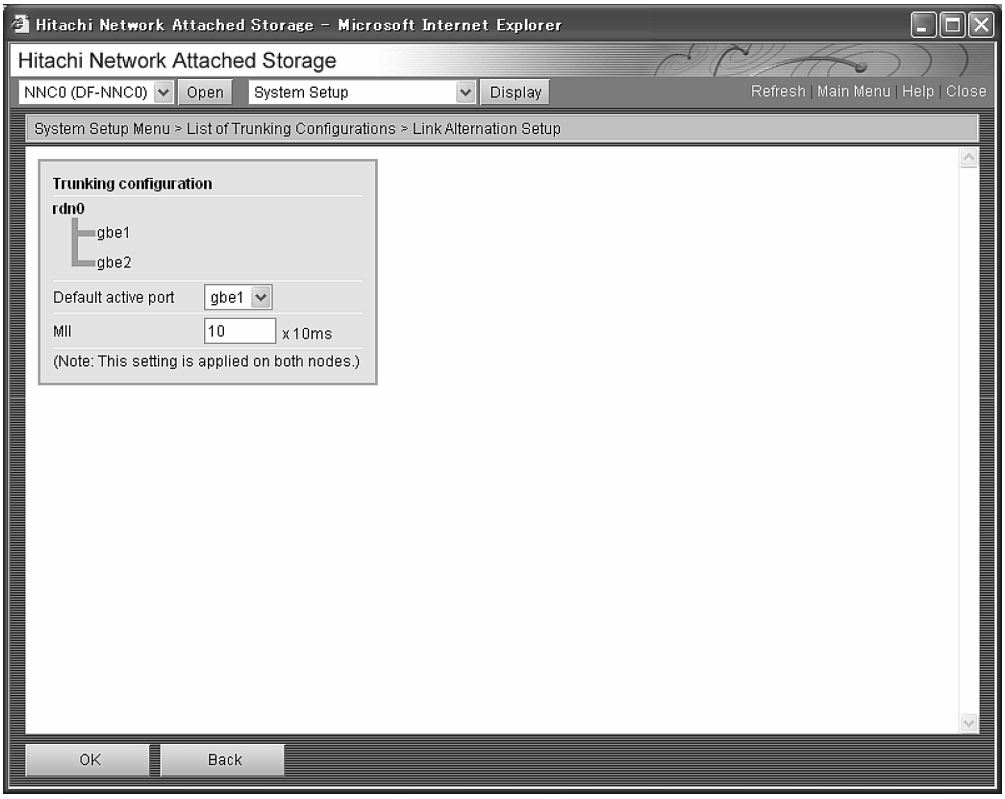



**Figure 4.47 Link Alternation Setup Window**

4. Enter the required information, and then click the **OK** button.

   Link alternation is set and the List of **Trunking Configurations** window appears again.

   In this window, make sure that the status of the port to be used during normal operation (the port selected in **Default** active port) is Active among the ports that comprise link alternation. To check the current status of the port, click **Refresh** to update the information displayed in the window. If the port to be used during normal operation does not become **Active** within 5 seconds, the other port that comprises link alternation automatically becomes **Active**. To make the port to be used during normal operation become **Active**, switch the link manually.

   The following table lists and describes the information to be specified in the **Link Alternation Setup** window:

**Table 4.30 Information to be Specified in the Link Alternation Setup Window**

| Item | Description |
|---|---|
| **Default Active Port** | This is a drop-down list that lets you select the port to be used during normal operation.<br>Select a port that is in the normal state. You can check the link status in Link status of the **List of Trunking Configurations** window.<br>For NAS Modular systems, we recommend that you select a link aggregation port during cascaded trunking setup. For details on cascaded trunking settings, see section 4.7.2. |
| **MII** | Specify the interval for checking the link status.<br>You can specify a value from 1 to 100 in units of 10 milliseconds. |

### 4.7.3.4 Editing Information on Link Alternation

You can edit information on link alternation in the **Link Alternation Setup** window.

To edit information on link alternation:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window appears. For details on this window, see section 4.7.

2. Click the **Trunking Setup** button.

   List of **Trunking Configurations** window appears. For details on this window, see section 4.7.2.

3. Select the link alternation port for which you want to change settings, click the **Edit Trunking** button.

   The **Link Alternation Setup** window appears. For details on this window, see section 4.7.2.

4. Select the required information, and then click the **OK** button.

   The link alternation settings are changed, and the **List of Trunking Configurations** window appears again.

### 4.7.3.5 Setting Cascaded Trunking

You can set up cascaded trunking by using the **Link Aggregation Setup** window to set link aggregation, and then by using the **Link Alternation Setup** window to set link alternation so that it contains a link aggregation port.

When cascaded trunking is used to operate a link aggregation port during normal operation, if all the ports comprising the link aggregation port fail, link alternation occurs automatically.

To set up cascaded trunking:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window appears. For details on this window, see section 4.7.

2. Click the **Trunking Setup** button.

   The **List of Trunking Configurations** window appears. For details on this window, see section 4.7.2.

3. Select the ports for which you want to set link aggregation, and then click the **Create Link Aggregation** button.

   The **Link Aggregation Setup** window appears. For details on this window, see section 4.7.2.

4. Enter the required information, and then click the **OK** button.

   Link aggregation is set and the **List of Trunking Configurations** window appears again.

5. Select two ports for which you want to set link alternation, including a link aggregation port. Then, click the **Create Link Alternation** button.

The **Link Alternation Setup** window appears. For details on this window, see section 4.7.2.

6. Enter the required information, and then click the **OK** button.

   Cascaded trunking is set, and the **List of Trunking Configurations** window appears again.

### 4.7.3.6 Editing Information on Cascaded Trunking

You can edit information on cascaded trunking in the **Edit Cascaded Trunking** window.

To edit information on cascaded trunking:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window appears. For details on this window, see section 4.7.

2. Click the **Trunking Setup** button.

   The **List of Trunking Configurations** window appears. For details on this window, see section 4.7.2.

3. Select a cascade trunking port, and then click the **Edit Trunking** button.

   The **Edit Cascaded Trunking** window appears.

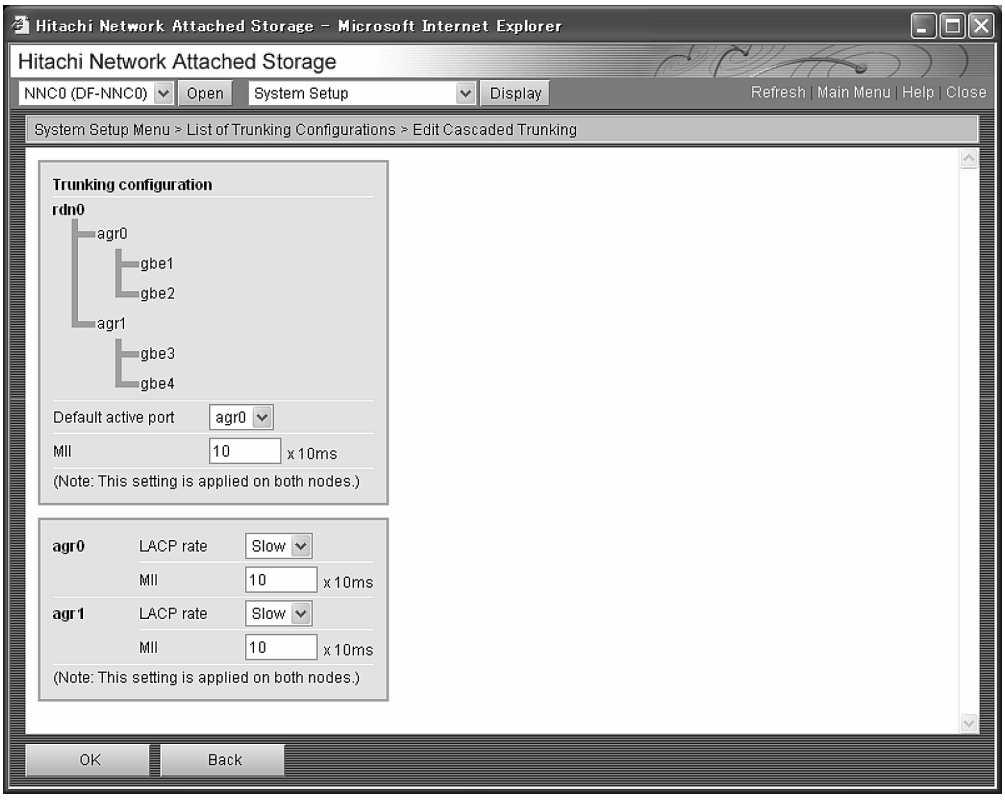



**Figure 4.48 Edit Cascaded Trunking Window**

4. Enter the required information, and then click the **OK** button.

   The cascaded trunking settings are changed, and the **List of Trunking Configurations** window appears again. The following table describes the information to be specified in the **Edit Cascaded Trunking** window:

**Table 4.31 Information to be Specified in the Edit Cascaded Trunking Window**

| Type of Trunking | Item | Description |
|---|---|---|
| **rdn0**<br>(Link Alternation) | **Default Active Port** | This is a drop-down list that lets you select the port to be used during normal operation.<br>For NAS Modular systems, we recommend that you select a link aggregation port during cascaded trunking setup. |
| | **MII** | Specify the interval for checking the link status.<br>You can specify a value from 1 to 100 in units of 10 milliseconds. |
| **agr0,agr1**<br>(Link Aggregation) | **LACP Rate** | This is a drop-down list that lets you select the interval for checking the status of ports for which link aggregation is set.<br>**Slow**<br>Select this to conduct a status check every 30 seconds.<br>**Fast**<br>Select this to conduct a status check every second. |
| | **MII** | Specify the interval for checking the link status.<br>You can specify a value from 1 to 100 in units of 10 milliseconds. |

### 4.7.3.7 Link Alternation

When link alternation has been set, you can manually switch the active link over to another link. Link alternation can be performed from the **List of Trunking Configurations** window.

You can perform manual link alternation only when both of the ports between which link alternation is set are able to communicate (that is, Link status is Up on both ports). If both ports are able to communicate, link alternation does not occur automatically.

For example, when cascaded trunking is used to operate a link aggregation port during normal operation, if all the ports comprising the link aggregation port fail, link alternation occurs automatically. After that, even when the failure is corrected, a link alternation does not occur automatically. To perform a link alternation, you must perform link alternation again using the **List of Trunking Configurations** window.

To perform link alternation manually:

1. In the **Main Menu** window, click the **System Setup** button.

   The **Main Menu** window, click the **System Setup** button.

2. Click the **Trunking Setup** button.

   The **List of Trunking Configurations** window appears. For details on this window, see section 4.7.2.

3. Select a link alternation port, and then click the **Change Active Port Status** button.

   A dialog box appears, asking if you really want to perform link alternation.

4. Click the **OK** button.

   The port that was active becomes inactive, and the port that was standing by becomes active.

#### 4.7.3.8 Releasing Trunking

You can release trunking in the List of **Trunking Configuration** window.

To release trunking:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window appears. For details on this window, see section 4.7.

2. Click the **Trunking Setup** button.

   The **List of Trunking Configurations** window appears. For details on this window, see section 4.7.2.

3. Select the trunking that you want to release, and then click the **Release Trunking** button.

   A dialog box appears, asking if you really want to release the selected trunking.

4. Click the **OK** button.

   The selected trunking is released.

   The specified trunking port cannot be released if other trunking ports of the same type, which were created after the specified one was created, still exist.

   To release the specified trunking port, first select and release, one by one, any subsequently created trunking ports of the same type in the **List of Trunking Configurations** window, in the reverse order to which they were created (starting with the most recently created one). Finally, release the originally specified trunking port.

### 4.7.4 Setting Interface and Network Information

You can view a listing of network and interface information, and add or delete settings. You must set the network and interface information after defining a cluster configuration.

#### 4.7.4.1 Viewing Interface and Network Information

In the **List of Interfaces** window shown below, you can view a listing of network and interface information.

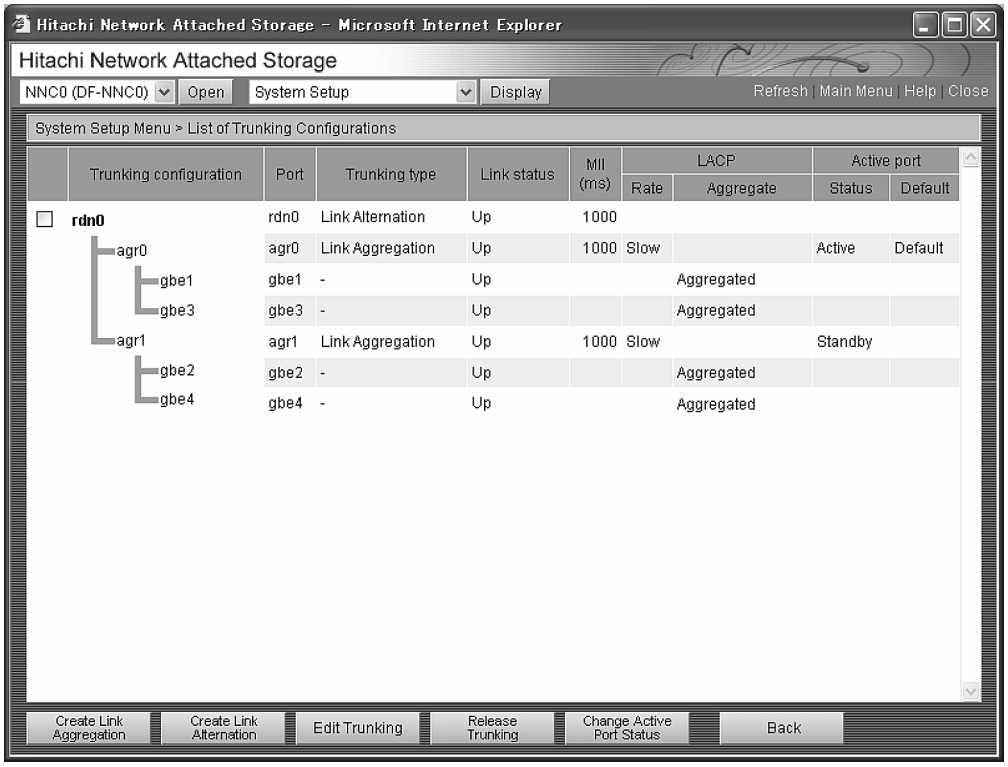



**Figure 4.49 List of Interfaces Window**

The following table describes the information displayed in the **List of Interfaces** window:

**Table 4.32 Information Displayed in List Of Interfaces Window**

| Item | Description |
|---|---|
| **Interface** | Interface information.<br>**Port**<br>The port name is displayed. As the port name, `agr0`, `agr1`, `rdn0`, `rdn1`, `mng1` or any of `gbe1` to `gbe4` is displayed.<br>If ▲ or ▼ is shown on the right side of **Port**, information in the list is sorted by **Port**. ▲ indicates that the information is sorted in ascending order. ▼ indicates that the information is sorted in descending order.<br>**VLAN ID**<br>The VLAN ID is displayed if a VLAN is used. A hyphen (-) is displayed if a VLAN is not used. If ▲ or ▼ is shown on the right of **VLAN ID**, information in the list is sorted by **VLAN ID**. ▲ indicates that the information is sorted in ascending order. ▼ indicates that the information is sorted in descending order. |
| **NNC*x***<br>(Displayed in the left pane. *x* shows a variable.) | The network information set for a node in the cluster is displayed. The node is the one to which the user is currently logged in. See ***Note 1.***<br>**Fixed IP addr (**See ***Note 1.)***<br>Fixed IP address.<br>**Service IP addr (**See ***Note 1.)***<br>Service IP address. A hyphen (-) is displayed if the service IP address has not been set.<br>**Netmask (**See ***Note 1.)***<br>Netmask. |

| Item | Description |
|---|---|
| **NNC*x***<br>(Displayed in the right pane. *x* shows a variable.) | The network information set for a node in the cluster is displayed. The node is the one to which the user is currently logged in.<br>**Fixed IP addr (**See ***Note 1.)***<br>Fixed IP address. `Unknown` is displayed if information cannot be obtained because, for example, the OS has not started.<br>**Service IP addr (**See ***Note 1.)***<br>Service IP address. A hyphen (`-`) is displayed if the service IP address has not been set. Unknown is displayed if information cannot be obtained because, for example, the OS has not started.<br>**Netmask**<br>The currently configured netmask.`Unknown` is displayed if information cannot be obtained because, for example, the OS has not started. |
| **MTU**<br>See ***Note 2*** | MTU value.<br>`Invalid` is displayed if the MTU values differ between nodes. Information cannot be obtained from the nodes not currently connected in the cluster because, for example, the OS has not started. In this case, the MTU value set for the currently connected node is displayed. |

***Note 1:*** If the collected information is invalid, such as when the interface settings have been set for only one node or when the fixed IP address has not been set, `Invalid` is displayed. When `Invalid` is displayed, a value is displayed on the next line in the format `(`*incorrect-value*`)`. For example:

```
Invalid
(192.168.0.1)
```

If the values in **Fixed IP addr** and **Netmask** cannot be obtained, `None` is displayed. For example:

```
Invalid
(none)
```

***Note 2:*** If `Invalid` is displayed in **MTU**, then the MTU values set for the **Login** node and the other node are displayed in the format `(`*MTU-value-set-for-the-login-node*, *MTU-value-set-for-the-other-node*`)`.

If the MTU value cannot be obtained because the NAS Modular system is not running or a communication error has occurred, `Unknown` is displayed. For example:

```
Invalid
(1500,Unknown)
```

If the MTU value cannot be obtained for other reasons, `None` is displayed. For example:

```
Invalid
(1500,none)
```

To view a listing of interface and network information:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Interface Management** button.

   The **List of Interfaces** window displays. As required, select the ports you want to display from the drop-down list, and then click the **Display** button. Information is displayed for the selected ports only.

#### 4.7.4.2 Before Setting or Editing the Interface and Network Information

You need to stop the cluster as well as the resource groups on both nodes before setting or editing the interface and network information. After you finish setting or editing, start the cluster as well as the resource groups on both nodes.

If you change the MTU value for the interface in order to use Jumbo Frame packets, make sure that the peripheral equipment and clients support Jumbo Frame packets, and then change the MTU value. After you change the MTU value, change the MTU values for the peripheral equipment and clients according to the changed MTU value. For details on how to change the MTU values for the peripheral equipment and a client, see the documentation for the peripheral equipment and for the client system.

#### 4.7.4.3 Setting Interface and Network Information

Use the **Add Interface** window to set interface and network information.

If the fixed IP addresses, service IP addresses or subnet masks have been set after a NAS Backup Restore license has been set up, the NDMP server must be restarted by using the NAS Backup Restore window or by using a command. For details on the procedure for, and notes on, restarting the NDMP server, see the manual *NAS Backup Restore Modular User's Guide*.

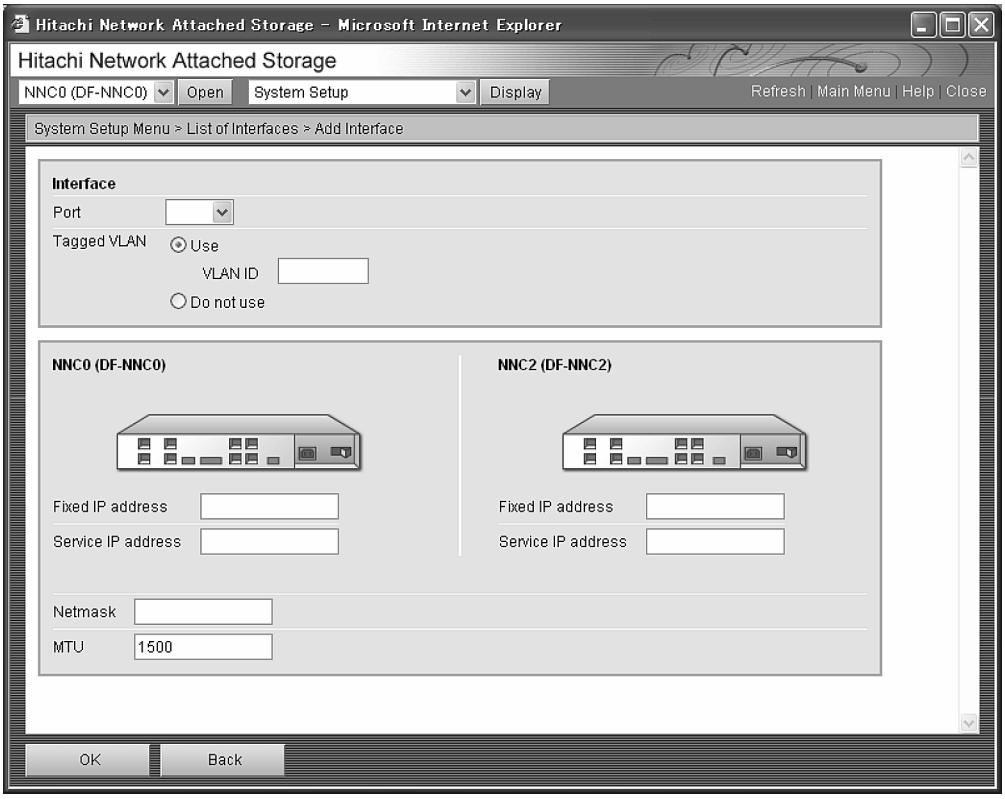



**Figure 4.50 Add Interface Window**

Before you set the interface and network information, the resource group and the cluster must be stopped:

- To stop the resource group, see section 4.5.8.
- To stop the cluster, see section 4.5.4.

Additionally, to change the MTU value of an interface to use a Jumbo Frame packet, the peripheral equipment and clients must support Jumbo Frame packets. Make sure that the peripheral equipment and clients support Jumbo Frame packets, and then change the MTU value. If you changed the MTU value, you also need to set the MTU values for the peripheral and clients according to the changed MTU value.

To set the interface and network information:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Interface Management** button.

   The **List of Interfaces** window displays. For window details, see section 4.7.4.1.

3. Click the **Add** button.

   The **Add Interface** window displays. Following is a description of the window's contents:

   – **Port** From the drop-down list, select the port you want to add. The name of a port using a VLAN is followed by `(Use VLAN)`. If you select a port name followed by `(Use VLAN)`, you need to use a radio button to select **Use** for **Tagged VLAN**.

- **Tagged VLAN** Use a radio button to select whether to use a VLAN.

  ***Note:*** When you select **Use**, enter any VLAN ID for **VLAN ID**.
- **Fixed IP address** Enter a fixed IP address for each NIC on the NAS Unit. (See ***Note 1***.)
- **Service IP address** Specify the service IP address that the client uses to connect to the services of a resource group. (See ***Note 1***.)
- **Netmask** Specify the netmask for both nodes.
- **MTU** Specify the MTU value of an NIC. Changing the MTU value of the NIC allows you to use the Jumbo Frame packet. Specify in the range 1,500-16,110. The default is 1500. (See ***Note 2***.)

***Note 1:*** Do not specify the following IP address for the network: 127.0.0.1. Also, do not specify an IP address from 172.29.1.0 to 172.29.4.255 and a network for the IP address set for the maintenance LAN port. These addresses are reserved by the disk system. If you must specify these addresses, consult your HDS representative. If the IP addresses on both nodes are changed or an IP address that was used by another interface up until just before the setting was set, then communication might not be possible until the ARP cache for external equipment (router or another server) is updated.

***Note 2:*** After changing the MTU value, if necessary, use the ping command from the client to make sure that the client can communicate with the NAS Unit even when the maximum MTU value is specified.

If a client cannot communicate with the NAS Unit although the MTU value is correctly set, the peripheral equipment or the client may have a problem. Check the settings of the peripheral equipment and the client.

#### 4.7.4.4 Editing Interface and Network Information

In the Edit Interface window shown below, you can edit the interface and network information. The interface and network information in `mngl` cannot be edited in the Edit Interface window, so edit that information through Storage Navigator Modular. For details on how to do this, refer to the *Storage Navigator Modular User's Guide*.

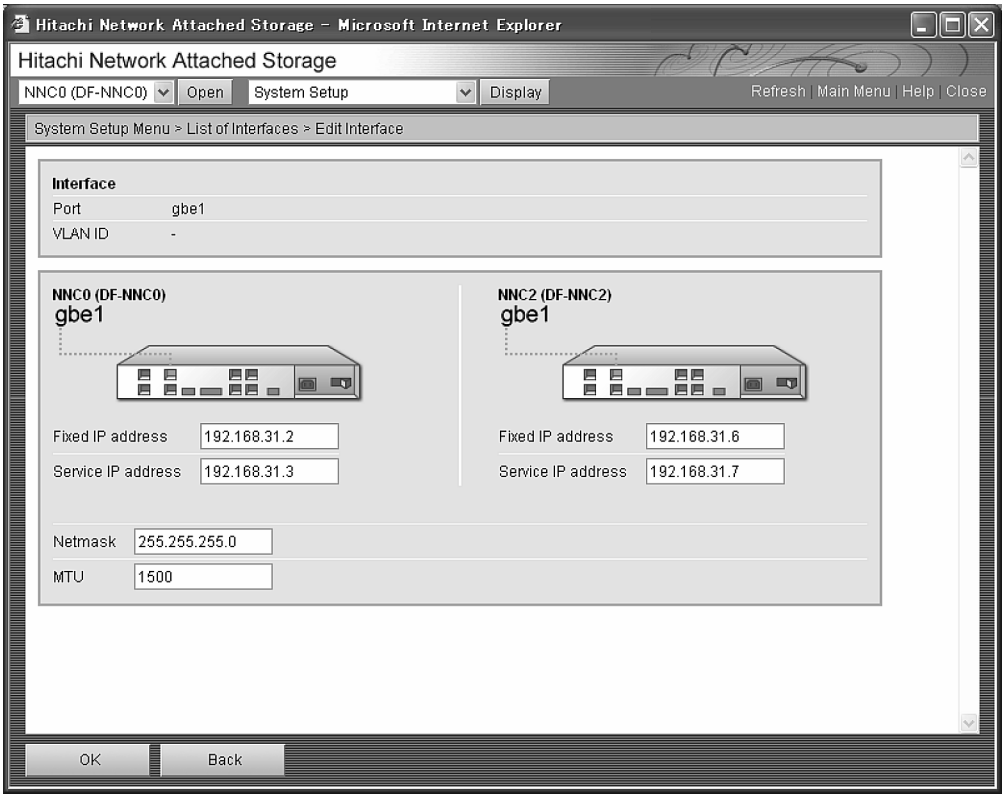



**Figure 4.51 Edit Interface Window**

If the fixed IP addresses or subnet masks have been changed after a NAS Backup Restore license has been set up, the NDMP server must be restarted by using the NAS Backup Restore window or by using a command. For details on how to restart the NDMP server, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

To edit the interface and network information:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7

2. Click the **Interface Management** button.

   The **List of Interfaces** window displays (for window details, see section 4.7.4.1). As required, select the ports you want to display from the drop-down list, then click the **Display** button. Information is displayed for the selected ports only.

3. Use a radio button to select the interface for which you want to set the interface and network information, and then click the **Edit** button.

   The Edit Interface window displays. Following is a description of the window's contents:

   - **Fixed IP address** Enter a fixed IP address for each NIC on the NAS Unit. (See ***Note 1***.)
   - **Service IP address** Specify the service IP address that the client uses to connect to the services of a resource group. (See ***Note 1***.)
   - **Netmask** Specify the netmask for both nodes.

- **MTU** Specify the MTU value of an NIC. Changing the MTU value of the NIC allows you to use the Jumbo Frame packet. Specify in the range 1,500-16,110. The default is 1500. (See ***Note 2***.)

***Note 1:*** Do not specify the following IP address for the network: 127.0.0.1. Also, do not specify An IP address from 172.29.1.0 to 172.29.4.255 and a network for the IP address set for the SVP. These addresses are reserved by the disk system. If you must specify these addresses, consult our Technical Support Division (TSD). For details on the network for the IP address set for the SVP, ask your HDS representative.

***Note 2:*** After changing the MTU value, if necessary, use the ping command from the client to make sure that the client can communicate with the NAS Unit even when the maximum MTU value is specified.

If you change the MTU value of eth1 by mistake and you cannot log in to NAS Manager on any nodes, but you can use SSH to log in to NAS Manager, then use the enas_mtuputeth1 command to change the MTU value.

If a client cannot communicate with the NAS Unit although the MTU value is correctly set, the peripheral equipment or the client may have a problem. Check the settings of the peripheral equipment and the client

4. Enter the required information, then click the **OK** button.

   The interface and network information is changed, and the **List of Interfaces** window re-displays.

### 4.7.4.5 Deleting Interface and Network Information

In the **List of Interfaces** window, you can delete the interface and network information.

To delete the interface and network information:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7

2. Click the **Interface Management** button.

   The **List of Interfaces** window displays (for window details, see section 4.7.4.1). As required, select the ports you want to display from the drop-down list, then click the **Display** button. Information is displayed for the selected ports only.

3. Use a radio button to select the interface for which you want to delete the interface and network information, then click the **Delete** button.

   A dialog box displays prompting you to confirm the deletion.

4. Click the **OK** button to delete the selected interface and network information.

### 4.7.5 Setting DNS, NIS, and LDAP Server Information

In the **DNS, NIS, LDAP Setup** window, the system administrator can set information about the DNS server, NIS server, and LDAP server for user authentication.

You need to stop the cluster as well as the resource groups on both nodes before specifying information in **LDAP setup (for user authentication)** for the first time or clearing all the setting during operation of the NAS Modular system. After you finish the operation, start the cluster as well as the resource groups on both nodes.

If you change the information set in **DNS setup** during operation of the NAS Modular system, you need to restart the NFS service after the change.

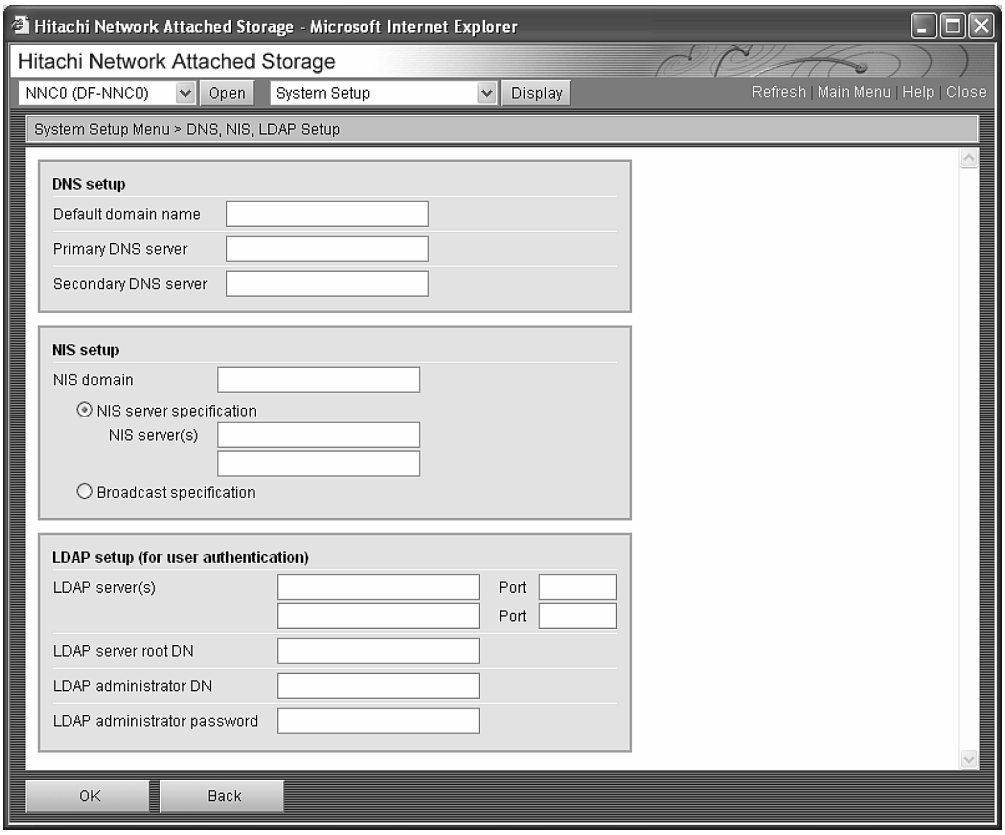



**Figure 4.52 DNS, NIS, LDAP Setup Window**

To set the NIS, DNS, and LDAP server information:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7

2. Click the **DNS, NIS, LDAP Setup** button.

   The **DNS, NIS, LDAP** Setup window displays. Following is a description of the window's contents:

- **DNS setup** When you want to use the DNS server, specify information about the DNS server. The specified information is set for both nodes in the cluster.

  When you do not want to use the DNS server, you can omit specification of this item.

- **NIS setup** To manage user information on an NIS server, specify the NIS domain name of the NIS server. The specified information is set for both nodes in the cluster. Make sure that there are no more than 10,000 users, including the users managed by NAS Manager, per cluster. Also make sure that there are no more than 10,000 groups, including the groups managed by NAS Manager, per cluster.

  You can omit this setting if user information is not to be managed on an NIS server.

  When you enter the domain name of an NIS server in the text box, use a radio button to select a method for specifying the NIS server:

  - **NIS server specification** Select this when you want to use a specific NIS server. In **NIS server(s)**, specify the name or IP address of the NIS server you want to use. (the IP address is recommended).
  - **Broadcast specification** Select this when you want to use broadcasting and it does not matter which NIS server on the network is used.

- **Default domain name** Enter the default domain name of the local host. The same value is set within a cluster. Enter a maximum of 255 characters. You can omit this setting if you are not using domain names.
- **Primary DNS server** Specify the IP address of the DNS server to be used for normal operation. The same value is set within a cluster. You can omit this setting if you are not using a DNS.
- **Secondary DNS server** Specify the IP address of the DNS server to be used if the primary DNS server fails. The same value is set within a cluster. You can omit this setting if you are not using a DNS.
- **LDAP setup**[1] When you want to use the LDAP server to authenticate users, specify information about the LDAP server. The specified information is set for both nodes in the cluster. When you do not want to use the LDAP server, you can omit specification of this item.

  - **LDAP server(s)** Enter name or IP address of LDAP server you want to use (the IP address is recommended). If necessary, specify the port number of the LDAP server in the **Port** text box. When this specification is omitted, `389` is set.
  - **LDAP Server root DN** Specify the root identification name of the LDAP server in the DN format.

  When OpenLDAP is used:

  Specify the value specified in the suffix directive from the LDAP server definitions.

  The following shows an example of specifying `dc=hitachi,dc=co,dc=jp` in the suffix directive:

  ```
  dc=hitachi,dc=co,dc=jp
  ```

  When Sun Java System Directory Server is used:

  Select the **Directory** page to display the data tree. Specify the identification name starting from `dc=` displayed at the top level of the data tree. The following shows an example of specifying `dc=hitachi,dc=co,dc=jp`:

dc=hitachi,dc=co,dc=jp

- LDAP Administrator DN2 Specify the identification name of the LDAP server administrator in the DN format.

  Specify the administrator DN that has been specified in rootdn, or the DN for the user who is allowed the administrator permissions. The following shows an example of specifying dc=hitachi,dc=co,dc=jp in **LDAP server root DN** when the DN of the LDAP administrator is cn=Administrator,dc=hitachi,dc=co,dc=jp:

  cn=Administrator,dc=hitachi,dc=co,dc=jp

- LDAP Adminstrator password2 Specify the password of the LDAP server administrator

3. Enter the required information, then click the **OK** button.

   The information for the NIS server and DNS server is set, and the **System Setup Menu** window re-displays.

4. Restart the NAS OS, if necessary.

   If you have specified information in **LDAP setup (for user authentication)** for the first time or you have cleared all the settings, restart the NAS OS on both NAS Units in the cluster.

   ***Notes***

   [1] In the NAS Modular system, the LDAP server for user authentication and for user mapping cannot coexist. If information about the LDAP server for user mapping has been set in the **CIFS Service Management** window, specifying information in **LDAP setup (for user authentication)** causes an error.

   [2] Make sure to specify this item when an end user logs in to NAS Manager and the security settings for the LDAP server to be used do not allow an anonymous user to obtain a password.

5. In the **List of RAS Information** (Batch-download) window, download the network information log group in a **Batch Operation**, and make sure that the servers have been set up correctly.

   Use the log_interfaces_check file to check the status of each server.

   For details on how to download the log files in a **Batch Operation**. For details on the output of the log_interfaces_check file, see *D.3 Output content of the log_interfaces_check file*.

## 4.7.6 Managing Routing Information

### 4.7.6.1 Viewing Routing Information

In the List of Routings window shown below, you can view a list of routing information.

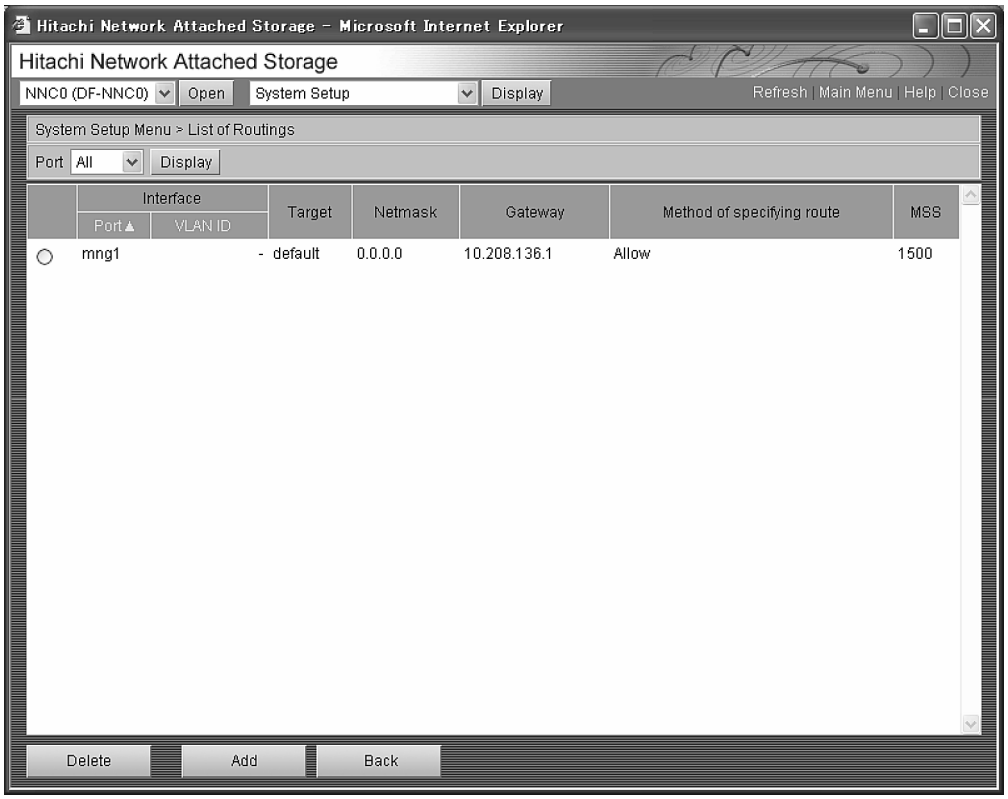



**Figure 4.53 List of Routings Window**

The following table lists and describes the routing information displayed in the List of Routings window:

**Table 4.33 Contents of List of Routings Window**

| Item | Description |
|---|---|
| **Interface** | Interface information.<br>**Port**<br>The port name is displayed. As the port name, `agr0`, `agr1`, `rdn0`, `rdn1`, `mng1` or any of `gbe1` to `gbe4` is displayed.<br>If ▲ or ▼ is shown on the right side of **Port**, information in the list is sorted by **Port**. ▲ indicates that the information is sorted in ascending order. ▼ indicates that the information is sorted in descending order.<br>**VLAN ID**<br>The VLAN ID is displayed if a VLAN is used. A hyphen (-) is displayed if a VLAN is not used.<br>If ▲ or ▼ is shown on the right of **VLAN ID**, information in the list is sorted by **VLAN ID**. |

| Item | Description |
|---|---|
| | ▲ indicates that the information is sorted in ascending order. ▼ indicates that the information is sorted in descending order. |
| **Target** | Routing target.<br>The IP address, host name, or network name of the target is displayed. |
| **Netmask** | The netmask is displayed for a network. A hyphen (-) is displayed for a host. |
| **Gateway** | Gateway through which network data is routed.<br>The IP address or host name of the gateway is displayed. |
| **Method of specifying route** | Whether a route has been set or routing is denied for the routing target.<br>`Allow`<br>A route has been set for the routing target.<br>`Reject`<br>Routing is denied for the routing target. |
| **MSS** | Maximum segment size of the TCP connection on the route. |

To view a list of routing information:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Routing Setup** button.

   The List of Routings window displays. As required, select the ports you want to display from the drop-down list, and then click the **Display** button. Information is displayed for the selected ports only.

### 4.7.6.2 Adding Routing Information

In the Add Routing window, you can add routing information. Each information item that you define in this window is set to the same value in the cluster. Make sure that there are no more than 512 items of routing information in the cluster.

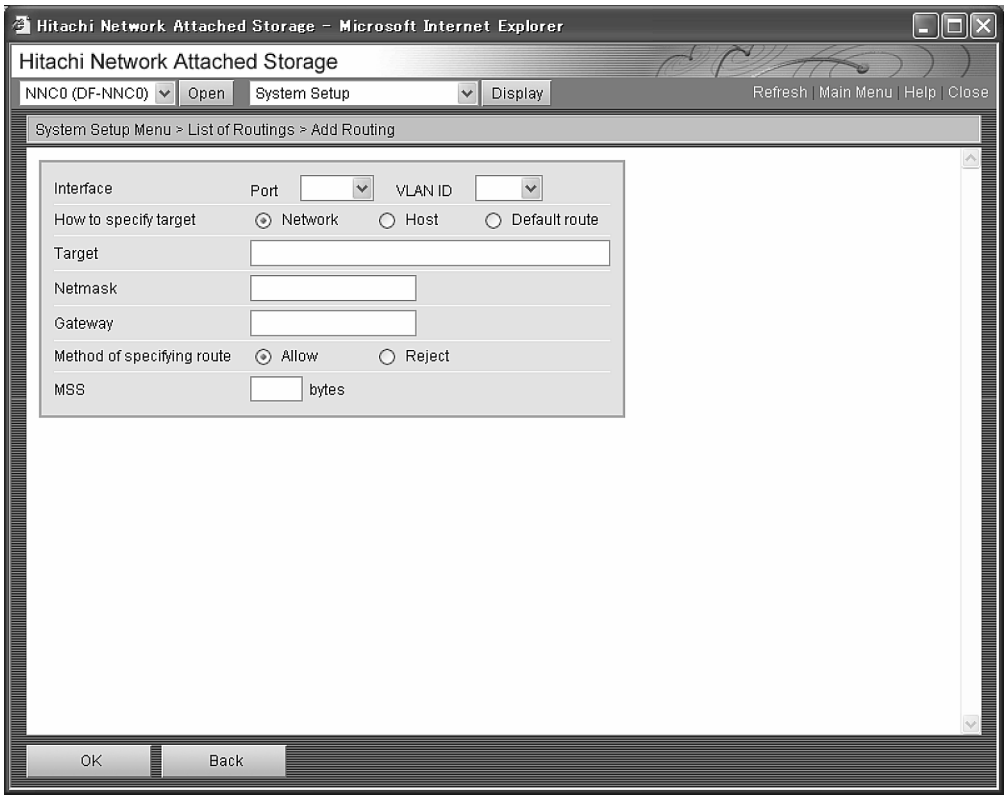



**Figure 4.54 Add Routing Window**

You must configure routing information for each NAS Unit in the same way for all NAS Units within the same cluster.

If the gateway IP address or host name has been changed after a NAS Backup Restore license has been set up, the NDMP server must be restarted by using the NAS Backup Restore window or by using a command.

For more information on restarting the NDMP server, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

To add routing information:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Routing Setup** button.

   The List of Routings window displays. For window details, see section 4.7.4.4.

3. Click the **Add** button.

   The Add Routing window displays. Information about the window is described in Table 4.34.

4. Enter the required information, then click the **OK** button.

   The routing information is added and the List of Routings window re-displays.

**Table 4.34 Information Specified in Add Routing Window**

| Item | Description |
|---|---|
| **Interface** | Select the target interface. The same value is set within a cluster.<br>**Port**<br>From the drop-down list, select the port name for which you want to set information. The drop-down list contains `agr0`, `agr1`, `rdn0`, `rdn1`, `mng1`, and `gbe1` to `gbe4`.<br>**VLAN ID**<br>If you select a port using a VLAN for **Port**, select the target VLAN ID from the drop-down list. A hyphen (`-`) is displayed if a VLAN is not used. |
| **How to specify target** | Use a radio button to select the method of specifying the routing target. The same value is set within a cluster.<br>You can select from the three methods: Specifying a network, directly specifying a host, or specifying the default route. Only one default route can be specified in the cluster.<br>**Network**<br>Specify the target by network address.<br>**Host**<br>Specify the target by host name or IP address.<br>**Default route**<br>Specify the target by the default route. |
| **Target** | Specify the routing target according to the setting of **How to specify target**. This item shows `default` if you select **Default route** for **How to specify target**. |
| **Netmask** | Specify one of the following according to the setting of **How to specify target**. The same value is set within a cluster.<br>When **Network** is selected:<br>Specify the netmask.<br>When **Host** is selected:<br>You do not need to specify anything. The system ignores the specification.<br>When **Default route** is selected:<br>You do not need to specify anything. The system ignores the specification. |
| **Gateway** | Enter the IP address or host name of the gateway through which network data is to be routed. The same value is set within a cluster. |
| **Method of specifying route** | Use a radio button to select whether to set a route or deny routing to the routing target. The same value is set within a cluster.<br>**Allow**<br>Set a route.<br>**Reject**<br>Deny routing. |
| **MSS** | Specify the maximum segment size of the TCP connection on the route (units: bytes).<br>Enter a number in the range from 64 to 65,536. The same value is set within a cluster. |

### 4.7.6.3 Deleting Routing Information

You can use the List of Routings window to delete routing information. When routing information is deleted, communications between the clients that are using the routing and the NAS Modular system cannot be performed. Thus, you might not be able to log in to NAS Manager when the routing information of the management LAN port (mng1) is deleted. If you cannot log in to NAS Manager, log in to NAS Manager from another machine on the same network as the NAS Modular system, and then set the necessary routing information.

To delete routing information:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Routing Setup** button.

   The List of Routings window displays. As required, select the ports you want to display from the drop-down list, and then click the **Display** button. Information is displayed for the selected ports only. For window details, see section 4.7.4.4.

3. Use a radio button to select the routing information you want to delete, and then click the **Delete** button.

   A dialog box confirms that you want to delete the routing information.

4. Click the **OK** button.

   The selected routing information is deleted.

## 4.7.7 Synchronizing Times of Client Machines

To synchronize the times of client machines that use the file system with the NAS Modular system time, the NAS Modular system uses the NTP server. In the Time Setup window, you can set the time at which the NAS Modular system time is synchronized with the NTP server time. In the Time Setup window, the system administrator can also check the address of the NTP server and the time zone set for the NAS Modular system.

Storage Navigator Modular can be used to set the address and time zone for the NTP server. For details on how to do this, see the *Storage Navigator Modular User's Guide*.

To set the time for synchronization with the NTP server time:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Time Setup** button.

   The Time Setup window displays.

3. Enter the required information, then click the **OK** button:

   ***Note:*** We recommend that you set the time zone by selecting a city name. If the time zone is set to the GMT format, the time zone offset is displayed with + for zones west of the Greenwich meridian and-for zones east of it.

- **NTP server** Enter the IP address or host name of the NTP server. The same value is set within a cluster. You can specify up to two NTP servers.
- **Synchronous time** Specify the synchronization time (units: hours and minutes). The same value is set within a cluster. You can specify the time in 5-minute units, in the range from 00:00 to 23:55. You can specify a maximum of 256 synchronization times:
  - To add a synchronization time to the list box, click the **Add** button. You can set the synchronization time only by selecting it in the list box.
  - To delete a synchronization time from the list box, select it and click the **Delete** button.
  - To enhance time accuracy, set synchronization to be performed every two hours or less.
- **Time zone setup** Select a time zone from the list box, then click the **Select** button. The same value is set within a cluster. The time zone is displayed in directory structure. If lower levels are included in the selected time zone, it is expanded to the lower time zones when you click the **Select** button. To go back to the upper levels, select **..** , then click the **Select** button. For example, to set the time zone to Japan, select `posix/Asia/Tokyo` or `posix/Japan`. To set it to Los Angeles in the US, select `posix/America/Los_Angeles`.

The time is set and the **System Setup Menu** window reappears.

4. Reboot the NAS OS as necessary.

   When changing NTP server or Time zone setup, reboot the NAS OS for all nodes within the same cluster. For details about rebooting the NAS OS, see section 4.5.12.

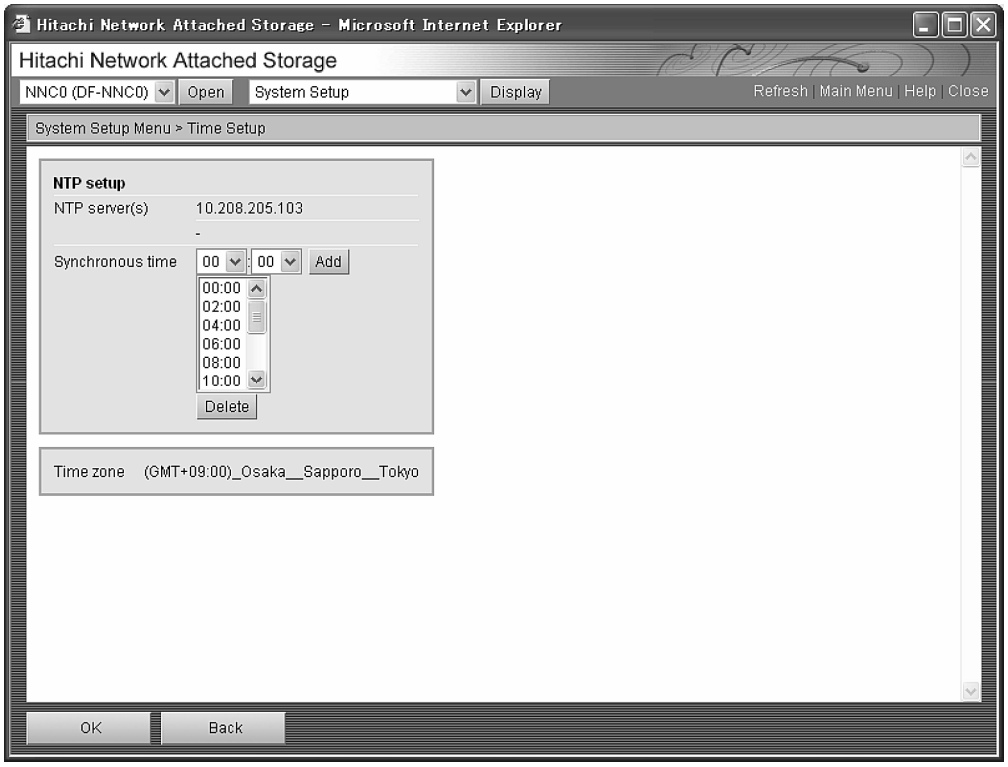



**Figure 4.55 Time Setup Window**

## 4.7.8 Setting System Log Transfer Destinations

You can list the output and transfer destinations for system logs, add transfer destinations, and you can change or delete the added system log transfer destinations.

### 4.7.8.1 Viewing the Contents of the System Log Setup File

In the **Syslog Setup** window shown below, you can view the contents of the system log setup file.

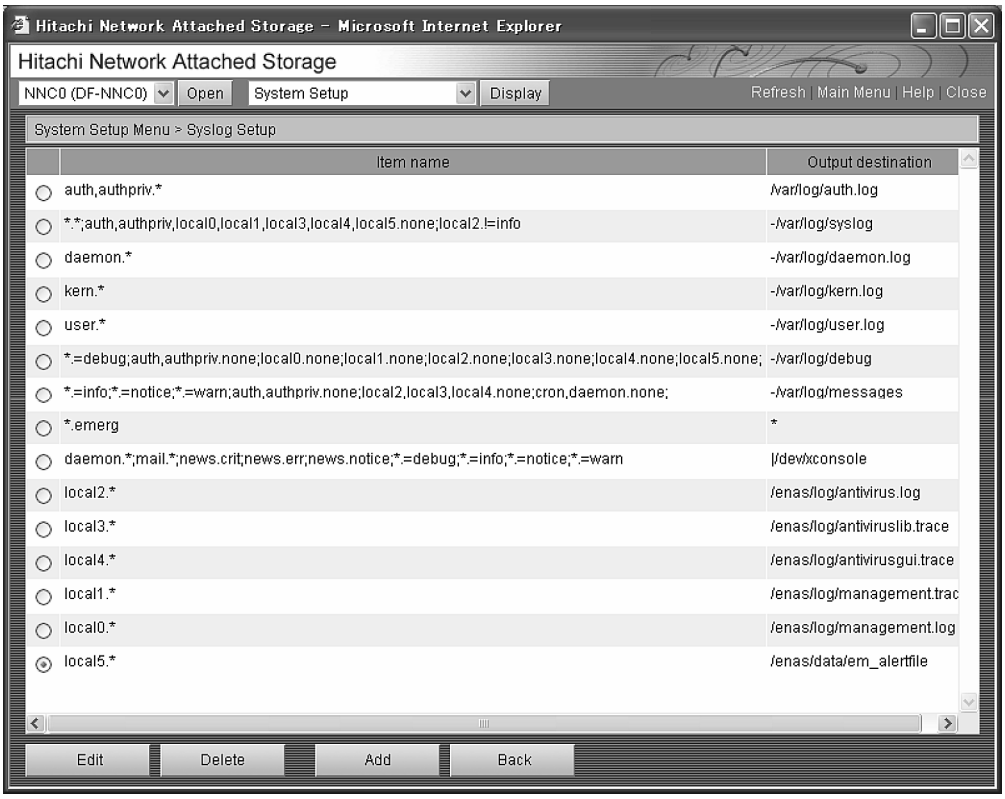



**Figure 4.56 Syslog Setup Window**

The following list describes the information that is displayed in the **Syslog Setup** window:

- **Item name** Facilities and priorities set in selector fields of the system log setup file.
- **Output destination** Host names of the transfer destinations for message logs about facilities and priorities, and host names of the output destinations of logs used in the NAS Modular system.

To view the contents of the system log setup file:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Syslog Setup** button.

   The **Syslog Setup** window displays and you can view a listing of system log transfer destinations.

### 4.7.8.2 Adding a System Log Transfer Destination

In the **Add Syslog Setup** window, you can add a transfer destination for system logs.

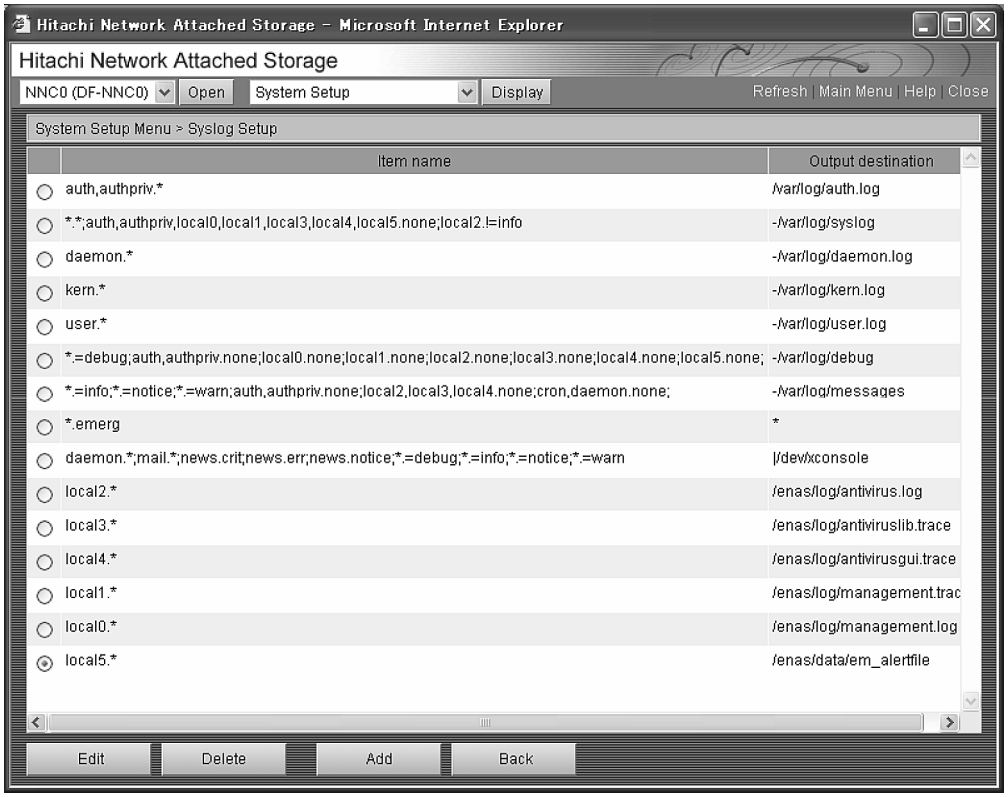



**Figure 4.57 Add Syslog Setup Window**

To add a system log transfer destination:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Syslog Setup** button.

   The **Syslog Setup** window displays. For window details, see section 4.7.8.

3. Click the **Add** button.

   The **Add Syslog Setup** window displays.

4. Enter the required information and click the **Add** button:

   - **Item name** Specify a facility and its priority to be set in a selector field of the system log setup file.
   - **Output destination** Specify a transfer destination for message logs about the facility and its priority. Specify the destination host name in the format *@host-name*.

   The system log transfer destination is added and the **Syslog Setup** window re-displays.

### 4.7.8.3 Changing a System Log Transfer Destination

In the Edit **Syslog Setup** window, you can change a system log transfer destination. Values other than those in the format *@host-name* of **Output destination** cannot be changed.

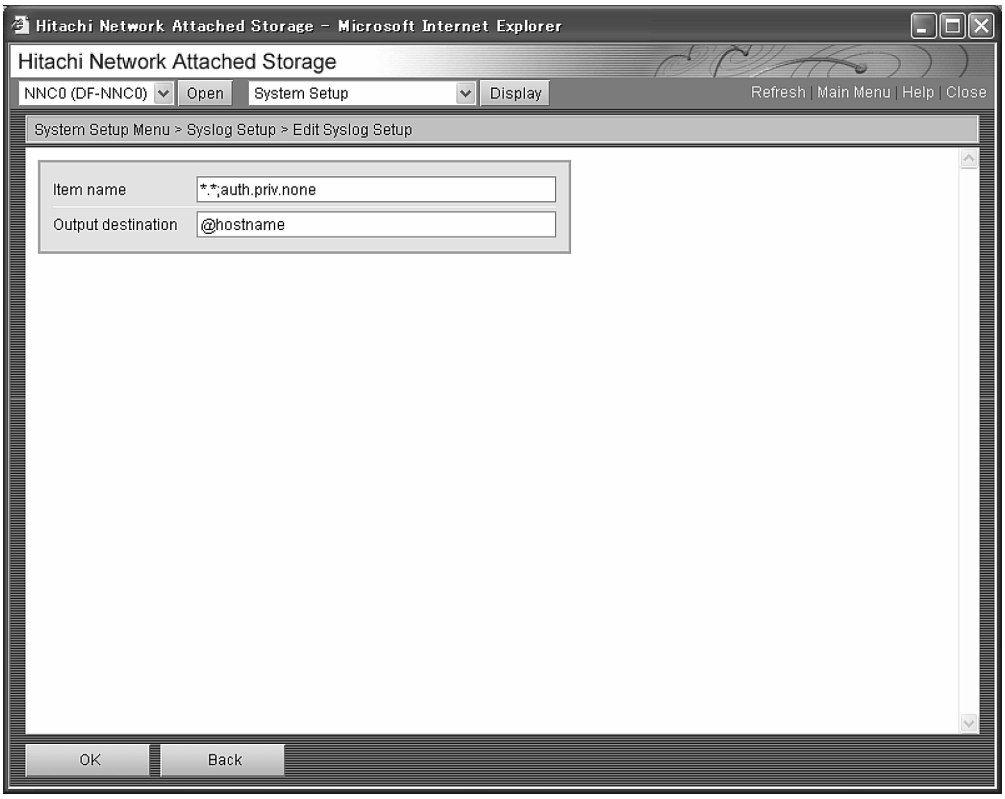



**Figure 4.58 Edit Syslog Setup Window**

To change a system log transfer destination:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Syslog Setup** button.

   The **Syslog Setup** window displays. For window details, see section 4.7.8.

3. Use a radio button to select the item you want to edit, and then click the **Edit** button.

   The Edit **Syslog Setup** window displays.

4. Enter the required information, and then click the **OK** button:

   - **Item name** Specify a facility and its priority to be set in a selector field of the system log setup file.
   - **Output destination** Specify a transfer destination for message logs about the facility and its priority. Specify the destination host name in the format *@host-name*.

   The system log transfer destination changes and the **Syslog Setup** window re-displays.

### 4.7.8.4 Deleting a System Log Transfer Destination

In the **Syslog Setup** window, you can delete a system log transfer destination that has been added. Values other than those in the format *@host-name* of **Output destination** cannot be deleted.

To delete a system log transfer destination:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Syslog Setup** button.

   The **Syslog Setup** window displays. For window details, see section 4.7.8.

3. Use a radio button to select the item you want to delete, and then click the **Delete** button.

   A dialog box confirms that you want to delete the item.

4. Click the **OK** button.

   The selected item is deleted.

### 4.7.9 Setting the Log File Size

You can set the number of log files to be kept, and the size of each log file using the **File Capacity** windows.

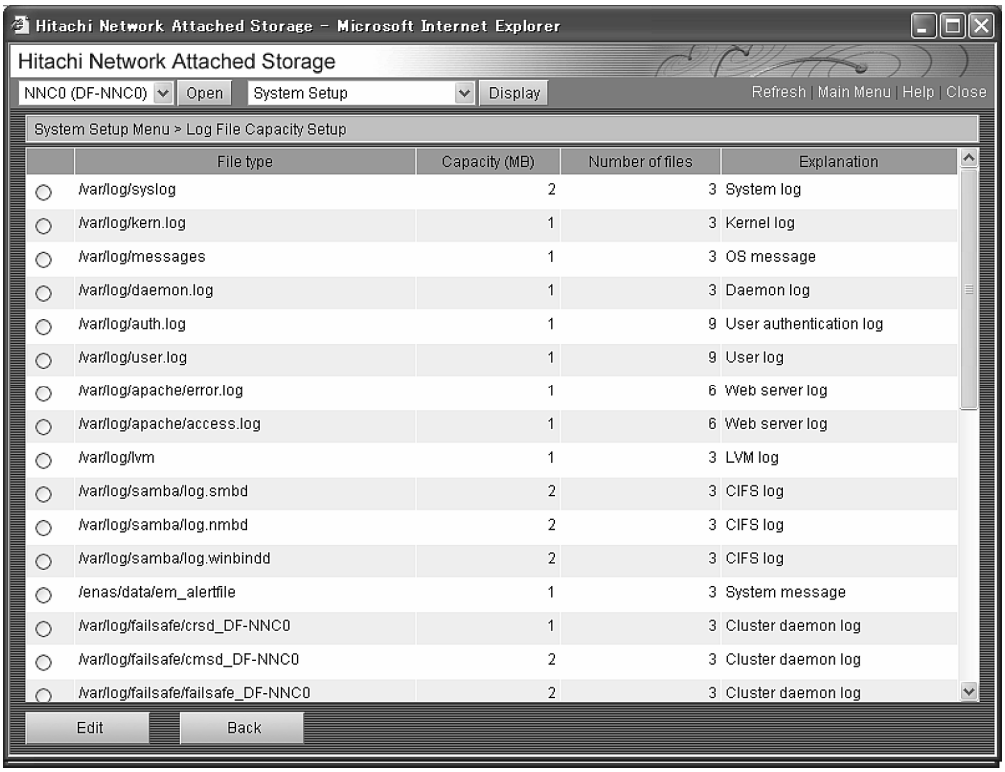



**Figure 4.59 Log File Capacity Setup Window**

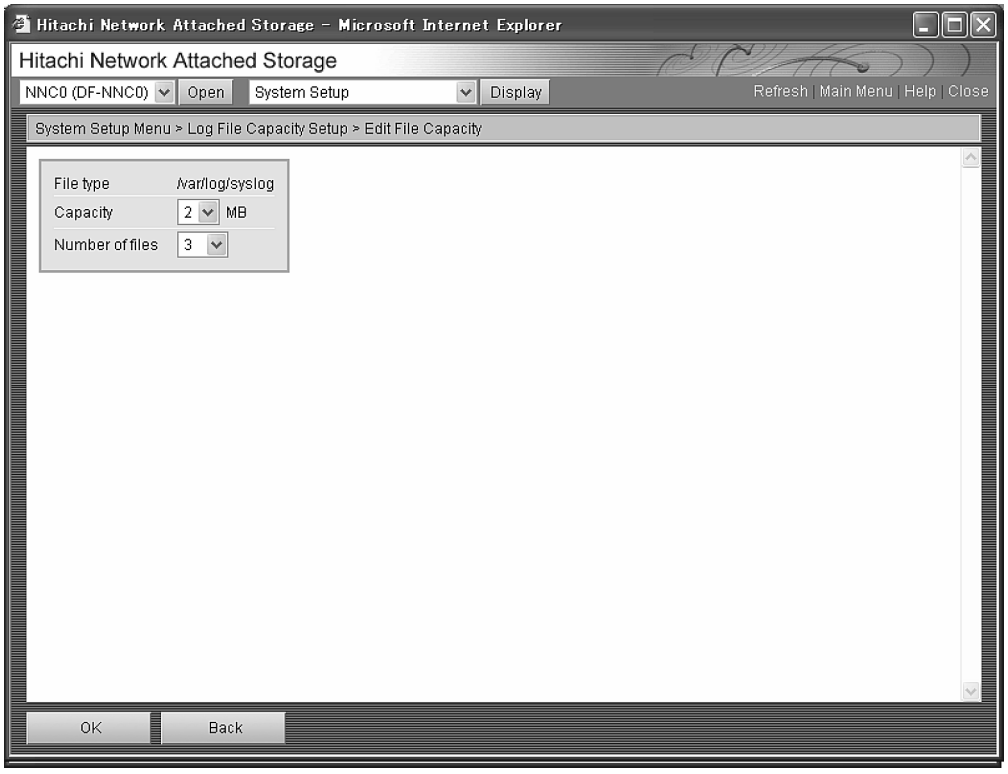



**Figure 4.60 Edit File Capacity Window**

The following table lists and describes the types of log files for which the number of log files to be kept and the size of each log file can be set:

**Table 4.35 Log File Types and Descriptions**

| Log File Type | Description |
|---|---|
| /var/log/syslog | System log |
| /var/log/kern.log | Kernel log |
| /var/log/messages | OS messages |
| /var/log/daemon.log | Daemon log |
| /var/log/auth.log | User authentication log |
| /var/log/user.log | User log |
| /var/log/apache/error.log | Web server log |
| /var/log/apache/access.log | Web server log |
| /var/log/lvm | LVM log |
| /var/log/samba/log.smbd | CIFS log |
| /var/log/samba/log.nmbd | CIFS log |
| /var/log/samba/log.winbindd | CIFS log |
| /var/log/wu-ftpd/xferlog | FTP log |

| Log File Type | Description |
|---|---|
| /enas/data/em_alertfile | System messages |
| /var/log/failsafe/crsd_*NNC-name* | Cluster log |
| /var/log/failsafe/cmsd_ *NNC-name* | Cluster log |
| /var/log/failsafe/failsafe_ *NNC-name* | Cluster log |
| /var/log/failsafe/gcd_ *NNC-name* | Cluster log |
| /var/log/failsafe/ifd_ *NNC-name* | Cluster log |
| /var/log/failsafe/srmd_ *NNC-name* | Cluster log |
| /var/log/failsafe/script_ *NNC-name* | Cluster log |
| /var/log/failsafe/cli_ *NNC-name* | Cluster log |
| /var/log/failsafe/cmond_ *NNC-name* | Cluster log |
| /var/log/failsafe/cdbd_ *NNC-name* | Cluster log |
| /enas/log/management.log | Management log |
| /enas/log/management.trace | Management trace log |
| /enas/log/antivirus.log | Anti-virus Agent log<br>See ***Note 2*** |
| /enas/log/antiviruslib.trace | Anti-virus library trace<br>See ***Note 2*** |
| /enas/log/antivirusgui.trace | Anti-virus GUI trace<br>See ***Note 2*** |
| /enas/log/ebr_alertfile | Backup Restore log<br>See ***Note 1*** |
| /enas/log/backuprestore.trace | Backup Restore trace log<br>See ***Note1*** |
| /enas/log/ndmpserver.log[1] | NDMP server log<br>See ***Note 1*** |
| /enas/log/syncimage.log | Sync Image log |
| /enas/log/syncimage.trace | Sync Image trace log |
| /var/log/wu-ftpd/xferlog | FTP log |
| /var/log/snmpd.log | SNMP daemon log |
| /var/log/xfs/xfslog | XFS log |
| /var/log/xfs/xfsclilog | XFS command log |
| /var/log/nfs/nfsinform.log | NFS notification log |

***Note 1:*** Can be set when a license has been set for NAS Anti Virus Agent. For details on license setup, see the *Storage Navigator Modular User's Guide*.

***Note 2:*** Can be set when a license has been set for NAS Backup Restore. For details on license setup, see the *Storage Navigator Modular User's Guide*.

To set the log file size and the number of files to be kept:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Log File Capacity Setup** button.

   The **Log File Capacity Setup** window displays. The following list describes the information that is displayed in the **Log File Capacity Setup** window:

   - **File type** Log file type and path.
   - **Capacity (MB)** The maximum size of the log file before it is switched to the next generation.
   - **Number of files** Number of log files to be kept.
   - **Explanation** Description of the log file.

3. Use a radio button to select the log file you want to redefine, and then click the **Edit** button.

   The **Edit File Capacity** window displays.

4. Enter the required information that is listed below, and then click the **OK** button:

   - **Capacity** Specify the maximum size of the log file before it is switched to the next generation (units: MB). Select a value from 1 to 6. When the logged data exceeds the specified size, the log file is switched to the next generation.

     ***Note:*** When you specify 5 MB or 6 MB for the CIFS log file size, the log file may be switched before the logged data exceeds the specified size.

   - **Number of files** Enter the number of log files to be kept. The log files will be kept up to the number you specified, excluding the file currently being output. When the number of kept files exceeds the specified number, files are deleted starting from the oldest. You can select from 1 to 14 generations.

   The settings for the selected log file change, and the **Log File Capacity Setup** window re-displays.

### 4.7.10 Setting the Period for Saving the Core File

In the **Core File Auto. Deletion Setup** window, you can set a storage period and automatic deletion time for core files. Core files whose storage period has elapsed are deleted at the specified deletion time. Automatic deletion of core files prevents the NAS OS LU from becoming full.

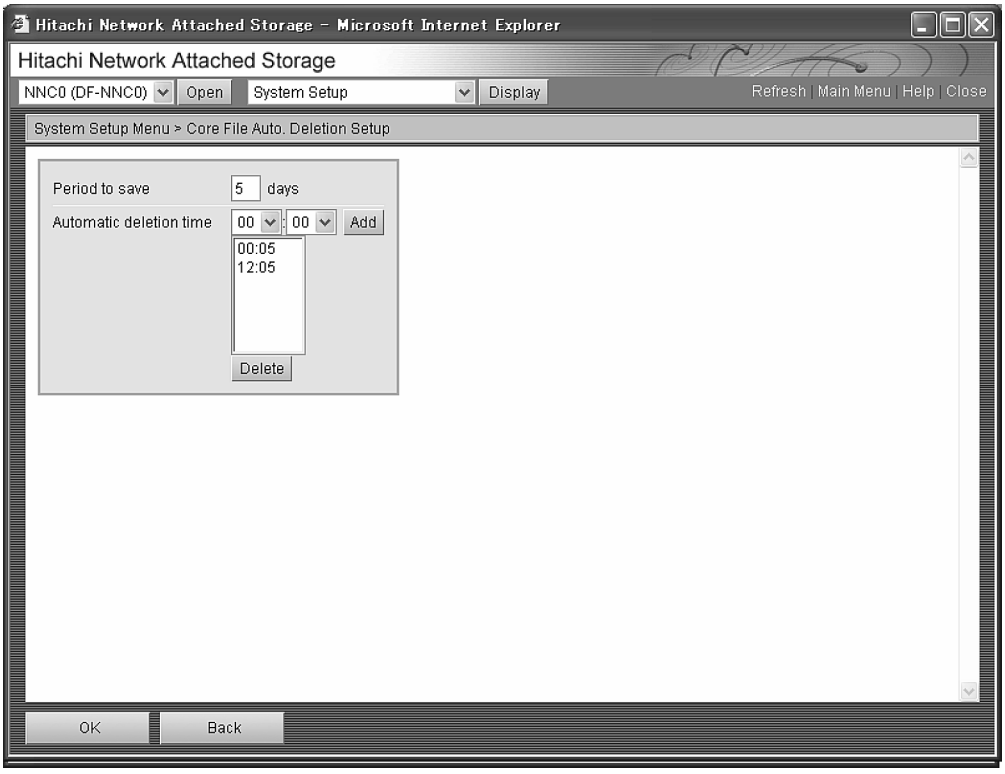



**Figure 4.61 Core File Auto. Deletion Setup Window**

To set a storage period and automatic deletion time for core files:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Core File Auto. Deletion Setup** button.

   The **Core File Auto. Deletion Setup** window displays. Following is information about the window's contents:

   - **Period to save** Specify the core file storage period (units: days). Set a number in the range from 0 to 30 (the default is `5)`. When the storage period has elapsed, core files are deleted at the time specified with **Automatic deletion time**.
   - **Automatic deletion time** Specify the time at which to check for and automatically delete core files (units: hours and minutes).

     You can specify the time in 5-minute units, in the range from 00:00 to 23:55.

     To add a time to the list box, click the **Add** button. You can set the checking and deletion time only by selecting it in the list box.

     To delete a time from the list box, select it and click the **Delete** button. You can specify a maximum of 48 automatic deletion times.

     Two defaults are set: `00:05` and `12:05`.

3. Enter the required information, and then click the **OK** button.

   The information is updated and the **System Setup Menu** window re-displays.

### 4.7.11 Editing System Files Directly

In the **Edit System File** window, you can directly **Edit System File**s of the NAS Modular system.

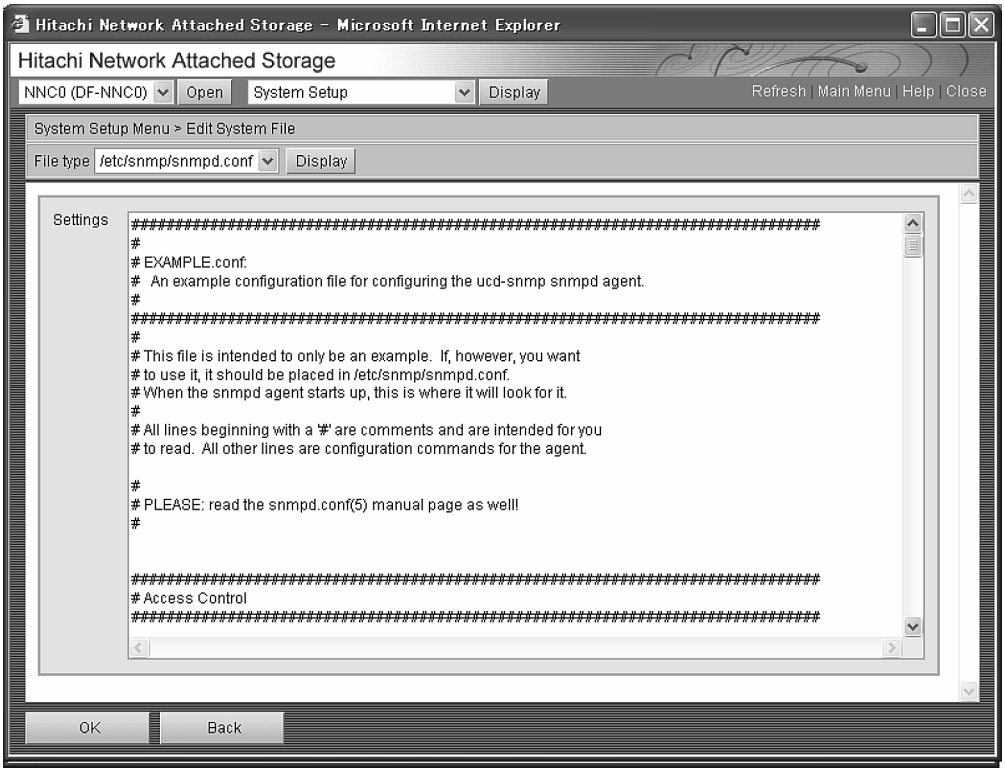



**Figure 4.62 Edit System File Window**

The following table describes the system files that you can edit:

**Table 4.36 Editable System Files in Edit System File Window**

| Item | Description |
|---|---|
| /etc/hosts<br>(See ***Note 1***.) | Associates host names with IP addresses when the host's information is managed by the NAS Modular system. Do not change or delete the values that were set in the `hosts` file when operations started.<br>If the NFS file lock is used from the public destination host for an NFS share, add the following information as required:<br>▪ Service IP address and host name of the resource group to which the mounted NFS share belongs.<br>▪ IP address and host name of the NFS client host that uses NFS file locks.<br>When using the host name to limit public destinations in the CIFS service and CIFS shares for the following operations, add the host name and IP address of the CIFS client that permits or prohibits CIFS access:<br>▪ **Host access restrictions** in the **CIFS Service Management** window<br>▪ **Host access restrictions** in the **Create CIFS File Share** window<br>▪ **Host access restrictions** in the **Edit CIFS File Share** window<br>▪ `-s` option of the `enas_cifscreate` command<br>▪ `-s option` of the `enas_cifsedit` command. |
| /etc/samba/lmhosts | For NT domain authentication or Active Directoryauthentication, this file associates NT domain controllers' IP addresses with domain names for the NT domains that have trust relationships. Add the following line in the `/etc/samba/lmhosts` file:<br>*`IP-address NetBIOS-domain-name-for-the-domain-controller-that-has-the-trust-relationship`*<br>*NetBIOS-domain-name-for-the-domain-controller-that-has-the-trust-relationship* indicates the domain |

| Item | Description |
|---|---|
| | name in short format used in Windows 2000 Professional or earlier operating systems. |
| /etc/snmp/snmpd.conf<br>(See ***Note 2***.) | SNMP setup file. If you want to enable notification via SNMP traps, add the following line to the `snmpd.conf` file:<br>`trap2sink` *`host-name`* [*`community-name`* [*`port-number`*]]<br>If you want to set the threshold for the number of responses to a *get* request issued by the SNMP manager for quota information, append the following line to the end of this file. You can specify the threshold in the range from 0 to 2,147,483,147.<br>`enas_quota_max` *threshold* |

***Note 1:*** When a NAS Backup Restore license has been set, after you register or edit backup server information in the hosts file, you must restart the NDMP server by using the NAS Backup Restore window or a command. For details on the procedure for, and notes on, restarting the NDMP server, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

***Note 2:*** By editing the `snmpd.conf` file directly, you can set the following information:

- The notification destination in SNMP trapping

  You can set the host name or port number of the SNMP manager to which SNMP traps are to be sent.

- The threshold for the number of responses when a *get* request is issued by the SNMP manager

  In the NAS Modular system, quota information for users and groups can be acquired by issuing a *get* request from the SNMP manager to the NAS OS. In the initial status after installation, when a *get* request is issued by the SNMP manager, quota information for all users and groups is returned to the SNMP manager. If the total number of users and groups who use a file system is 10,000, it takes at least 4 minutes until the NAS OS finishes responding to each SNMP manager.

  Take into consideration the total number of users and groups who use a file system, the performance of the SNMP manager, and network load, and then set the threshold for the number of responses (the number of users and groups whose quota information is to be returned from the NAS OS to the SNMP manager) when a *get* request is issued. If the total number of users and groups who use a file system exceeds the threshold set by the administrator, a warning is issued to the SNMP manager, and no response is made to individual quota information.

Do not edit `Access Control` (keywords: `com2sec`, `group`, `view`, and `access`) in the `snmpd.conf` file directly. `Access Control` is edited when SNMP information is set up in the **Add SNMP** or **Edit SNMP** windows. If you edit `Access Control` in the `snmpd.conf` file directly, `Access Control` might no longer be editable using the **Add SNMP** or **Edit SNMP** windows. If you need to edit `Access Control` directly, contact the Technical Support Center.

Configure each NAS Unit in the same way for all NAS Units within the same cluster.

To edit a system file:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Edit System File** button.

   The **Edit System File** window displays.

3. From the **File type** drop-down list, select the system file you want to edit, and then click the **Display** button.

4. The contents of the selected system file display in the **Settings** area. Edit the data in **Settings**.

5. Click the **OK** button.

   The system file is updated and the **System Setup Menu** window re-displays.

### 4.7.12 Tuning the System's Performance

In the **Performance Tuning** window, you can tune the performance of the system. For normal operation, however, there is no need to make any changes. If you wish to tune the system performance, consult our Technical Support Division (TSD).

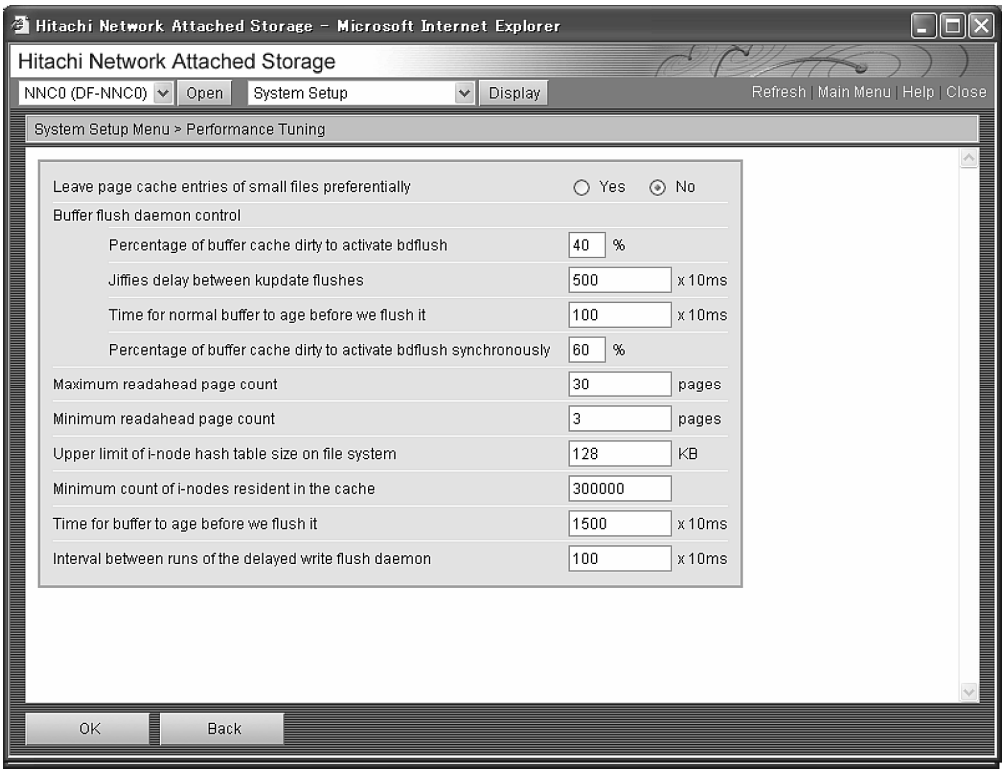



**Figure 4.63 Performance Tuning Window**

To tune the system performance:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **Performance Tuning** button.

   The **Performance Tuning** window displays. Information about the window's contents is described in Table 4.37.

3. Enter the required information, and then click the **OK** button.

   The file system performance is tuned and the **System Setup Menu** window re-displays.

**Table 4.37 Information Specified in Performance Tuning Window**

| Item | Description |
|---|---|
| **Leave page cache entries of small files preferentially** | Specify whether to preferentially keep cache entries of small files. Select either of the following radio buttons:<br>**Yes** Keep cache entries.<br>**No** Do not keep cache entries. |
| **Buffer flush daemon control** | Specify the following control parameters for the buffer flush daemon:<br>**Percentage of buffer cache dirty to activate bdflush**<br>Specify the level of dirty cache at which to start flushing the buffer cache (units: %).<br>Set a number from 0 to 100.<br>The default is 40.<br>**Jiffies delay between kupdate flushes**<br>Specify the interval between buffer cache flushes (units: 10 ms).<br>Set a number from 1 to 1,000,000. We recommend that you specify a number no more than 60,000. Even if you specify a number greater than 60,000, normal operation is not affected. Failover might not work properly when restarting the system after the system terminated abnormally.<br>The default is 500.<br>**Time for normal buffer to age before we flush it**<br>Specify the time to wait before starting to flush the buffer (units: 10 ms).<br>Set a number from 100 to 600,000.<br>The default is 100.<br>**Percentage of buffer cache dirty to activate bdflush synchronously**<br>Specify the level of dirty cache at which to start an urgent buffer flush process (units: %).<br>This parameter activates the flush process even if the dirty cache percentage is reached before the age time elapses.<br>Set a number from 0 to 100.<br>The default is 60. |
| **Maximum readahead page count** | Specify the maximum number of pages to read ahead.<br>Set a number from 0 to 1,024.<br>The default is 30. |
| **Minimum readahead page count** | Specify the minimum number of pages to read ahead.<br>Specify a value less than or equal to the **Maximum readahead page count**.<br>Set a number from 0 to 1,024.<br>The default is 3. |

| Item | Description |
|---|---|
| **Upper limit of i-node hash table size on filesystem** | Specify the maximum size of the i-node hash table per file system (units: KB).<br>Set a number from 128 to 10,240.<br>The default is `128`. |
| **Minimum count of i-nodes resident in the cache** | Specify the minimum number of i-nodes resident on the buffer cache.<br>**For TagmaStore AMS 500 or AMS 1000:**<br>Set a number from 300,000 to 1,400,000.The default is 600000.<br>**For TagmaStore AMS 200 or TagmaStore WMS 100:**<br>Set a number from 300,000 to 900,000.The default is 300000. |
| **Time for buffer to age before we flush it** | Specify the time to wait before starting to flush the buffer cache for meta data (units: 10 ms).<br>Set a number from 100 to 30,000.<br>The default is `1500`. |
| **Interval between runs of the delayed write flush daemon** | Specify the interval between flushes of the buffer cache for write-delayed meta data (units: 10 ms).<br>Set a number from 50 to 3,000.<br>The default is `100`. |

## 4.7.13 Setting SNMP Information

In the **List of SNMPs** window shown below, you can view a listing of SNMP information.

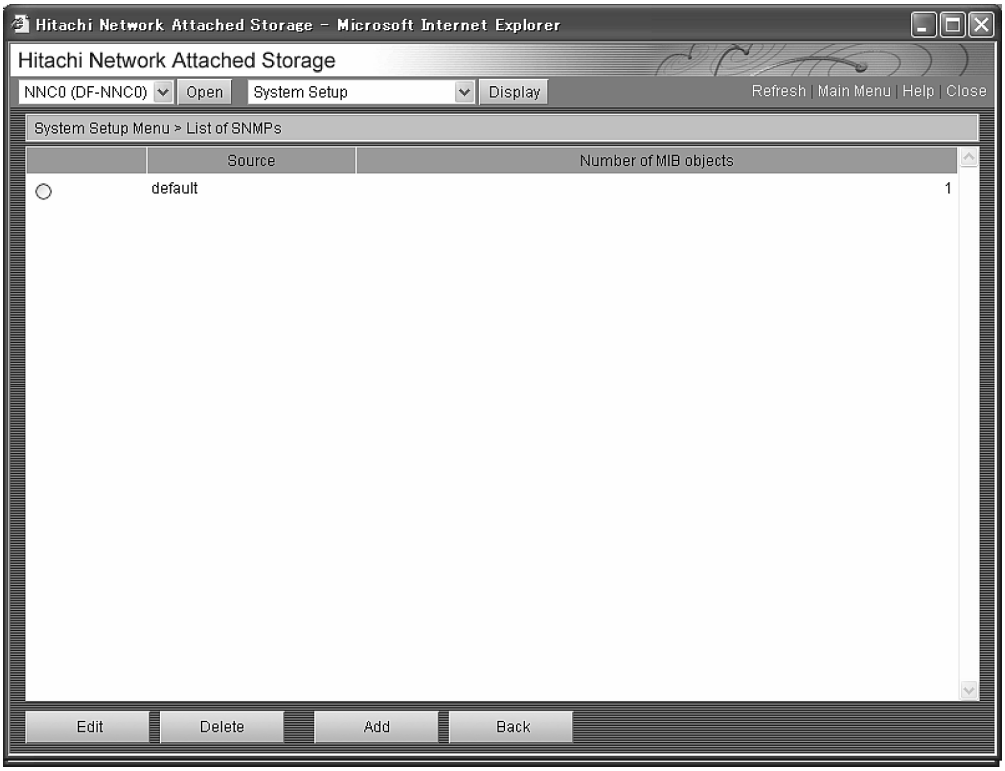



**Figure 4.64 List of SNMPs Window**

The following list describes the information that is displayed in the **List of SNMPs** window:

- **Source** Server name and network of the SNMP manager
- **Number of MIB objects**

To view a listing of SNMP information:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **SNMP Setup** button.

   The **List of SNMPs** window displays.

### 4.7.13.1 Adding SNMP Information

In the **Add SNMP** window shown below, you can add SNMP information. Make sure that there are no more than 128 items of SNMP information per node.

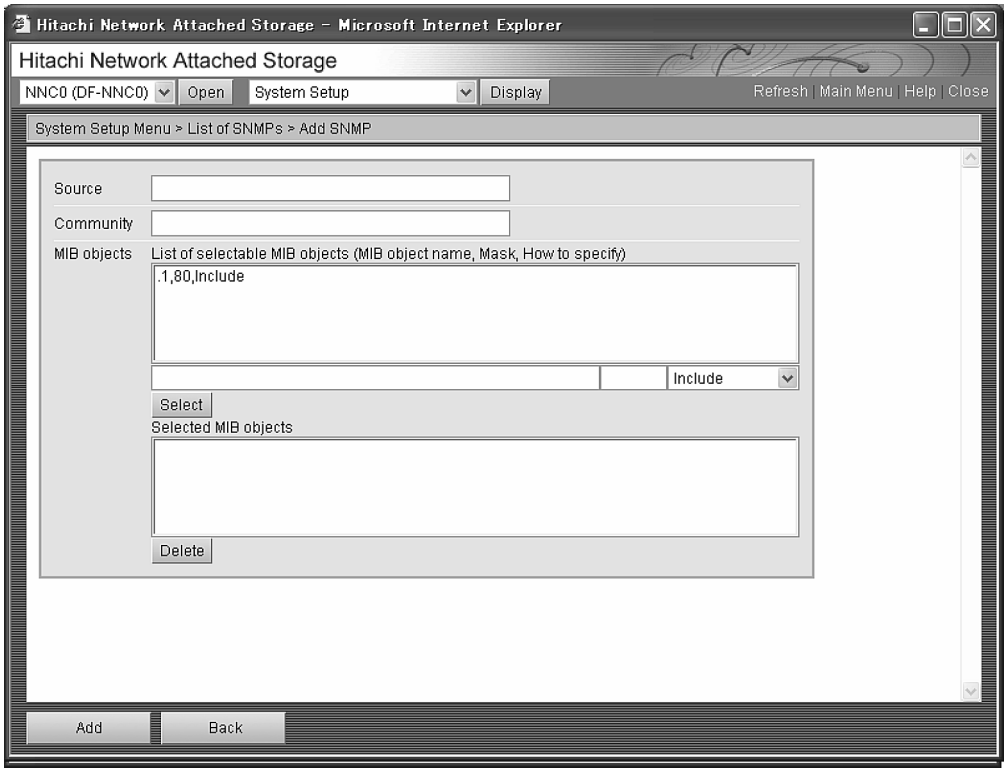



**Figure 4.65 Add SNMP Window**

***Note:*** To use the SNMP trap notification, it is necessary to edit the `snmpd.conf` file.

To add SNMP information:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **SNMP Setup** button.

   The **List of SNMPs** window displays. For window details, see section 4.7.13.

3. Click the **Add** button.

   The **Add SNMP** window displays. Information about the window's contents is described in Table 4.38.

4. Enter the required information, and then click the **Add** button.

   The SNMP information is added and the **List of SNMPs** window re-displays.

**Table 4.38 Information Specified in the Add SNMP Window**

| Item | Description |
|---|---|
| **Source** | Specify the server name and network of the SNMP manager.<br>The specified source SNMP manager can access and acquire information from the MIB object. |
| **Community** | Specify a community name.<br>The SNMP manager uses the community name to access the MIB value of an SNMP agent.<br>Enter a maximum of 32 characters.<br>You can use any alphanumeric character, exclamation mark (!), number sign (#), dollar sign ($), percent sign (%), ampersand (&), apostrophe ('), left parenthesis ( (), right parenthesis ( )), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), forward slash (/), semicolon (;), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left bracket ( [), backslash (\), right bracket (] ), circumflex (^), underscore (_), grave accent (`), left brace ( {), vertical bar ( \|), right brace ( }), and tilde (~). |
| **MIB object** | Specify the MIB object name, mask, and the specification method.<br>**List of selectable MIB objects (MIB object name, Mask, How to specify)**<br>For each MIB object to be added to the SNMP setup file, set the object name, mask, and the specification method.<br>Text box<br>The name and mask for the MIB object selected in **List of selectable MIB objects (MIB object name, Mask, How to specify)** are shown.<br>For a listing of MIB objects, see Appendix A.2, List of MIB Objects.<br>Drop-down list<br>Select whether to include or exclude subtrees of the MIB object displayed in the text box. When you want to include subtrees of the MIB object name, select **Include**. Otherwise, select **Do not include**.<br>Click the **Select** button to add the MIB object to **Selected MIB objects**. Only the MIB objects displayed in **Selected MIB objects** can be set as the SNMP information. When you want to delete an MIB object from **Selected MIB objects**, select the MIB object and click the **Delete** button. |

### 4.7.13.2 Editing SNMP Information

In the **Edit SNMP** window, you can change the SNMP information.

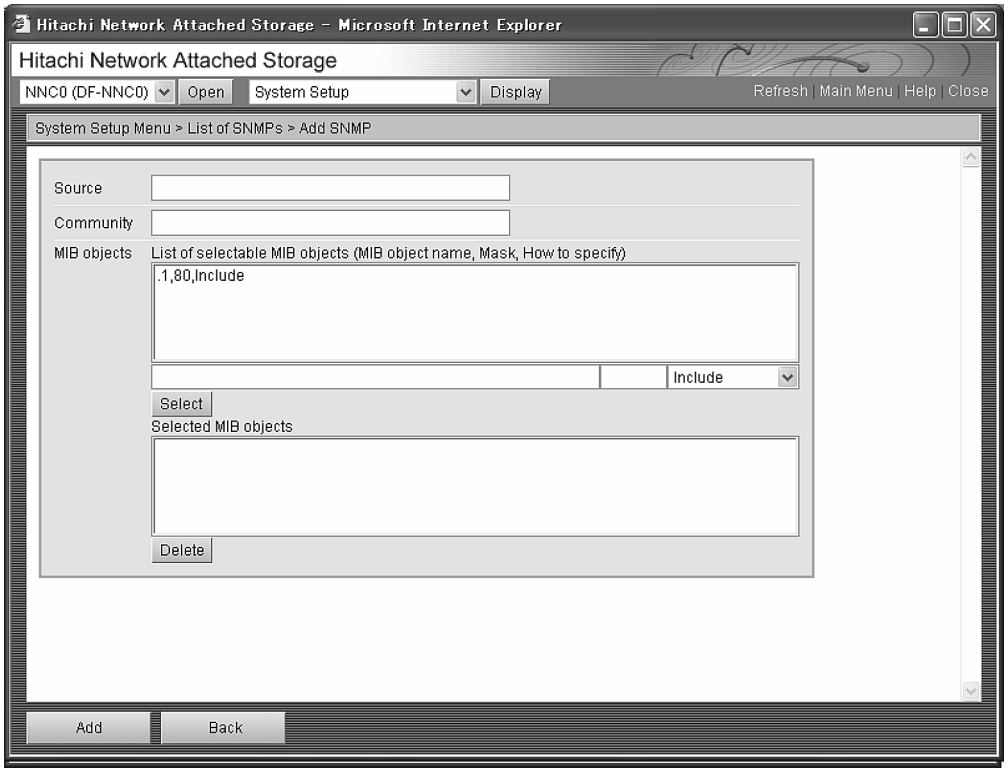



**Figure 4.66 Edit SNMP Window**

***Note:*** To use the SNMP trap notification, it is necessary to edit the `snmpd.conf` file. For details about how to use the SNMP trap notification, see section 4.7.11.

To edit SNMP information:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **SNMP Setup** button.

   The **List of SNMPs** window displays. For window details, see section 4.7.13.

3. Use a radio button to select the SNMP information you want to edit, and then click the **Edit** button.

   The **Edit SNMP** window displays. Information about the window's contents is described in Table 4.39.

4. Enter the required information, and then click the **OK** button.

   The SNMP information is updated and the **List of SNMPs** window re-displays.

**Table 4.39 Information Specified in Edit SNMP Window**

| Item | Description |
|---|---|
| **Source** | Specify the server name and network of the SNMP manager.<br>The specified source SNMP manager can access and acquire information from the MIB object. |
| **Community** | Specify a community name.<br>The SNMP manager uses the community name to access the MIB value of an SNMP agent. |
| **MIB object** | Specify the MIB object name, mask, and the specification method.<br>**List of selectable MIB objects (MIB object name, Mask, How to specify)**<br>For each MIB object to be added to the SNMP setup file, set the object name, mask, and the specification method.<br>Text box<br>The name and mask for the MIB object selected in **List of selectable MIB objects (MIB object name, Mask, How to specify)** are shown.<br>For a listing of MIB objects, see Appendix A.2, List of MIB Objects.<br>Drop-down list<br>Select whether to include or exclude subtrees of the MIB object displayed in the text box. |

### 4.7.13.3 Deleting SNMP Information

In the **List of SNMPs** window, you can delete the SNMP information.

To delete SNMP information:

1. In the **Main Menu** window, click the **System Setup** button.

   The **System Setup Menu** window displays. For window details, see section 4.7.

2. Click the **SNMP Setup** button.

   The **List of SNMPs** window displays. For window details, see section 4.7.13.

3. Use a radio button to select the SNMP information you want to delete, and then click the **Delete** button.

   A dialog box confirms that you want to delete the SNMP information.

4. Click the **OK** button.

   The selected SNMP information is deleted.

## 4.7.14 Selecting the User Interface Mode

A system administrator can use the **Select User Interface** window to select the user interface mode to be used. The selected mode is applied to both NAS Units in the cluster. The selected mode is also applied to all system administrators who can operate the NAS Units in the cluster.

You can select the command operation mode to avoid a GUI operation that might be terminated by a timeout. When the NAS Modular system is operating in any of the following environments, you should use the command operation mode:

- An environment in which the total number of users registered by NAS Manager, the NIS server, and the LDAP server for user authentication exceeds10,000
- An environment in which the total number of groups registered by NAS Manager, the NIS server, and the LDAP server for user authentication exceeds10,000

To select the user interface mode:

- In the **Main Menu** window, click the **System Setup** button.

  The **System Setup Menu** window appears. Click the **Select User Interface** button.

  The **Select User Interface** window appears.

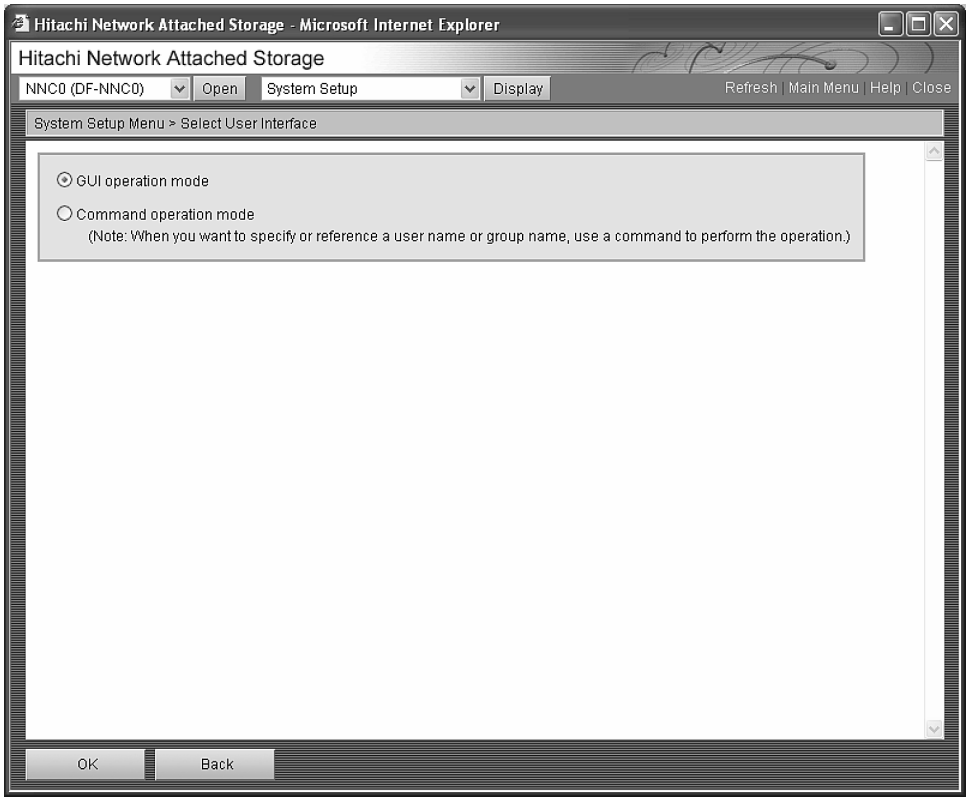



**Figure 4.67 Select User Interface window**

3. Enter the required information, and then click the **OK** button.

   The user interface mode used by system administrators is switched.

   The following table lists and describes the information to be specified in the **Select User Interface** window.

**Table 4.40 Information specified in the Select User Interface window**

| Item | Description |
|---|---|
| **GUI operation mode** | Select this item to operate the NAS Modular system in GUI operation mode.<br>In this mode, you can use all windows and commands. |
| **Command operation mode** | Select this item to operate the NAS Modular system in command operation mode.<br>The following operations must be performed using commands:<br>▪ Setting the users or groups permitted to write to CIFS shares<br>▪ Setting the users or groups prohibited from writing to CIFS shares<br>▪ Setting quotas for users or groups for a file system<br>▪ Viewing quota information for users or groups set for a file system |

## 4.8 Using Anti Virus Agent

If a license is set for NAS Anti Virus Agent, NAS Manager can be linked with the scan server on the network, enabling management of virus scan function such as virus scan implementation, scanning condition settings, and scan result notification.

If the virus scan function is used, at the scan server a virus scan is performed on the corresponding file when a CIFS client accesses files in the disk array or stores files in the disk array.

If a virus-infected file is detected, the virus information and the information about the client that has been manipulating the infected file is output to the system log (syslog). Also, the information can be notified using the SNMP trap. For details on viewing the system log (syslog), see section 4.13.4.

Do the following to protect the NAS Modular system from viruses:

- Views the status of a scan server
- Registers a scan server
- Changes the information of a registered scan server
- Deletes a registered scan server
- Sets the scan conditions
- Starts and stops the virus scan function

The system administrator must configure the virus scan function (which is set up in the **Scan Conditions** window) of each NAS Unit equally to avoid any inconsistency among NAS Units in a cluster. If the settings for NAS Units inside a cluster are different, dispersion may occur in the scan results and repair results for infected files before and after failovers.

This section describes how you can manage the virus scan function of a NAS Modular system.

### 4.8.1 Completing Prerequisites for Linking to Scan Servers

In a NAS Modular system, before linking to scan servers, it is necessary to set the operating environment for all the scan servers on the network. You must also set up all the scan servers and scanning conditions from the NAS Manager.

We recommend that 2 or more scan servers be registered in each cluster in case an error occurs on a scan server or multiple access requests are received within a short period of time. The number of required scan servers varies depending on the usage environment, for example, the types of files to be scanned, or the number of clients who simultaneously access the server.

The following four sections describe the outline of the tasks that must be performed before linking to a scan server.

#### 4.8.1.1 Installing Scan Software

Install scan software at the scan server on the network. The same version of a single type of scan software must be installed on all the scan servers in a cluster. Be particularly careful when using multiple scan servers.

The scan software that can link with NAS Manager is:

Symantec AntiVirus Solution™, version 4.3.13

For details on the preliminary conditions, installation procedure, and notes on scan software, see the documentation for the scan software you are using.

#### 4.8.1.2 Setting Scan Software

The settings necessary to link scan server, on which scan software has been installed, with the NAS Modular system are as follows. For details on setting procedure and notes, see the documentation for the scan software you are using.

- Setting the scan software connection protocol:

  Set the scan software so that the ICAP interface can be used as the connection protocol to NAS Manager.

- Setting the bind address:

  When limiting the number of clients that can connect, set up a bind address to enable the NAS Unit to access as a client of the scan server.

- Setting the port number:

  Set the port number that will be used to control the scan server from NAS Manager. You must enter the same port number that was entered in either the **Add Scanner Server** or **Edit Scanner Server** windows of NAS Manager. If the port numbers entered on the NAS Manager side and the scan server side differs, NAS Manager cannot connect to the scan server.

  For details on the **Add Scanner Server** window, see section 4.8.3. For details on the **Edit Scanner Server** window, see section 4.8.4.

- Setting methods of repairing infected files:

  Set the way in which the system responds to infected files when they are detected.

- Setting scan targets:

  In the archive file, set the file extension for the scan target. Be careful that file extensions that are not specified at the scan server will not be scanned, even if their extensions are specified by NAS Manager. This only applies during virus scans of the archive file.

- Setting the data trickle function:

  Disable the data trickle function. If you enable the data trickle function, the trickled data might contain a virus.

All the scan servers registered to each NAS Unit in a cluster must have the same settings. Also, all the virus definition files of the scan servers registered to each NAS Unit in a cluster must be updated to the latest status at the same time to prevent the invasion of the recently-discovered viruses.

#### 4.8.1.3 Setting Up NAS Manager

After completing settings at the scan server, use the NAS Manager to perform the settings necessary to use the virus scan function. To start using the virus scan function on a NAS Modular system:

1. Register the scan server.

   In the **Add Scanner Server** window, register the scan server in the NAS Modular system. For details on registering a scan server, see section 4.8.3.

2. Set the scanning conditions.

   In the **Scan Conditions** window, set the conditions for requesting a scan server virus scan from NAS Manager. For details on setting scan conditions, see section 4.8.6.

3. Start the virus scan function.

   In the **List of Scanner Servers** window, start the virus scan function. For details on starting the virus scan function, see section 4.8.7.

#### 4.8.1.4 Guidelines for Performing a Virus Scan

Keep the following in mind when performing a virus scan:

- When the CIFS client updates files during a virus scan, the amount of free space on the file system must be at least that of the files to be scanned. Files cannot be updated if free space is not sufficient.

- From the **Scan Conditions** window, if in **Procedure if scanning fails**, **Deny access** is selected, and the virus scan fails after the CIFS client copies files, the copied files are deleted from the disk array.

- From the **Scan Conditions** window, if in **Maximum size for scanning**, the **Permit access to files that have exceeded the maximum size** check box is not selected, when the CIFS client copies files whose size exceeds that specified in **Maximum file size**, the copied files are deleted once copying is complete.
- A virus scan is performed even if the user clicks or right-clicks the files in Windows explorer on the CIFS client.
- A virus scan is performed for ordinary files (as determined by `stat()`). Any other files, such as character device files and FIFO files, are not scanned, and can be accessed.
- When a virus scan is performed for a large file, a timeout error may occur on the CIFS client while the file is being scanned. In this case, processing continues on the NAS Modular system until the virus scan finishes.
- In the **Scan Conditions** window, if **Read and write** or **Write only** is set for **Scan timing**, a temporary file is created in the same folder as that of the file targeted for a virus scan in case a virus infection occurs when a file is updated. The format of the temporary file name is:

  `ava` *`process-id unique-string_name-of-scan-target-file`*`_bak`

  The variable *`process-id`* has 5 characters, and the *`unique-string`* has 6 characters.

  If a system error occurs, sometimes the temporary file remains. If the temporary file remains, disk space might become insufficient. Check whether the file to be scanned has been infected by a virus or data has been damaged, and then delete or restore the file.

  Also, the name of the temporary file is 19 characters longer than the name of the file to be scanned. Therefore, if the length of the file path to the temporary file is longer than the allowable maximum for Windows® (255 characters), sometimes the temporary file cannot be accessed. If the temporary file cannot be accessed, adjust the name of the parent folder so that the length of the file path becomes 255 characters or less, and then delete or restore the temporary file.

### 4.8.2 Viewing Scan Server Status

In the **List of Scanner Servers** window, shown below, you can view the status of scan servers registered in the NAS Modular system.

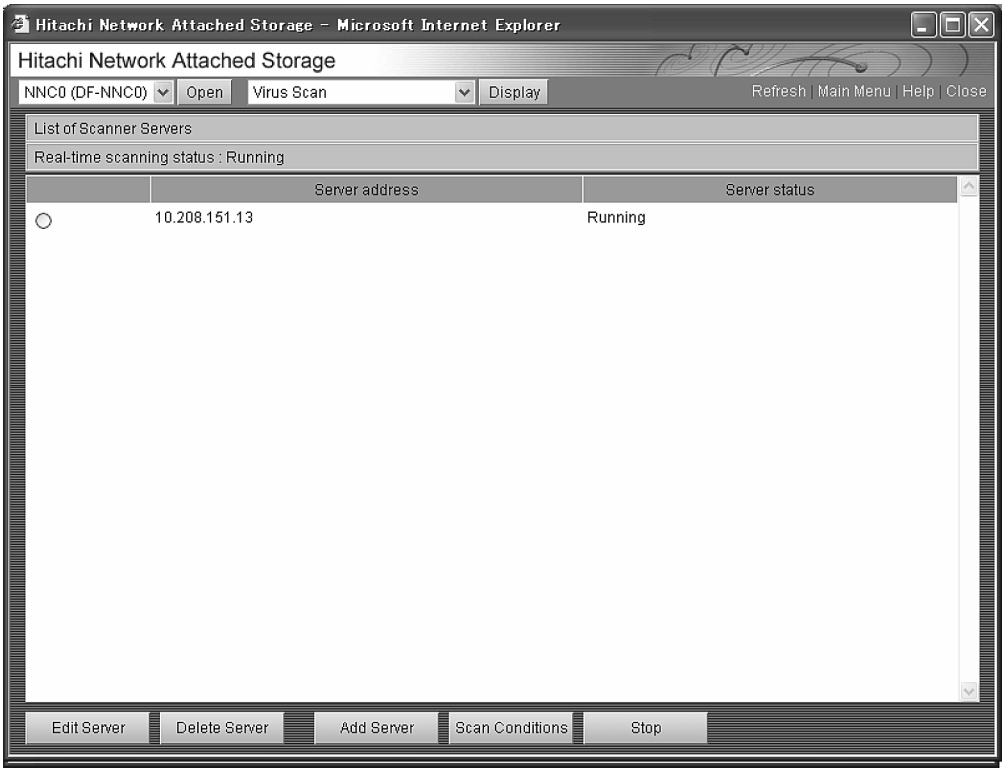



**Figure 4.68 List of Scanner Servers Window**

The following table describes the window's contents:

**Table 4.41 Contents of List of Scanner Servers Window**

| Item | Description |
|---|---|
| **Real-time scanning status** | Displays the status of the NAS Modular system's virus scan function.<br>`Running`<br>Displayed when the virus scan function is running.<br>`Stopped`<br>Displayed when the virus scan function is stopped. |
| **Server address** | Displays either the IP address or the host name of the scan server. Displays the content of the **Server address** specified in the **Add Scanner Server** window. |
| **Server status** | Displays the status of the scan server.<br>`-`<br>Displayed when the virus scan function is stopped.<br>`Running`<br>Displayed when the scan server is functioning normally.<br>`Blocked (Server not found)`<br>Displayed when connection to the scan server is blocked because the scan server could not be found.<br>Make sure that the IP address or host name of the scan server is correct.<br>`Blocked (Access is impossible)`<br>Displayed when connection to the scan server is blocked because the port numbers set at NAS Manager and the scan server are different or the virus scan service is not available. |

| Item | Description |
|---|---|
| | Make sure that the IP address or host name of the scan server, and the port number of the scan server, are correct. Also make sure that ICAP is selected as the communication protocol for the scan server.<br>`Blocked (Time-out)`<br>Displayed when connection to the scan server is blocked because the scan server timed out.<br>Make sure that no network failure has occurred.<br>`Blocked (Version conflict)`<br>Displayed when connection to the scan server is blocked because the protocol versions for NAS Manager and the scan server are not compatible.<br>Acquire all the log data, and then inform maintenance personnel.<br>`Blocked (License expired)`<br>Displayed when connection to the scan server is blocked because the scan software license that was installed at the scan server is invalid.<br>Make sure that the scanning software license has been set up.<br>`Blocked (Scanner server error)`<br>Displayed when connection to the scan server is blocked because a fault occurred in the scan server.<br>`Blocked (Under registration)`<br>Displayed while a process is running to apply the changes to a NAS Modular system after a scan server is registered or a registration is modified.<br>Displayed while the information about the registered scan server is being applied to a NAS Modular system.<br>Wait a few minutes, and then click **Refresh** to update the information displayed in the window.<br>`Error (System failure)`<br>Displayed when a failure occurs in the NAS Modular system.<br>Acquire all the log data, and then inform maintenance personnel. |

In a NAS Modular system, the status of the scan server is periodically monitored. When recovery of a blocked scan server is confirmed, the connection is unblocked automatically.

To view the status of the scan server registered in the NAS Modular system, click the **Virus Scan** button in the **Main Menu** window.

The **List of Scanner Servers** window displays.

### 4.8.3 Registering a Scan Server

In the **Add Scanner Server** window, you can register a scan server into the NAS Modular system. Make sure that the scan server to be registered has been prepared in the network. For details on setting up an operation environment for the scan server, see section 4.8.1.

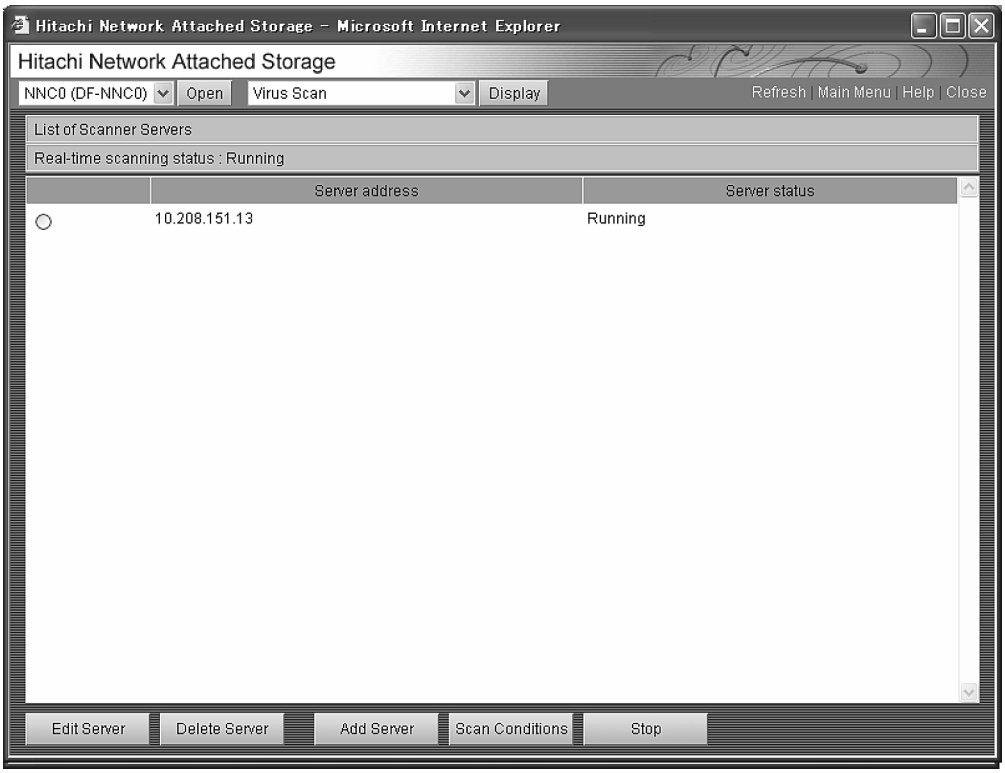



**Figure 4.69 Add Scanner Server Window**

In the NAS Modular system, you do not need to register the same scan server to each NAS Unit within a cluster; that is, you can register a different scan server for each NAS Unit in the same cluster. Note, however, that all the scan servers within a cluster must have the same settings.

To register a scan server NAS Modular system:

1. In the **Main Menu** window, click the **Virus Scan** button.

   The **List of Scanner Servers** window displays. For window details, see section 4.8.2.

2. Click the **Add Server** button.

   The **Add Scanner Server** window displays.

3. Enter the required information, and then click the **Add** button:
   - **Server address** Specify the host name or the IP address of the scan server.
   - **Port number** Specify a port number of the scan server, from 1,024 to 65,535.

   The scan server is added and the **List of Scanner Servers** window re-displays.

### 4.8.4 Changing the Registered Contents of a Scan Server

In the **Edit Scanner Server** window shown below, you can change information for scan servers registered to NAS Manager. The scan servers registered in a cluster must have the same settings. The setting of the modified scan server must be the same as that of other scan servers in the cluster.

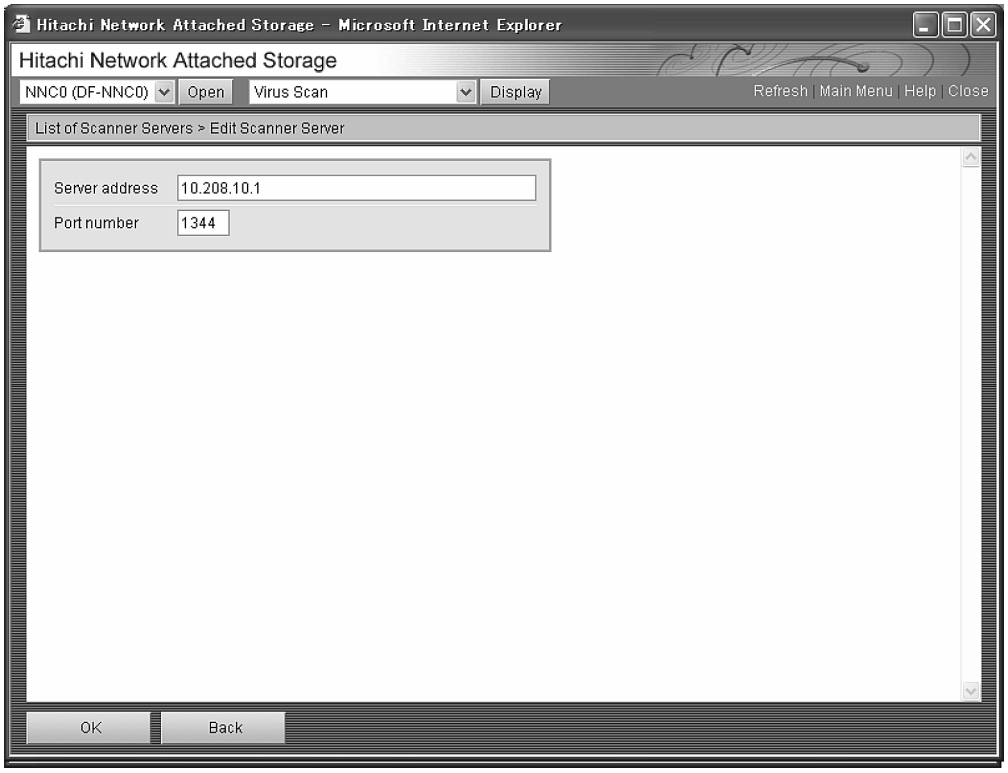



**Figure 4.70 Edit Scanner Server Window**

To change the registered contents for scan servers:

1. In the **Main Menu** window, click the **Virus Scan** button.

   The **List of Scanner Servers** window displays. For window details, see section 4.8.2.

2. Use the radio buttons to select the registered contents you want to change, and then click the **Edit Server** button.

   The **Edit Scanner Server** window displays.

3. Enter the required information, and then click the **OK** button:
   - **Server address** Specify the host name or the IP address of the scan server.
   - **Port number** Specify a port number of the scan server.

   The scan server settings change and the **List of Scanner Servers** window re-displays.

### 4.8.5 Deleting a Registered Scan Server

In the **List of Scanner Servers** window, you can delete a server registered in NAS Manager.

To delete a scan server that has been registered:

1. In the **Main Menu** window, click the **Virus Scan** button.

   The **List of Scanner Servers** window displays. For window details, see section 4.8.2.

2. Use the radio buttons to select the server you want to delete, and then click the **Delete Server** button.

   A dialog box confirms that you want to delete the scan server.

3. Click the **OK** button.

   The selected scan server is deleted.

### 4.8.6 Setting the Scan Conditions

In the **Scan Conditions** window shown below, you can set the conditions for a scan server virus scan to be requested from NAS Manager. Set the scanning conditions for each NAS Unit so that each NAS Unit within the cluster has the same settings.

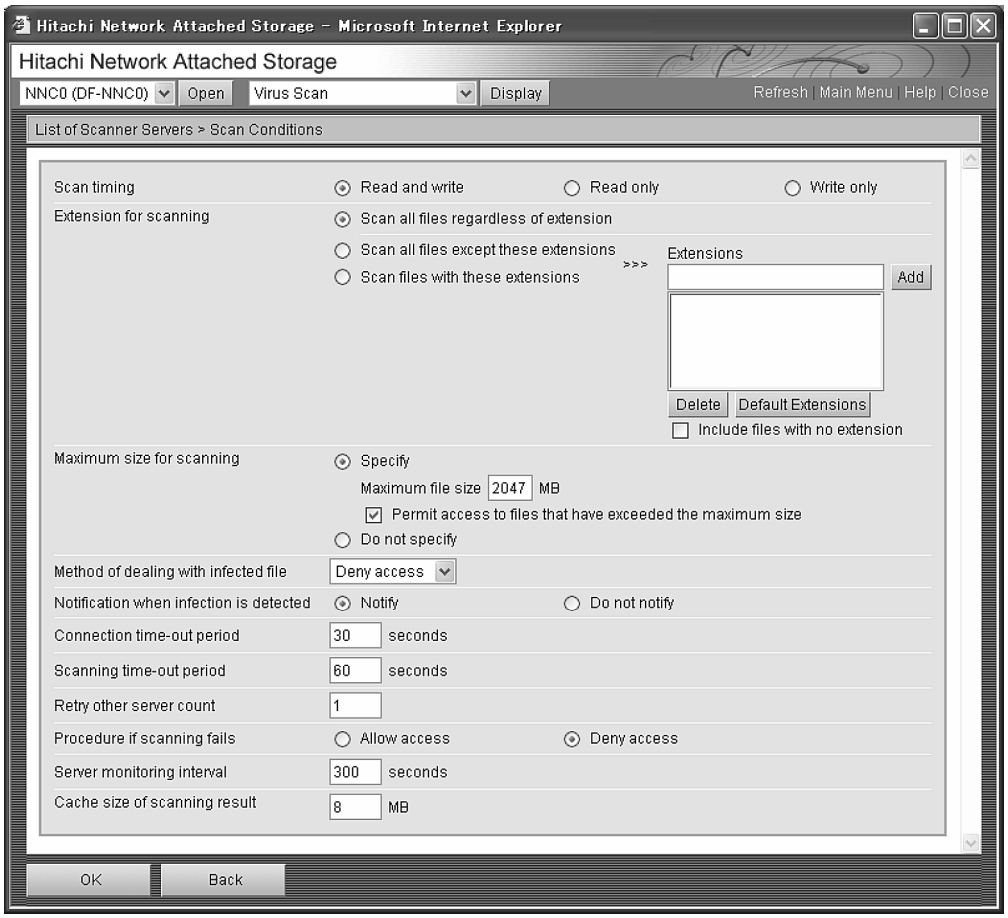



**Figure 4.71 Scan Conditions Window**

At the scan server, scan requests are received from NAS Manager and virus scans are used in accordance with the scan server settings. For example, if the extension of a file for which a scan request was received from NAS Manager is not set as a scan target, a virus scan cannot be used. For details on setting the operating environment of the scan server, see section 4.8.1.

To set conditions related to virus scans:

1. In the **Main Menu** window, click the **Virus Scan** button.

   The **List of Scanner Servers** window displays. For window details, see section 4.8.2.

2. Click the **Scan Conditions** button.

   The **Scan Conditions** window displays. Information about the window's contents is described in Table 4.42.

3. Enter the required information, and then click the **OK** button.

   The virus scan conditions are set, and the **List of Scanner Servers** window re-displays.

**Table 4.42 Information Specified in Scan Conditions Window**

| Item | Description |
|---|---|
| **Scan timing** | Use the radio buttons to select the timing of virus scans.<br>**Read and write**<br>Select this radio button to run a virus scan when the CIFS client has read or written files.<br>**Read only**<br>Select this radio button to run a virus scan when the CIFS client has read files.<br>**Write only**<br>Select this radio button to run a virus scan when the CIFS client has written files. |
| **Extension for scanning** | Use the radio buttons to select the files to be scanned.<br>**Scan all files regardless of extension**<br>Select this radio button to scan all the files for viruses.<br>**Scan all files except these extensions**<br>Select this radio button to run a virus scan on files other than those whose extensions were specified in the **Extensions** list box.<br>**Scan files with these extensions**<br>Select this radio button to perform a virus scan on files whose extensions were specified in the **Extensions** list box. |
| **Extensions** | Specify the extensions to be used when you selected either the **Scan all files except these extensions** or **Scan files with these extensions** radio buttons in the **Extension for scanning** field.<br>Specify a maximum of 16 characters.<br>You can use any alphanumeric character, exclamation mark (!), number sign (#), dollar sign ($), percent sign (%), ampersand (&), apostrophe ('), left parenthesis ( (), right parenthesis ( )), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), forward slash (/), semicolon (;), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left bracket ( [), backslash (\), right bracket (] ), circumflex (^), underscore (_), grave accent (`), left brace ({), vertical bar (|), right brace (}), and tilde (~).<br>Specify a maximum of 255 characters for each compatible radio button.<br>When the **Scan all files except these extensions** radio button is selected, the default setting appears in the list box as follows:<br>.aif, .aifc, .aiff, .asc, .au, .avi, .bmp, .eps, .gif, .ief, .jpe, .jpeg, .jpg, .kar, .latex, .log, .mid, .midi, .mov, .movie, .mp2, .mp3, .mpe, .mpeg, .mpg, .mpga, .pbm, .pcx, .pdf, .pgm, .png, .pnm, .ppm, .ps, .qt, .ra, .ram, .rgb, .rm, .rof, .snd, .swf, .tex, .texi, .texinfo, .tif, .tiff, .tsv, .wav, .xbm, .xpm, and .xwd<br>When the **Scan files with these extensions** radio button is selected, there are no default settings in the list box.<br>Enter an extension and click the **Add** button to add an extension in the list box. Information that has not been added to the list box cannot be set.<br>To delete an extension from the list box, select it and click the **Delete** button.<br>Select the radio button that corresponds to how you want settings information saved to the system. To discard the settings information saved to the system and restore the default settings, click the **Default Extensions** button.<br>To scan files without extensions, select the **Include files with no extension** check box. You can specify whether or not files without extensions are scan targets. |

| Item | Description |
|---|---|
| **Maximum size for scanning** | Use the radio button to select whether or not to specify an upper limit for the size of files to be scanned.<br>**Specify**<br>Select this radio button to perform a virus scan on all files whose size is the same as or smaller than the size specified in **Maximum file size.**<br>In the **Maximum file size** field, specify the upper size limit (in megabytes) of the file to be scanned.<br>Specify within the range from 1 to 9,999.<br>The default is 2047.<br>To permit access for files larger than the limit specified in **Maximum file size**, select the **Permit access to files that have exceeded the maximum size** check box. This means that even if the file size exceeds that specified in **Maximum file size**, it will be stored within the disk array.<br>**Do not specify**<br>Select this radio button when not limiting the size of the file to be scanned. |

| Item | Description |
|---|---|
| **Method of dealing with infected file** | Select the method of dealing with infected files from the drop down menu if an infected file that cannot be repaired is detected in the scan server.<br>**Delete the file**<br>Select this radio button to delete infected files.<br>**Deny access**<br>Select this radio button to deny access from the client to infected files.<br>**Allow access**<br>Select this radio button to allow access from the client to infected files.<br>Depending on the method of dealing with infected files, the operation result for the client accessing the infected file differs.<br>When the client creates the target file, the operation result is as follows: An error is not reported to the operation result.<br>When selecting the **Delete the file** button<br>The target file is deleted and therefore cannot be created newly.<br>When selecting the **Deny access** button<br>The target file is deleted and therefore cannot be created newly.<br>When selecting the **Allow access** button<br>The target file can be created newly.<br>When the client views the target file, the operation result is as follows:<br>When selecting the **Delete the file** button<br>The target file is deleted and therefore cannot be viewed.<br>When selecting the **Deny access** button<br>The target file access is denied. The target file cannot be viewed.<br>When selecting the **Allow access** button<br>The target file can be viewed.<br>When the client updates the target file, the operation result is as follows: An error is not reported to the operation result.<br>When selecting the **Delete the file** button<br>The target file is deleted and therefore cannot be updated.<br>When selecting the **Deny access** button<br>The target file status returns to the status before the update and therefore the target file cannot be updated.<br>When selecting the **Allow access** button<br>The target file can be updated. |
| **Notification when infection is detected** | Use the radio buttons to select whether or not you want to receive notification regarding detection results of infected files.<br>**Notify**<br>Select this radio button to notify the SNMP trap of the name of the infected file, the name of the virus, and the results of the actions taken in regard to the infected file. The KAQV10022-E message is notified to the SNMP server.<br>To receive notifications, it is necessary to set up NAS Manager so that SNMP can be used. For details on the settings required to use SNMP trap notification, see section 4.7.11.<br>**Do not notify**<br>Select this radio button if you do not want to be notified when infected files are detected. |

| Item | Description |
|---|---|
| **Connection time-out period** | Specify the interval (in seconds) from the time the connection request is sent from the NAS Manager to the scan server until timeout.<br>Scan servers that do not respond during the timeout are blocked, and the virus scan is requested to another scan server.<br>Specify from 1 to 600 seconds.<br>The default is `30`. |
| **Scanning time-out period** | Specify the interval (in seconds) from the time a scan request is sent from the NAS Manager to the scan server until timeout.<br>If there is no response within the specified amount of time, the response method selected in the **Procedure if scanning fails** field will be followed.<br>Specify from 1 to 1,800 seconds.<br>The default is `60`. |
| **Retry other server count** | Specify the number of times to request a virus scan at another scan server in the event of a timeout.<br>Specify from 0 to 32. Specify a value at or below the number of scan servers registered in NAS Manager.<br>The default is `1`.<br>Specifying `0` will cause virus scans to fail if a timeout occurs. |
| **Procedure if scanning fails** | Use the radio buttons to select the response method you want to use in the event that the virus scan fails.<br>**Allow access**<br>Specify this to permit access to files that could not be scanned for viruses.<br>**Deny access**<br>Specify this to refuse access to files that could not be scanned for viruses.<br>Files not scanned (such as files whose folder and file sizes are 0 bytes, and files with extensions specified not to be scanned) can be stored within the disk array, even if all scan servers are blocked.<br>Depending on the method of dealing with infected files, the operation result for the client accessing the infected file differs.<br>When the client creates the target file, the operation result is as follows: An error about the operation result is not reported.<br>When selecting the **Allow access** button<br>The target file can be created newly.<br>When selecting the **Deny access** button<br>The target file is deleted and therefore cannot be created newly.<br>When the client views the target file, the operation result is as follows:<br>When selecting the **Allow access** button<br>The target file can be viewed.<br>When selecting the **Deny access** button<br>The target file access is denied. The target file cannot be viewed.<br>When the client updates the target file, the operation result is as follows: An error about the operation result is not reported.<br>When selecting the **Allow access** button<br>The target file can be updated.<br>When selecting the **Deny access** button<br>The target file status returns to the status before the update and therefore the target file cannot be updated. |

| Item | Description |
|---|---|
| **Server monitoring interval** | Specify (in seconds) the polling interval to confirm the status of the scan server.<br>Specify from 1 to 86,400 seconds.<br>The default is 300. |
| **Cache size of scanning result** | Specify the size (in megabytes) of the cache that stores the information on files that were determined to be free of infection as the result of a virus scan.<br>Specify from 1 to 64.<br>The default is 8.<br>1 MB stores an amount of information equivalent to approximately 760 files. Files whose contents have not been changed from the information that is stored in the cache can be directly accessed without a virus scan. |

### 4.8.7 Starting and Stopping the Virus Scan Function

In the NAS Modular system, files that received read or write requests from the CIFS client are scanned for viruses when the virus scan function is started. Using the **List of Scanner Servers** window, you can start and stop the virus scan function for each NAS Unit so that the settings for each NAS Unit within the cluster are identical.

***Note:*** Before starting the virus scan function, the scan server must be registered in a NAS Modular system. For details on registering a scan server, see section 4.8.3.

To start and stop the virus scan function:

1. In the **Main Menu** window, click the **Virus Scan** button.

   The **List of Scanner Servers** window displays. For window details, see section 4.8.2.

2. To start the virus scan function, click the **Start** button. To stop it, click the **Stop** button.

   When the virus scan function starts, a confirmation dialog box for starting the function and prompting restart of the CIFS service appears. When the virus scan function stops, a confirmation dialog box for stopping the function appears.

3. Click the **OK** button.

   The virus scan function either starts or stops. Confirm the status of the virus scan function by looking in **Server status** in the **List of Scanner Servers** window.

## 4.9 Managing User Information

In the NAS Modular system, user IDs, group IDs, passwords, and other user information related to file system users can be managed using NAS Manager. Before registering a user in NAS Manager, make sure that the group to which the user will belong has been added to NAS Manager.

This section describes how the system administrator can register and delete user information in NAS Manager. The system administrator cannot use NAS Manager to view or change the user information managed by the NIS server or the LDAP server for user authentication.

### 4.9.1 Viewing User Information

A system administrator can use the **List of Users / Groups** (List of Users) window to view information about the users registered by NAS Manager.

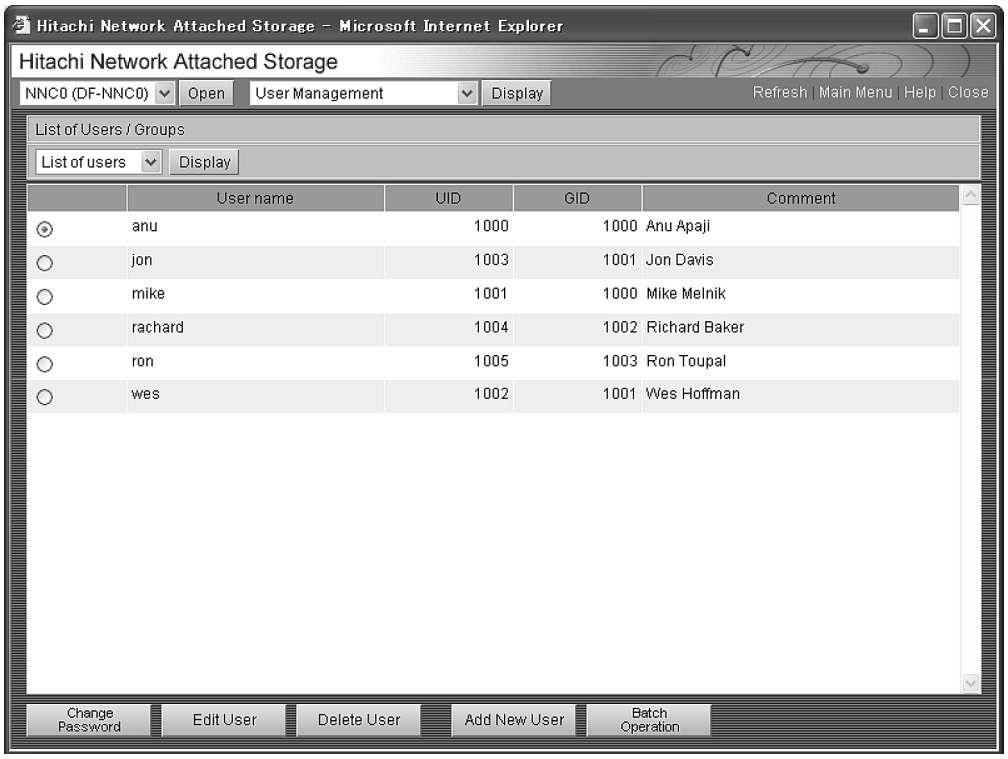



**Figure 4.72 List of Users / Groups Window**

To view user information:

1. In the **Main Menu** window, click the **User Management** button.

   The **List of Users / Groups** (List of Users) window displays.

2. From the **List of Users / Groups** (List of Groups) window, select **List of users** from the drop-down list, and then click the **Display** button. Following is a description of the window's contents:
   - **User name** User name
   - **UID** User ID
   - **GID** ID of the primary group to which the user belongs
   - **Comment** Note for the user (nothing is displayed unless a comment has been set)

### 4.9.1.1 Adding Users

In the Add User window shown below, you can add users. Make sure that there are no more than 2,000 users per cluster.

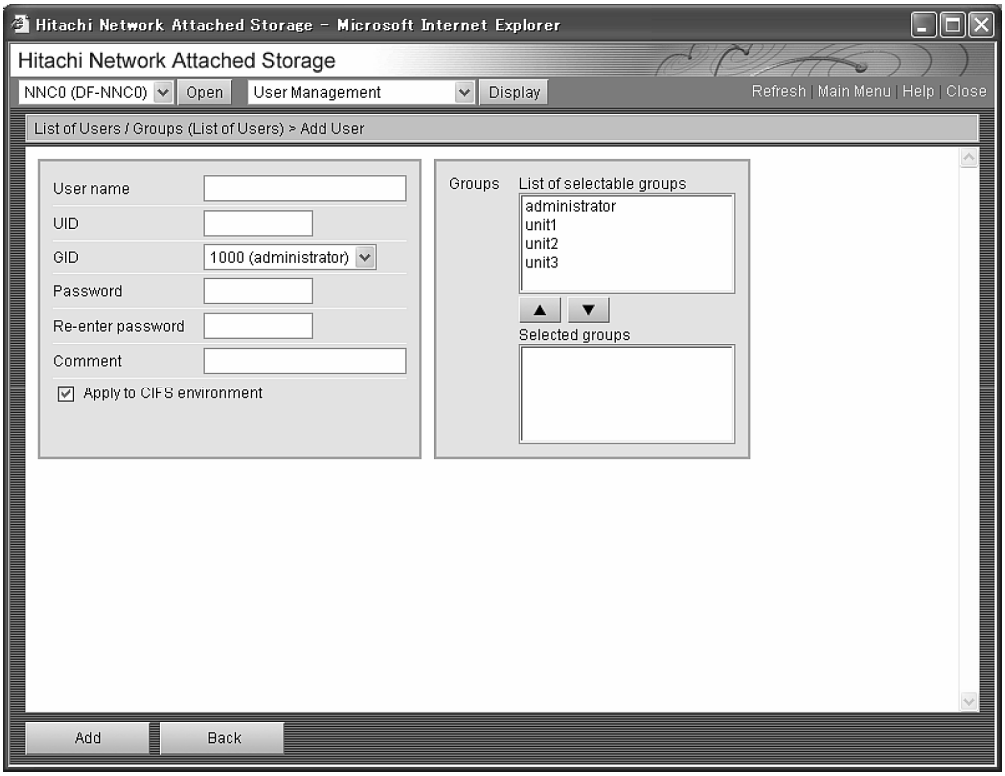



**Figure 4.73 Add User Window**

To add a user:

1. In the **Main Menu** window, click the **User Management** button.

   The **List of Users / Groups** (List of Users) window displays. For window details, see section 4.9.1. If the **List of Users / Groups** (List of Groups) window is active, select **List of users** from the drop-down list, and then click the **Display** button.

2. Click the **Add New User** button.

   The Add User window displays. Information about the window's contents is described in Table 4.43.

3. Enter the required information, and then click the **Add** button.

   The user is added and the **List of Users / Groups** (List of Users) window re-displays.

**Table 4.43 Information Specified in Add User Window**

| Item | Description |
|---|---|
| **User name** | Enter the user name. You cannot specify a user name that has already been registered by NAS Manager, the NIS server, or the LDAP server for user authentication.<br>Enter a maximum of 16 characters.<br>The first character must be an alphabetic character.<br>You can use any alphanumeric character, hyphen (-), and underscore (_) after the first character.<br>In Windows, the entered value is not case sensitive. Specify a name that is unique regardless of whether upper-case or lower-case alphabetic characters are used.<br>Also, you cannot specify a user name already reserved in the NAS OS.<br>The following are reserved NAS OS user names.<br>backup, bin, daemon, enasroot, ftp, games, gnats, identd, irc, list, lp, mail, majordom, man, msql, nasroot, news, nobody, operator, postfix, postgres, proxy, root, sshd, sync, sys, telnetd, uucp, and www-data |
| **UID** | Enter the user ID.<br>Specify a value from 104 to 2,147,483,147. You cannot specify 65534 or any other value already in use.<br>You cannot specify 65534 or any other value that has already been registered by NAS Manager, the NIS server, or the LDAP server for user authentication. In addition, when user mapping is being used, you cannot specify the user IDs within the ID range set by user mapping. |
| **GID** | From the drop-down list, select the ID of the primary group to which the user belongs. |
| **Password** | Enter the user password.<br>Specify from 6 to 8 (inclusive) characters. You can use any alphanumeric character, exclamation mark (!), quotation mark ("), number sign (#), dollar sign ($), percent sign (%), ampersand (&), apostrophe ('), left parenthesis ( (), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), forward slash (/), colon (:), semicolon (;), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left bracket ( [), backslash (\), right bracket (]), circumflex (^), underscore (_), grave accent (`), left brace ({), vertical bar (\|), right brace (}), and tilde (~). |
| **Re-enter password** | Re-enter the password you set in **Password**. |
| **Comment** | Enter a comment for the user.<br>Use a maximum of 32 characters.<br>You can use any alphanumeric character, number sign (#), percent sign (%), ampersand (&), apostrophe ('), left parenthesis ( (), right parenthesis ()), asterisk (*), plus sign (+), hyphen (-), period (.), forward slash (/), semicolon (;), left angle bracket (<), right angle bracket (>), question mark (?), at mark (@), left bracket ( [), right bracket (]), circumflex (^), underscore (_), left brace ({), vertical bar (\|), right brace (}), and tilde (~). You can also specify spaces, but not at the beginning or end of the character string.<br>This item is optional. |
| **Apply to CIFS environment** | Select this check box when you want to add the user as a user of CIFS shares. |
| **Groups** | Using the **List of selectable groups** list box, specify the groups to which the user belongs.<br>Up to 32 groups can be specified per user.<br>Select a group, then click the button to add that group to the **Selected groups** list box.<br>When you click the ▼ button, the groups selected in **List of selectable groups** are added to the **Selected groups** list box. Only groups listed in the **Selected groups** list box will be set as groups to which the user belongs.<br>To delete a group from the **Selected groups** list box, select the group and click the button. |

### 4.9.1.2 Editing User Information

In the Edit User window shown below, you can edit user information. After editing, current settings remain for unchanged items.

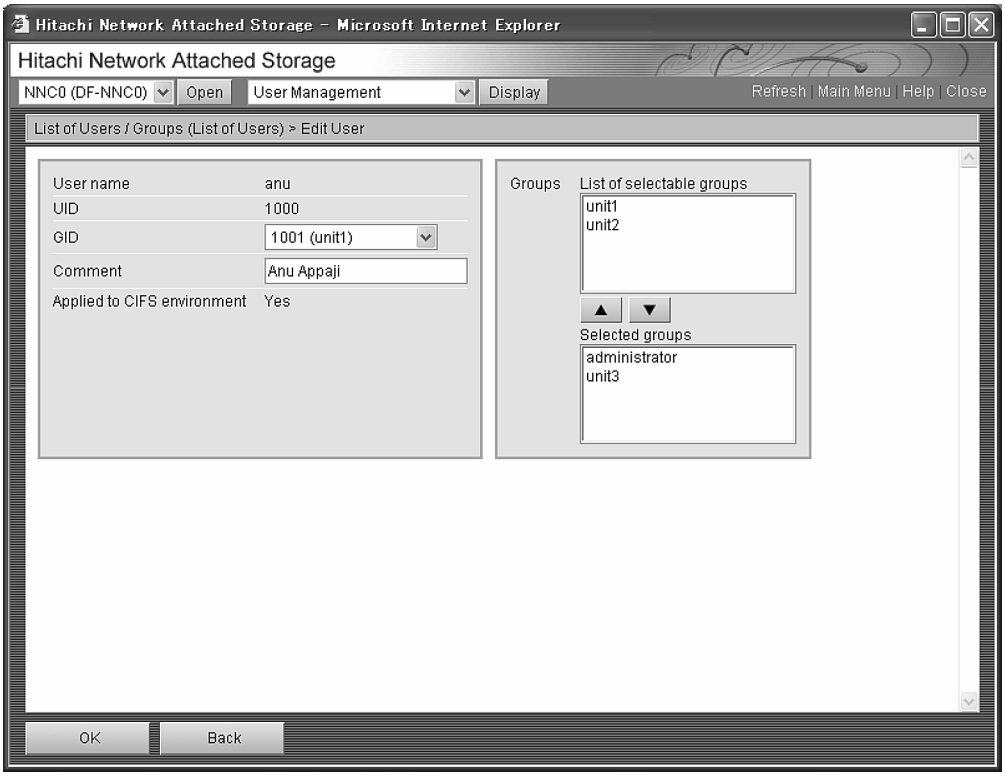



**Figure 4.74 Edit User Window**

To edit user information:

1. In the **Main Menu** window, click the **User Management** button.

   The **List of Users / Groups** (List of Users) window displays. For window details, see section 4.9.1. Select **List of users** from the drop-down list, and then click the **Display** button.

2. Use a radio button to select the user you want to edit, and then click the **Edit User** button.

   The Edit User window displays. Information about the window's contents is described in Table 4.44. Enter the required information, and then click the **OK** button.

**Table 4.44 Information Specified in Edit User Window**

| Item | Description |
|---|---|
| **GID** | From the drop-down list, select the ID of the primary group to which the user belongs. |
| **Comment** | Enter a comment for the user. This item is optional. |
| **Groups** | Use the **List of selectable groups** list box to select the groups to which the user belongs. Up to 32 groups |

| Item | Description |
|---|---|
| | can be specified per user.<br>When you click the ▼ button, the groups selected in **List of selectable groups** are added to the **Selected groups** list box. Only groups listed in the **Selected groups** list box will be set as groups to which the user belongs.<br>To delete a group from the **Selected groups** list box, select the group and click the ▲ button. |

### 4.9.1.3 Changing a Password

You can use the **Change Password** (user setup) window to modify a password.

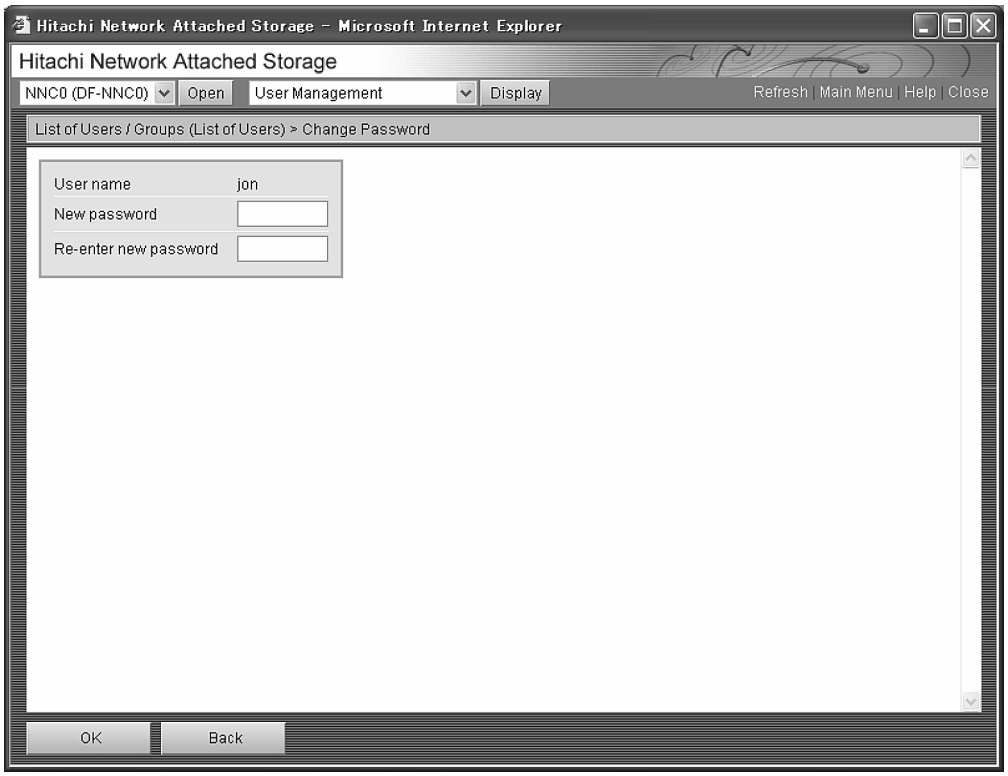



**Figure 4.75 Change Password (User Setup) Window**

To change a password:

1. In the **Main Menu** window, click the **User Management** button.

   The **List of Users / Groups** (List of Users) window displays. For window details, see section 4.9.1. If the **List of Users / Groups** (List of Groups) window is active, select **List of users** from the drop-down list, and then click the **Display** button.

2. Use a radio button to select the user you want to edit, and then click the **Change Password** button.

   The **Change Password** (user setup) window displays.

3. Enter the required information listed below, and then click the **OK** button:
   - **New password** Enter the new password.
   - **Re-enter new password** Re-enter the password you set in **New password**.

   The password is changed and the **List of Users / Groups** (List of Users) window re-displays.

#### 4.9.1.4 Deleting Users

In the **List of Users / Groups** (List of Users) window, you can delete users individually, whether they were registered individually or in a **Batch Operation**.

To delete a user:

1. In the **Main Menu** window, click the **User Management** button.

   The **List of Users / Groups** (List of Users) window displays. For window details, see section 4.9.1. If the **List of Users / Groups** (List of Groups) window is active, select **List of users** from the drop-down list, and then click the **Display** button.

2. Use a radio button to select the name of the user you want to delete, and then click the **Delete User** button.

   A dialog box confirms that you want to delete the user.

3. Click the **OK** button.

   The selected user is deleted.

#### 4.9.1.5 Registering and Deleting User Information as a Batch Operation

In the **Batch Operation** window, you can register or delete settings for multiple users as a **Batch Operation**. To register or delete user information in a batch, you must first prepare a CSV-formatted file containing the user information. The password information, which is provided for users who are to be registered, is also contained in the CSV-formatted file. Manage the file carefully. This file is loaded by using the **Batch Operation** window.

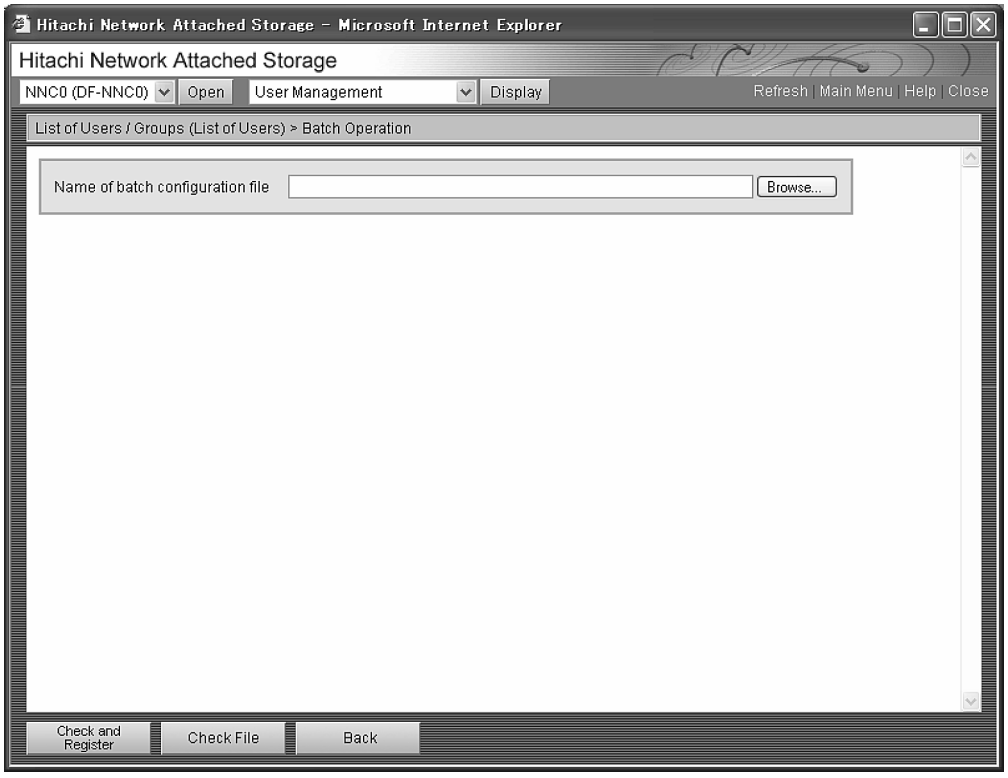



**Figure 4.76 Batch Operation Window**

Example of registering user information concurrently using a CSV file:

```
#execution-category, process-category, registration-target, user-name, UID, GID, password,
comment, groups
Data,UA01,3,username,105,105,password,fullname,"106,107,108"
```

Example of deleting user information concurrently using a CSV file:

```
#execution-category, process-category,, user-name
Data,UD01,,username
```

Specify the path name of the CSV file with a maximum of 512 characters. You can use alphanumeric characters, hyphens (-), underscores (_), and periods (.) to specify a file name.

The following table lists and describes the information to be specified in a CSV file for registering and deleting user information in a batch:

**Table 4.45 Information Specified for Batch Registration or Deletion of User Data**

| Item | When Registering | When Deleting | Description |
|---|---|---|---|
| Execution category | Required | Required | Specify the execution category of the data.<br>Write as `Data`.<br>Specify # for a comment line. |
| Process category | Required | Required | Specify the data process category. |

| Item | When Registering | When Deleting | Description |
|---|---|---|---|
| | | | UA01 Batch-register the data.<br>UD01 Batch-delete the data.<br>UA01 and UD01 cannot exist within the same file. |
| Registration target | Required | Not Required | Specify where to register or apply the user information.<br>1 Register the data using NAS Manager<br>3 Register the data by NAS Manager and apply the user information to the CIFS environment. |
| User name | Required | Required | Specify the user name.<br>The values that can be specified are the same as those that can be specified in **User name**, in the Add User window. For more details about specifiable values, see section 4.9.1.1. |
| UID | Required | Not Required | Specify the user ID.<br>The values that can be specified are the same as those that can be specified in **UID**, in the Add User window. For more details about specifiable values, see section 4.9.1.1. |
| GID | Required | Not Required | Specify the ID of the primary group to which the user belongs. |
| Password | Required | Not Required | Specify the user password.<br>The values that can be specified are the same as those that can be specified in **Password**, in the Add User window. For more details about specifiable values, see section 4.9.1.1. |
| Comment | (If Needed) | Not Required | Enter a comment for the user.<br>The values that can be specified are the same as those that can be specified in **Comment**, in the Add User window. For more details about specifiable values, see section 4.9.1.1. |
| Groups | (If Needed) | Not Required | Specify the secondary groups to which the user belongs by group name or group ID.<br>Use commas to delimit multiple group names or group IDs, and enclose the entire string with quotation marks ("). |

***Note:*** In the **Batch Operation** window, you can run an error check on the user information specified in a CSV file by clicking the **Check File** button.

To register or delete user information in a batch:

1. In the **Main Menu** window, click the **User Management** button.

   The **List of Users / Groups** (List of Users) window displays. For window details, see section 4.9.1. If the **List of Users / Groups** (List of Groups) window is active, select **List of users** from the drop-down list, and then click the **Display** button.

2. Click the **Batch Operation** button.

   The **Batch Operation** window displays.

3. In **Name of batch configuration file**, enter the path of the CSV file containing the user information.

   To browse a list of file names, click the **Browse** button.

4. Click the **Check and Register** button.

   An error check is performed on the user information written in the CSV file. If the file contains an error, user information will not be batch registered or batch deleted. If no errors are detected, the user information will be batch registered or batch deleted.

   To perform an error check on the file without actually registering or deleting the user information, click the **Check File** button.

   To cancel the operation during an error check, click the **Stop** button.

   When processing finishes, a result message displays. At the same time, the download window will appear, and then a Web browser download dialog box will appear to download the CSV file that records the execution results.

5. In the dialog box, specify where to download the file.

   The CSV file is downloaded to the specified location.

   The execution result is recorded in the execution category of the CSV file. `#Completed` is recorded when batch registration and batch deletion succeeds, `OK` is recorded when the error check result is normal, and `NG` is recorded when an error occurs.

6. Click the **Close** button in the download window.

   The download window closes.

7. Click the **OK** button.

   If an error occurs, the **Batch Operation** window re-displays. If batch registration or batch deletion has finished, the **List of Users / Groups** (List of Users) window re-displays. Depending on the number of users to be registered or to be deleted, it might take a long time to finish the operation.

#### 4.9.1.6 Correcting Errors in User Information for Batch Registration or Deletion

When batch registration or batch deletion finishes successfully, the execution category of the corresponding data is changed to `#Completed`.

When an incorrect line exists in the specified CSV file, batch registration or batch deletion fails. In such a case, in the line where there is an error, the execution category of the line is changed from the execution category (for example, `Data)` to `NG`(*error-message*). Following is an example:

```
#execution-category, process-category, registration-target, user-name, UID,
GID, password, comment, groups
NG(The specified UID is already
registered),UA01,1,hitachi,1000,1000,Hitachi,,1001
```

Correct all the lines that display `NG`(*error-message*) in the CSV file, then re-run the batch registration or batch deletion.

The following table explains the error messages, error causes, and the corrective actions to take when an error occurs during batch registration or batch deletion:

**Table 4.46 Batch Registration Error Messages, Causes, and Corrective Actions**

| Error Message | Error Cause | Action |
|---|---|---|
| An attempt to acquire an exclusion resource failed | An internal error occurred:<br>▪ You could not obtain an exclusive resource (a timeout occurred). | Re-run batch registration of the user information. If the error occurs repeatedly, download all the management log files and then contact your HDS representative. For details on how to download log files, see section 4.13.10. |
| An attempt to register failed | An internal error occurred:<br>▪ You could not obtain an exclusive resource (a timeout does not cause the error).<br>▪ The GID of the group to which the user belongs could not be converted into the group name (file operations might fail or group information might not exist).<br>▪ The user registration command failed. | Re-rune batch registration of the user information. If the error occurs repeatedly, download all the management log files and then contact your HDS representative. For details on how to download log files, see section 4.13.10. |
| The affiliation group name value is incorrect | The group name or GID specified in the Groups could not be found. | Check the Groups. |
| The comment is incorrect | The comment is incorrect. The value might contain a character that cannot be used or the value length might be incorrect. | Check the comment. The valid length of the comment is from 1 to 32 characters. You can also leave the comment blank. |
| The data classification value is incorrect | The value specified in the process category is incorrect. | Check the value specified in the process category. Specify `UA01` in the process category. |
| The data registration destination value is incorrect | The data registration destination value is incorrect. | Check the data registration destination value. Specify `1` or `3` in the data registration destination value. |
| The execution classification value is incorrect | The value specified in the execution category is incorrect. | Check the value specified in the execution category. Specify `Data` or `#` in the execution category. |
| The GID value is incorrect | The GID value is incorrect or a group within the specified GID cannot be found. The value might contain a character that cannot be used or the specified value may be out of range. | Check the GID. The valid range of the value is from 104 to 2,147,483,147. However, you cannot use 65,534. |
| The number of elements is invalid | The number of elements for batch registration specified in the CSV file is incorrect. | Check the number of elements for batch registration. The number of elements for batch registration is from 7 to 9. |
| The password is incorrect | The specified password is incorrect. The password might contain a character that cannot be used or the value length might be incorrect. | Check the password. The length of the password is from 6 to 8 characters. |
| The same UID registration (or deletion) specification exists in the file | The same UID exists in the CSV file. | Check the UID. |

| Error Message | Error Cause | Action |
|---|---|---|
| The same user registration (or deletion) specification exists in the file | The same user name exists in the CSV file. | Check the user name. |
| The specified UID is already registered | The specified UID has already been registered. | Check the UID. |
| The specified user is already registered | The specified user name has already been registered. | Check the user name. |
| The UID value is incorrect | The UID value is incorrect. The value might contain a character that cannot be used or the or the specified value may be out of range. | Check the UID. The valid range of the value is from 104 to 2,147,483,147. However, you cannot use 65,534. |
| The user name value is incorrect | The user name value is incorrect. The value might contain a character that cannot be used or the value length might be incorrect. | Check the correct user name. The valid length of the value is from 1 to 16 characters. |
| The specified user name is already specified for a group name registered in the CIFS ACL environment | The specified user name is the same as the group name registered in the CIFS (ACL) environment. | Specify another user name. |
| An attempt to acquire an exclusion resource failed | An internal error occurred:<br>▪ You could not obtain an exclusive resource (a timeout occurred). | Re-run batch deletion of user information. If the error occurs repeatedly, download all the Management log files and then contact your HDS representative. For details on how to download log files, see section 4.13.10. |
| An attempt to delete failed | An internal error occurred.<br>▪ The user deletion command failed. | Re-run batch deletion of user information. If the error occurs repeatedly, download all the Management log files and then contact your HDS representative. For details on how to download log files, see section 4.13.10. |
| An attempt to register failed | An internal error occurred:<br>▪ You could not obtain an exclusive resource (a timeout does not cause the error). | Re-run batch deletion of user information. If the error occurs repeatedly, download all the Management log files and then contact your HDS representative. For details on how to download log files, see section 4.13.10. |
| The data classification value is incorrect | The value specified in the process category is incorrect. | Check the value specified in the process category. Specify `UD01` in the process category. |
| The execution classification value is incorrect | The value specified in the execution category is incorrect. | Check the value specified in the execution category. Specify `Data` or # in the execution category. |
| The number of elements is invalid | The number of elements for batch deletion specified in the CSV file is incorrect. | Check the number of elements for batch deletion.<br>For batch deletion of user information, assume four elements as shown below:<br>*#execution-category*, *process-category*, *user-name*<br>`Data,UD01,,username` |
| The same user registration (or deletion) specification exists in the file | The same user name exists in the CSV file. | Check the user name. |

| Error Message | Error Cause | Action |
|---|---|---|
| The specified user is already deleted | The specified user name has not been registered. | Check the user name. |
| The user name value is incorrect | The user name value is incorrect. The value might contain a character that cannot be used or the value length might be incorrect. | Check the user name. The valid length of the value is from 1 to 16 characters. |

## 4.9.2 Managing Group Information

A system administrator can use the **List of Users / Groups** (List of Groups) window to view information about the groups registered by NAS Manager.

### 4.9.2.1 Viewing Group Information

In the **List of Users / Groups** (List of Groups) window shown below, you can view group information registered in the system. However, groups registered in the NIS server and groups registered by user mapping are not displayed.

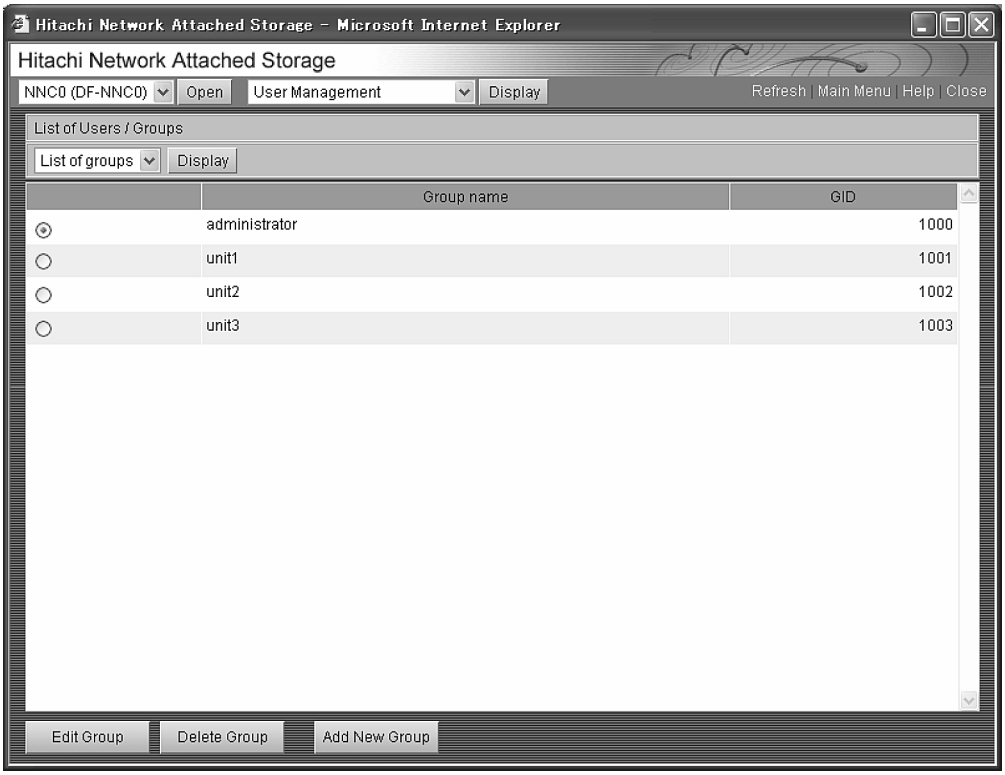



**Figure 4.77 List of Users / Groups Window**

The following list describes the window's contents:

- **Group name** Name of the group
- **GID** Group ID

To view group information:

1. In the **Main Menu** window, click the **User Management** button.

   The **List of Users / Groups** (List of Users) window displays. For window details, see section 4.9.2.1.

2. Select **List of groups** from the drop-down list, and then click the **Display** button.

   The **List of Users / Groups** (List of Groups) window displays.

### 4.9.2.2 Adding Groups

You can use the **Add Group** window to add a group. Ensure that there are no more than 2,000 groups per cluster.

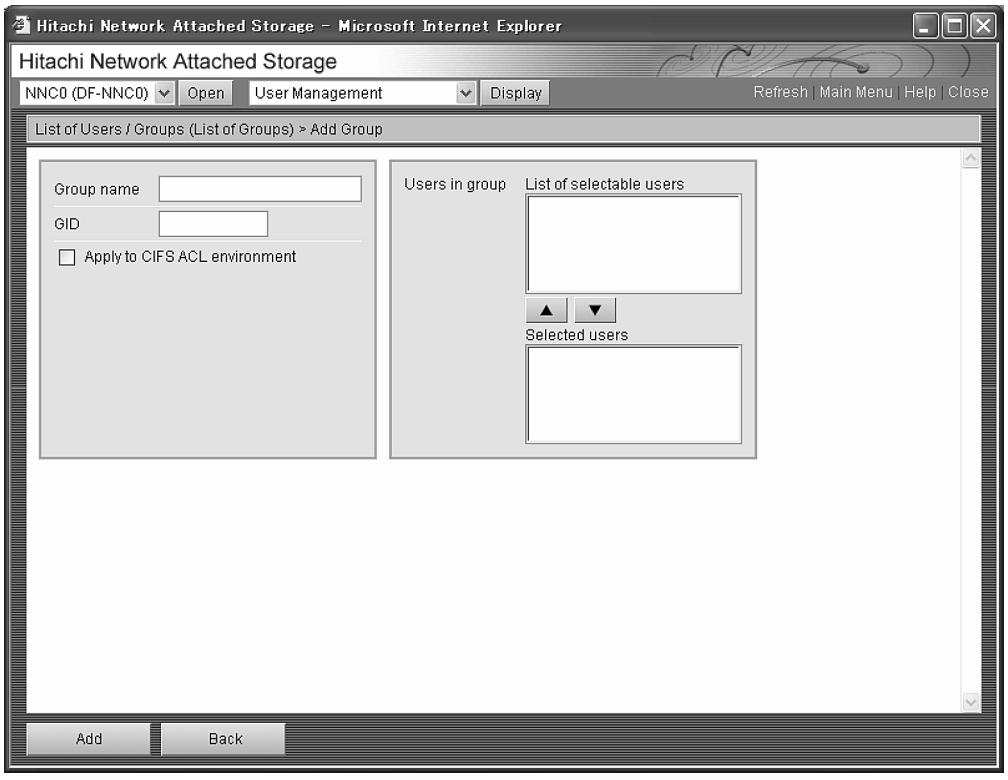



**Figure 4.78 Add Group Window**

To add a group:

1. In the **Main Menu** window, click the **User Management** button.

   The **List of Users / Groups** (List of Users) window displays. For window details, see section 4.9.1.

2. Select **List of groups** from the drop-down list, and then click the **Display** button.

   The **List of Users / Groups** (List of Groups) window displays. For window details, see section 4.9.2.1.

3. Click the **Add New Group** button.

   The **Add Group** window displays Information about the window's contents is described in Table 4.47.

4. Enter the required information, and then click the **Add** button.

   The group is added and the **List of Users / Groups** (List of Groups) window re-displays.

**Table 4.47 Information Specified in Add Group Window**

| Item | Description |
|---|---|
| **Group name** | Enter the group name. You cannot enter any group name that has already been registered by NAS Manager, the NIS server, or the LDAP server for user authentication.<br>Enter a maximum of 16 characters.<br>The first character must be an alphabetic character.<br>You can use any alphanumeric character, hyphen (-), and underscore (_) after the first character.<br>In Windows, the entered value is not case sensitive. Specify a name that is unique regardless of whether upper-case or lower-case alphabetic characters are used.<br>When the entered name and the name specified in **User name** in the Add User window are the same, the ACL will not be set even though the **Apply to CIFS ACL environment** check box is selected.<br>Also, you cannot specify a group name already reserved in the NAS OS.<br>The following are reserved NAS OS group names.<br>adm, audio, backup, bin, cdrom, daemon, dialout, dip, disk, enasroot, fax, floppy, ftp, games, gnats, irc, kmem, list, lp, mail, majordom, msql, nasroot, news, nogroup, operator, postdrop, postfix, postgres, proxy, root, shadow, src, staff, sudo, sys, tape, telnetd, tty, users, utmp, uucp, video, voice, and www-data |
| **GID** | Enter the group ID.<br>You cannot specify 65534 or any other value that has already been registered by NAS Manager, the NIS server, or the LDAP server for user authentication. In addition, when user mapping is being used, you cannot specify the group IDs within the ID range set by user mapping. |
| **Apply to CIFS ACL environment** | Select this check box when setting an ACL for the adding group. |
| **Users in group** | In the **List of selectable users** list box, specify the users who belong to this group.<br>Make sure that there are no more than 2,000 users per group.<br>When you click the ▼ button, the users selected in the **List of selectable users** list box are added to the **Selected users** list box. Only users listed in the **Selected users** list box will be set as members of this group.<br>To delete a group member listed in the **Selected users** list box, select the user and then click the button. |

### 4.9.2.3 Editing Group Information

You can use the Edit Group window to edit group information. After editing, current settings remain for unchanged items.

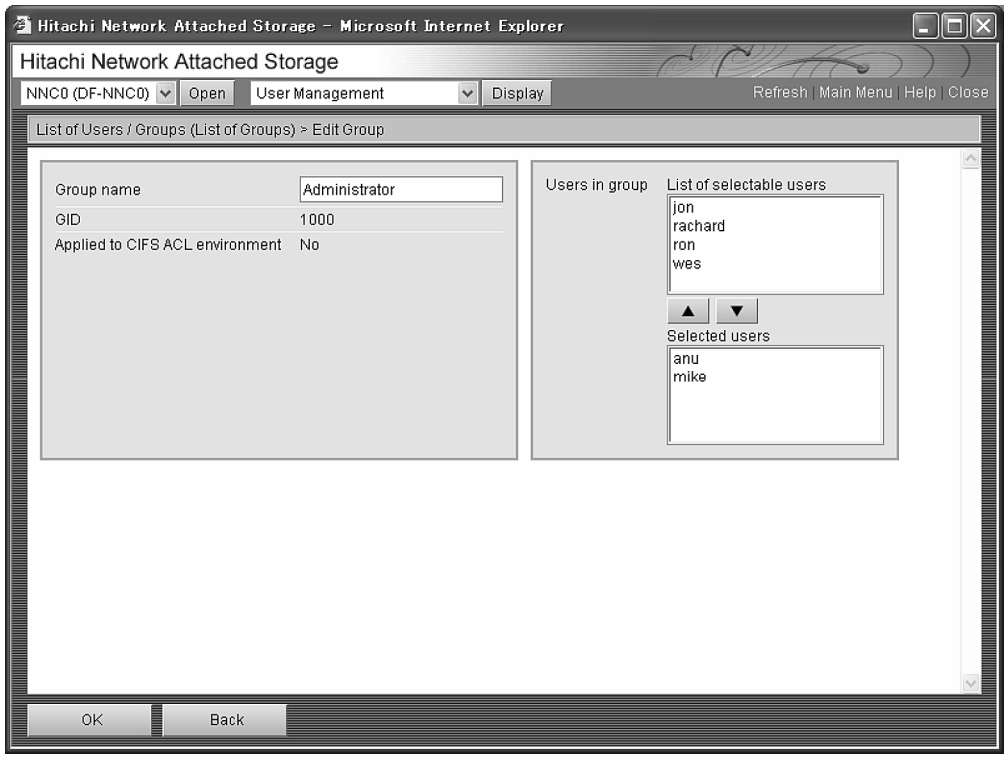



**Figure 4.79 Edit Group Window**

To edit group information:

1. In the **Main Menu** window, click the **User Management** button.

   The **List of Users / Groups** (List of Users) window displays. For window details, see section 4.9.1.

2. Select **List of groups** from the drop-down list, and then click the **Display** button.

   The **List of Users / Groups** (List of Groups) window displays. For window details, see section 4.9.2.1.

3. Use a radio button to select the group to be edited, and then click the **Edit Group** button.

   The Edit Group window appears. Following is information about the window's contents:

   - **Group name** Enter the group name (the group name cannot be changed when **Apply to CIFS ACL environment** is set to **Yes**).
   - **Users in group** In the **List of selectable users** list box, select a user who belongs to this group, then click the ▼ button to add that user to the **Selected users** list box. Only users listed in the **Selected users** list box will be set as members of this group. There can be no more than 2,000 users per group.

To delete a group member, select the user and click the ▲ button.

4. Enter the required information, and then click the **OK** button to update group data.

   The **List of Users / Groups** (List of Groups) window re-displays.

#### 4.9.2.4 Deleting Group Information

You can use the **List of Users / Groups** (List of Groups) window to delete a group.

To delete a group:

1. In the **Main Menu** window, click the **User Management** button.

   The **List of Users / Groups** (List of Users) window displays. For window details, see section 4.9.1.

2. Select **List of groups** from the drop-down list, and then click the **Display** button.

   The **List of Users / Groups** (List of Groups) window displays. For window details, see section 4.9.2.1.

3. Use a radio button to select the name of the group you want to delete, and then click the **Delete Group** button.

   A dialog box confirms that you want to delete the group.

4. Click the **OK** button.

   The selected group is deleted.

### 4.10 Managing File Systems

This section describes how you can use the NAS Manager GUI to create, mount, and unmount file systems. In NAS Manager, you can create a file system from multiple device files. When using multiple device files, use a logical volume manager. In NAS Manager, an LVM is used as a volume manager.

Before beginning to manage a file system, the system administrator must check the following:

- Managing the warning notification related to file system usage see 5.5.7.
- Managing automatic failover if a file system becomes blocked, see 5.5.8.
- Managing the settings for recording the file creation time (settings for existing file systems), see 5.5.9.

#### 4.10.1 Note on Device files to be used

You must carefully consider the purpose of the file system, drive characteristics, and other matters to determine the device files to be used for the file system.

A SATA drive and an FC drive have different I/O performance levels and processing speeds.

Before using device files in the NAS Modular system, the system administrator must use Storage Navigator Modular to allocate a user LU to the NAS Unit. For details on how to allocate a user LU, see the manuals for disk array.

### 4.10.2 Allocating a Device File

For a file system, the system administrator must use device files to which the controller for the local node is assigned as the default controller.

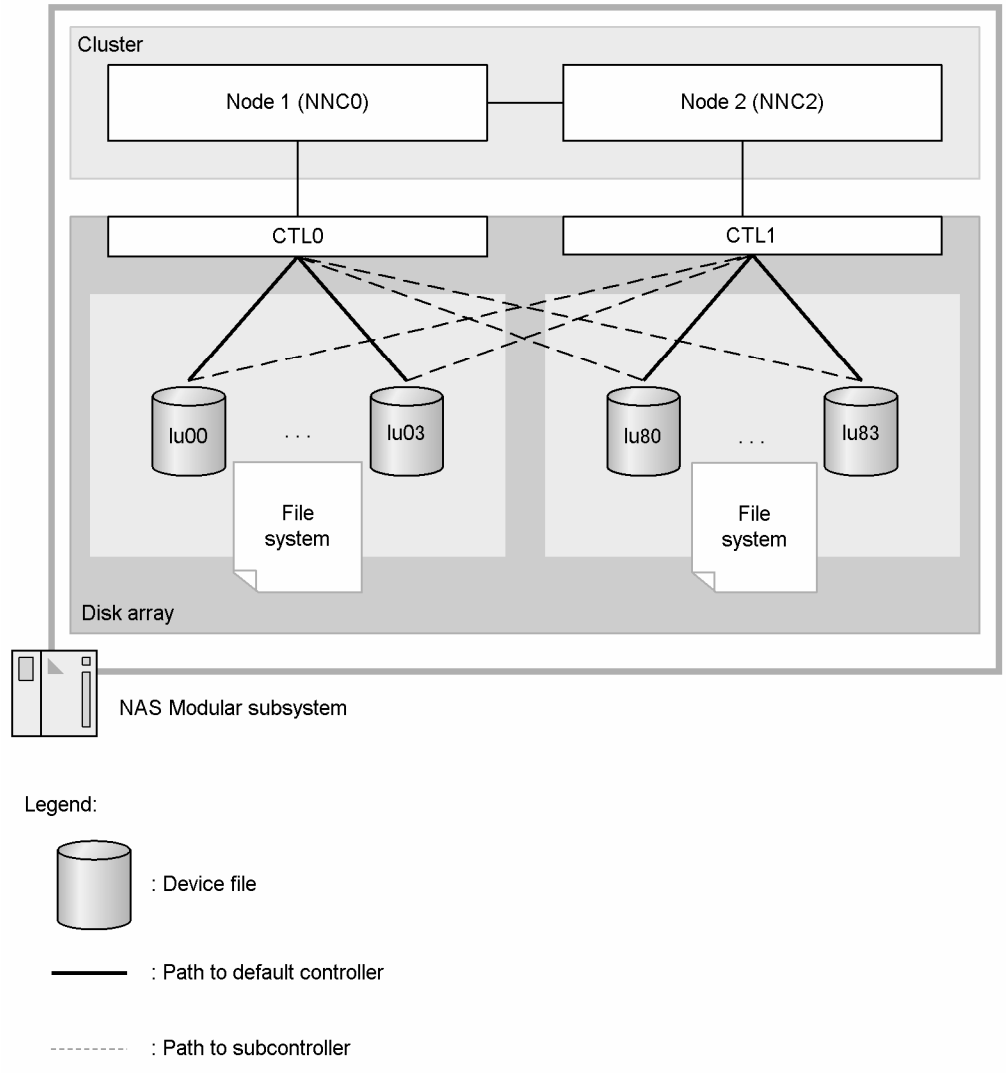



**Figure 4.80 Assigning Device FilesUsed for File System (TagmaStore AMS 500)**

For the file system to be created in Node 1 (NNC0), use device files to which CTL0 is assigned as the default controller. For the file system to be created in Node 2 (NNC2), use device files to which CTL1 is assigned as the default controller.

**Note:** If you use a device file that is assigned to the controller of the other node, the I/O performance and processing speed of the NAS Unit may decrease. Before creating the file system, use Storage Navigator Modular to check the default controllers of the device files to be used. For details on how to assign device files and how to check the default controllers, see the manual *Storage Navigator Modular User's Guide*.

### 4.10.3 Planning File System Capacity

In a NAS Modular system, a file system can be created with a capacity from 128 MB and up to (but not including) 2 TB. This section describes the concept of file system capacity, which differs between cases when LVM is used, and when it is not.

**Using LVM**

When LVM is used, each device file requires 33 MB for header information. To calculate the total available file system capacity, first subtract the 33 MB for the header information, and then divide the remaining amount by 32 MB (the required size for each unit of file system capacity). Then, round down the result to the nearest whole integer, and multiply the result by 32 MB. For example, when the device file capacity is 128 MB, 33 MB is used for header information, leaving 95 MB. Dividing 95 MB by 32 MB and rounding down gives a result of 2. Then, if you multiply 2 by 32MB, the maximum space available for file system capacity is 64 MB. The remaining 31 MB (95 MB minus 64 MB) cannot be used for file system capacity.

Figure 4.81 illustrates the space available for file system capacity when the device file capacity is 128 MB.

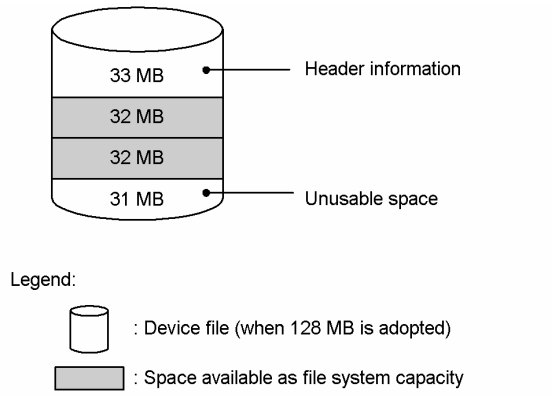



**Figure 4.81 File System Capacity when LVM is Used**

A file system cannot be created with LVM when the device file capacity is less than 65 MB (33 MB plus 32 MB). When the capacity of each device file is assumed to be n (in megabytes), the file system capacity can be calculated as follows:

$$\downarrow \frac{n - 33}{32} \downarrow \times 32 \times \text{the number of device files} \quad \text{(MB)}$$

Legend:

↓ ↓ : Truncates the figures after the decimal point
n : Capacity for each device file

**Not Using LVM**

Divide the device file size by the specified size for each unit of file capacity (you specify this in **Size of file system division** in the **Create New File System** window). Then, round down the result to the nearest whole integer, and multiply the result by 32 MB. You can use that multiple for the device file capacity. If the remaining amount is 16 MB or more, that amount is also available for the device file capacity (this means the entire device file area can be used).

For example, when the device file capacity is 150 MB and you select 32 MB for the file system division size, dividing 150 MB by 32 MB and rounding down gives a result of 4. Then if you multiply by 32 MB, the multiple amount is 128 MB. As the remaining amount is 22 MB (more than 16 MB), this amount can also be used, and the space available for file system capacity is 150 MB.

#### 4.10.3.1 Guidelines for Managing a File System using an External System

Considering the importance and purpose of a file system, you must determine the device file to be used. When using a device file in the external system, note the following:

- When you use an external system, as compared with using a local disk system, there is a higher possibility of operational mistakes causing errors in the device file (operational mistakes such as starting the NAS OS while the external system is not running, or disconnecting the cable connecting the local disk system and the external system). If an error occurs in the external system, deletion of the file system might be necessary.
- For high file system performance, create a file system that is made up of device files in the local disk system. We do not recommend that a file system be managed by using an external system.
- Do not use device files of different disk systems for a file system. Use Storage Navigator to check which disk system contains the device file, before creating a file system.

### 4.10.4 Viewing File System Information

In the **List of File Systems** window, the system administrator can view file system information.

When NAS Sync Image is used, you can also view information on differential-data snapshots that have been created and mounted using NAS Sync Image.

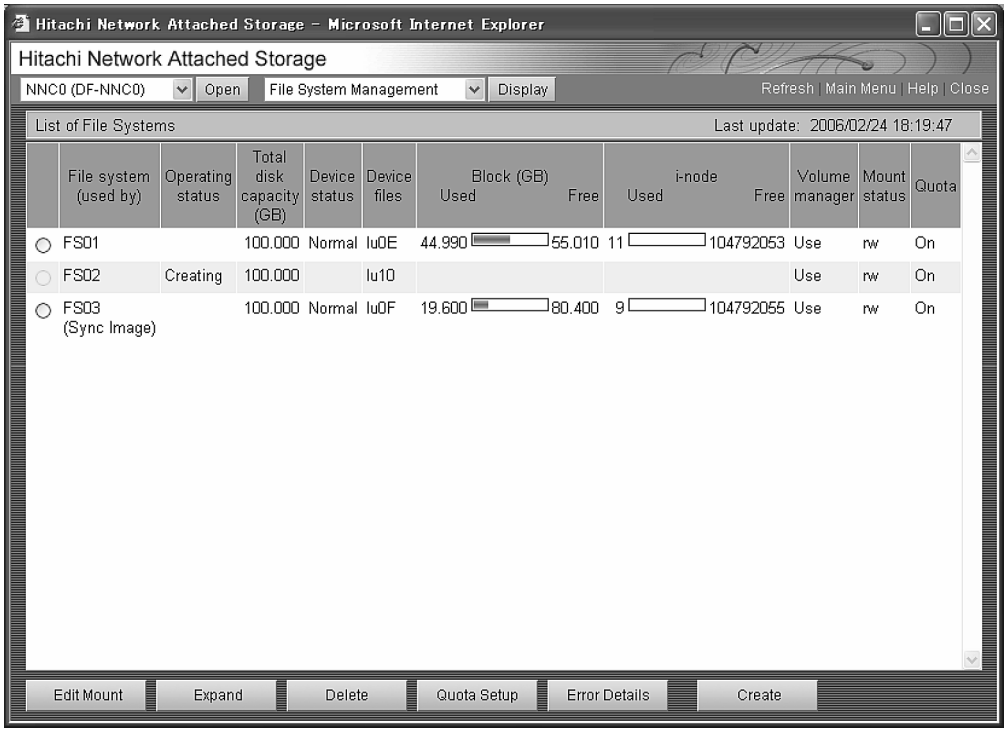



**Figure 4.82 List of File Systems Window**

The following table lists and describes the information displayed in the **List of File Systems** window:

**Table 4.48 Contents of List of File Systems Window**

| Item | Description |
|---|---|
| **Last update** | The date and time the information displayed in the window was last updated. |
| **File system (used by)** | The name of the file system.<br>When using NAS Sync Image to create or mount a differential-data snapshot, the mount point directory name of the snapshot is displayed as follows:<br>*differential-data-snapshot-mount-point-directory-name*(Sync Image)<br>The file system for which a differential-data storage device has been set by using NAS Sync Image is displayed as follows:<br>*file-system-name*(Sync Image) |
| **Operating status** | The status of the creation or mounting of a file system.<br>Creating<br>Processing to create the file system is waiting to be executed or is being executed.<br>Mounting<br>The mounting of the file system is waiting for execution or being used.<br>Error<br>The attempt to create or mount the file system terminated abnormally after it was queued, or a warning message has been output.<br>Take action, following the procedure in section 4.10.2.<br>When creation or mounting of the file system has terminated normally, nothing is displayed. |

| Item | Description |
|---|---|
| **Total disk capacity (GB)** | The capacity of the file system.<br>For NAS Sync Image differential-data snapshots, the capacity of the creation-source file system is displayed. |
| **Device status** | The status of the device files that comprise the file system.<br>For NAS Backup Restore snapshots, the status of the device files that comprise the copy device is displayed.<br>For NAS Sync Image differential-data snapshots, the status of the device files that comprise the differential-data storage device and creation source file system is displayed.<br>The following shows the information displayed.<br>▪ `Normal` The status is not blocked.<br>▪ `Error` The status is blocked. Check the information displayed in **Mount status**, and act accordingly.<br>If the **Operating status** changes from `mounting` to `error`, `normal` is displayed as the **Device status**. |
| **Device files** | The name of the device files used on the file system. Drive type information is not displayed.<br>For NAS Sync Image differential-data snapshots, the names of the device files used on the creation-source file system and differential-data storage device are displayed. The device files used on the creation-source system are displayed, followed by the device files used on the differential-data snapshot. |
| **Block (GB)** | Used and free block space.<br>The color of the indicator changes depending on the percentage of block space being used. Blue indicates usage of less than or equal to 70 %, yellow indicates usage of more than 70 % but less than or equal to 80 %, and red indicates usage of more than 80 % but less than or equal to 100 %.<br>This will not be displayed in the following cases:<br>▪ When the device file or file system is blocked<br>▪ When the file system is not mounted<br>▪ When the capacity of the NAS Sync Image differential-data storage device is insufficient |
| **i-node** | Within the space currently available for i-nodes usage, the number of i-nodes being used and the number of i-nodes not being used are displayed.<br>The color of the indicator changes depending on the percentage of the number of i-nodes being used. Blue indicates usage of less than or equal to 70 %, yellow indicates usage of more than 70 % but less than or equal to 80 %, and red indicates usage of more than 80 % but less than or equal to 100 %.<br>This will not be displayed in the following cases:<br>▪ When the device file or file system is blocked<br>▪ When the file system is not mounted<br>▪ When the capacity of the NAS Sync Image differential-data storage device is insufficient |
| **Volume Manager** | Whether the file system is using a volume manager or not.<br>The following shows the information displayed:<br>▪ `Use` A volume manager is being used.<br>▪ **--** A volume manager is not being used.<br>For NAS Sync Image differential-data snapshots, `Use` is displayed. |

| Item | Description |
|---|---|
| **Mount status** | The mount status of the file system.<br>For NAS Sync Image differential-data snapshots, the status of the currently mounted differential-data snapshot is displayed.<br>▪ `ro` Read-only.<br>▪ `rw` Read/write.<br>▪ `Overflow` The capacity of the NAS Sync Image differential-data storage device is insufficient.<br>▪ `Error` The status is blocked. Mount the file system again after unmounting. Run the mount operation again. If this does not clear the blocked status, contact your HDS representative.<br>If this is displayed for the NAS Sync Image differential-data snapshot, see the *Hitachi AMS/WMS NAS Sync Image User's Guide*.<br>▪ `fatal error` The status is blocked. Delete the file system, and contact your HDS representative. For details on deleting a file system, see section 4.10.9.<br>`Not available`<br>▪ This is displayed if an error has occurred in the differential-data storage device for NAS Sync Image. This may also be displayed if a failover has occurred or the resource group has stopped. If you cannot identify the error, contact maintenance personnel.<br>▪ **--** The item is not mounted. |
| **Quota** | The Quota setting when the file system was mounted.<br>For NAS Sync Image differential-data snapshots, the Quota setting when the differential-data snapshot was created is displayed.<br>The following shows the information displayed.<br>▪ `On` Quota setup enabled.<br>▪ `Off` Quota setup disabled.<br>▪ **--** The item is not mounted.<br>If the device file or file system is currently blocked, the status before the error occurred is displayed.<br>Additionally, when `Off` appears after a failure, one of the following has occurred:<br>▪ The Quota setting that was applied before the failure was disabled, and operations continued.<br>▪ The Quota setting from before the failure was enabled, and operations continued. However, the status was changed when, for example, an unmount operation was performed after the failure. |

***Note:*** The drive types of the device files that comprise a file system can be checked in the following ways:

- Use Storage Navigator Modular to view LU information:

  For details on how to do this, see the *Storage Navigator Modular User's Guide*.

- Use the **Expand File System** window to view the device file information displayed in **Device files being used**:

  For details on the **Expand File System** window, see section 4.10.6.

- Use the `enas_fslist` command to output information on the file system:

  For details on `enas_fslist`, see Chapter 6.

To view file system information:

1. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window appears.

2. To display the latest status, click **Refresh**.

### 4.10.4.1 When Setting Up a File System Fails

If an attempt to create or mount a file system or set up the default quota fails, you must check and clear the error details, and perform the operation again.

To clear the error details:

1. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window appears. For details on this window, see section 4.10.3.

2. Use a radio button to select the file system for which the task for creating or mounting has terminated abnormally, and then click the **Error Details** button.

   The **Error Details** window appears.

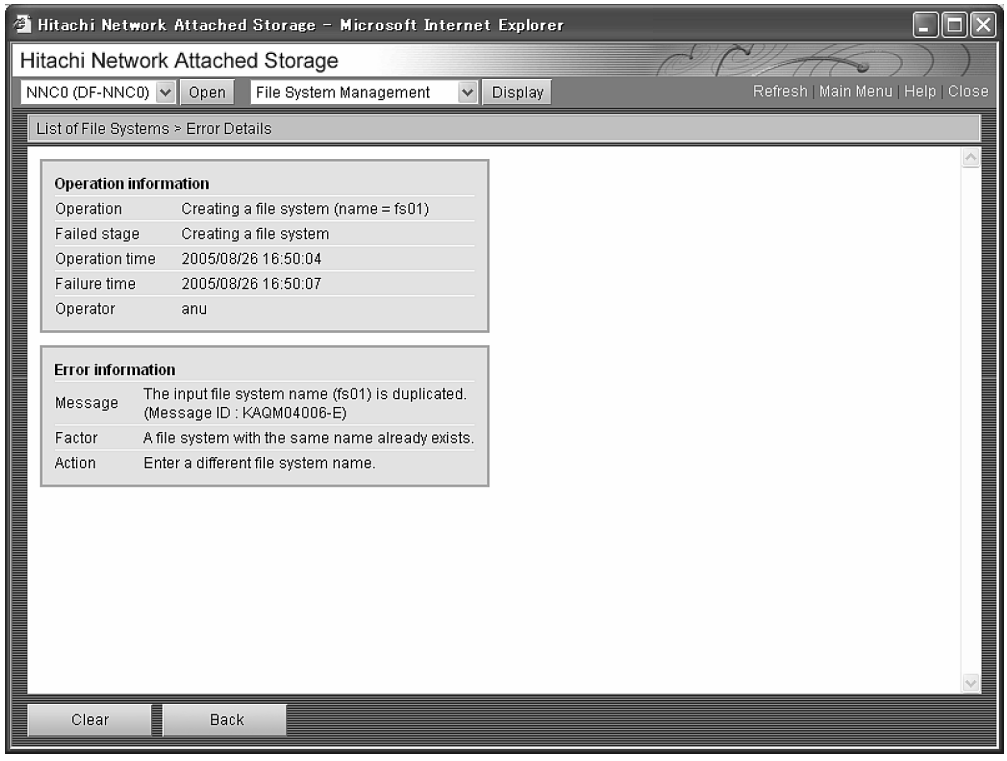



**Figure 4.83 Creating a File System Error Details Window**

3. Check the displayed information, such as an error message and information on the cause of the error, and the action to be taken. Then, click the **Clear** button.

   A dialog box appears asking you to confirm whether the error details can be cleared.

   The following table describes the information displayed in the **Error Details** window:

**Table 4.49 Creating File System Error Details Window (Displayed Information)**

| Item | Description |
|---|---|
| **Operation** | Displays information on the operation that terminated abnormally.<br>▪ When an attempt to create a file system failed:<br>*Creating a file system (name = file-system-name)*<br>▪ When an attempt to mount a file system failed:<br>*Mounting a file system (name = file-system-name)* |
| **Failed Stage** | Displays the operation in which an error has occurred.<br>This item is displayed when processing is performed to create a file system in the **Create New File System** window. It is not displayed when processing is performed to mount a file system in the **Edit Mount** window.<br>*Creating a file system*<br>This is displayed if an error occurred during creation of a file system.<br>*Mounting a file system*<br>This is displayed if an error occurred during mounting of a file system.<br>*Setting up the default quota*<br>This is displayed if an error occurred during setup of the default quota.<br>`Waiting for execution`<br>This is displayed if the resource group stopped, or failure or failover occurred on the NAS OS while the OS was waiting for execution.<br>`Starting execution`<br>This is displayed if failure occurred for the NAS OS immediately after processing started. |
| **Operation Time** | Displays the date and time the operation was performed. |
| **Failure Time** | Displays the date and time the operation failed. |
| **Operator** | Displays the user name of the system administrator who tried to run the operation. |
| **Message** | Displays the error message and message ID. |
| **Factor** | Displays the cause of the error. |
| **Action** | Displays corrective action. |

4. Click the **OK** button.

   Take action according to the error details that you checked.

5. After taking appropriate action, create or mount the file system or set up the default quota as necessary.

   For details on how to create a file system, see section 4.10.5. For details on how to mount a file system, see section 4.10.6. For details on how to set the default quota, see section 4.12.5.

### 4.10.5 Creating a File System

The maximum number of file systems that can be created for one cluster is 256. When a volume manager is used, the maximum number of file systems that can be created for one node is 128, and the maximum number of logical volumes that can be created for one node is 4,096. Thus, you cannot create a new file system when the number of logical volumes reaches 4,096.

If you use NAS Sync Image, you must use a volume manager to create any source file systems that are set for a differential-data storage device. If NAS Sync Image uses a created file system, select **Use** for **Volume manager** in the **Create New File System**s window.

In addition to creating file systems, you can mount file a file system and you can set up a default quota:

- **Mounting a file system**

  Because mount information is saved on the disk system, mount status is maintained during failover of the resource group that is providing the mounted file system services or restart of the services. The NAS Modular system allows full-time access to the file system by maintaining the mount status.

- **Setting up a default quota**

  If a default quota is set up for a file system, it is applied when a user for whom a quota has not been set uses the file system. The default quota prevents excessive usage of block space and i-nodes in a file system when a quota has not been explicitly set for each user.

Immediately after creating and mounting a file system and setting up a default quota, you can create an NFS or CIFS share. For details on NAS Sync Image, see the *NAS Sync Image User's Guide*.

#### 4.10.5.1 Creating a File System

Use the **Create New File System** window to create a file system, mount the file system and set the default quota. After creating a file system, you can also create an NFS or CIFS share.

To create a file system:

1. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window displays. For window details, see section 4.10.4.

2. Click the **Create** button.

   The **Create New File System** window displays (see . Information about the window’s contents is described in Table 4.50.

3. Enter the required information, and then click the **Create**, **Create and Set Up NFS Share**, or **Create and Set Up CIFS Share** button:

   – When creating only a file system:

     In **Mount Option**, select **Mount.**

To set the default quota, in **Mount option**, for **Quota** select **On**. Then, for **Default quota option**, select **Set default quota** and specify the soft and hard limits.

After setting the required information, click the **Create** button. The file system is created and mounted (and the default quota is set), and then the **List of File Systems** window re-displays.

– When creating a file share immediately after creating and mounting a file system (and setting the default quota):

In **Mount Option**, select **Mount.**

To set the default quota, in **Mount option**, for **Quota** select **On**. Then, for **Default quota option**, select **Set default quota** and specify the soft and hard limits.

After setting the required information, click the **Create and Set Up NFS Share** or **Create and Set Up CIFS Share** button:

– To create an NFS share, click the **Create and Set Up NFS Share** button.

– To create a CIFS share, click the **Create and Set Up CIFS Share** button.

The processing to create and mount the file system (and set the default quota) starts, and the **Create NFS File Share** window or **Create CIFS File Share** window is displayed. For each window, the file system created and mounted in the **Create New File System** window can be shared. For details on creating a file share, see section 4.11.2 and section 4.11.8.

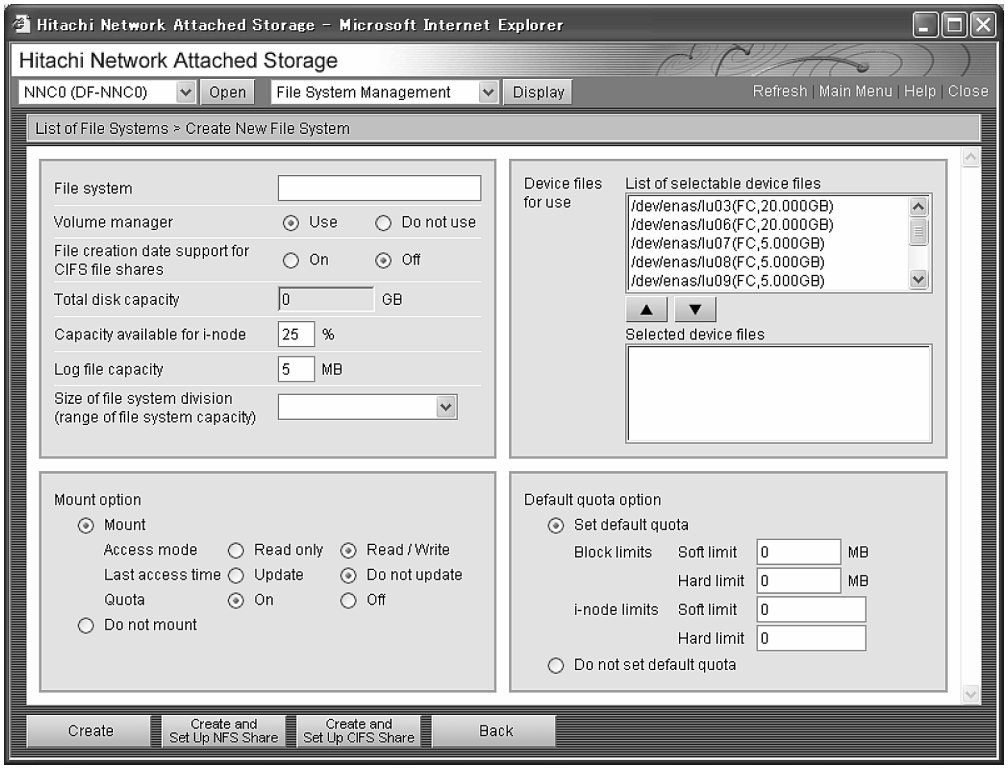



**Figure 4.84 Create New File System Window**

**Table 4.50 Create New File System Window (Information Specified)**

| Item | Description |
|---|---|
| **File system** | Name of the file system to be created.<br>Specify a unique name within the cluster.<br>You can use a maximum of 16 alphanumeric characters and underscores (_). |
| **Volume manager** | Use a radio button to select whether to use a volume manager:<br>If you want to create a file system using multiple device files, or expand the capacity of the file system, use a volume manager.<br>When you use a volume manager, you can expand the capacity once you create the file system.<br>**Use**<br>Use a volume manager.<br>**Do not use**<br>Do not use a volume manager. |
| **File creation date support for CIFS file shares** | Use a radio button to select whether to record the file creation time in the file system. If you want to create a CIFS share in the file system to be created, We recommend that you select **On**.<br>**On**<br>Select this radio button to enable recording of the file creation time.<br>**Off**<br>Select this radio button to disable recording of the file creation time.<br>Note that if an NFS share is created in the file system, NFS clients cannot view the file creation time even when **On** is selected. |
| **Capacity available for i-node** | Specify the maximum file system capacity that can be used as i-nodes (units: %).<br>Set a value in the range from 1 to 100.<br>The default is 25. |
| **Log file capacity** | Specify the size of the disk space for storing logs (units: MB).<br>Set a value in the range from 2 to 128. Specify a value smaller than **Size of file system division**.<br>The default is 5. For normal operation, the value does not need to be changed. Specify the default value.<br>When performing parallel processing to update one file system by using many processes (100 or more), the update processing performance can be enhanced by increasing this value (40 MB or more). |

| Item | Description |
|---|---|
| **Size of file system division (range of file system capacity)** | Select the file system division size from the drop-down list.<br>Of the following file system division sizes, only those that are specifiable are displayed in the drop-down list:<br>**16MB (128MB-256MB)**, **32MB (128MB-512MB)**, **64MB (128MB-1GB)**, **128MB (128MB-2GB)**, **256MB (256MB-4GB)**, **512MB (512MB-8GB)**, **1GB (1GB-16GB)**, **2GB (2GB-32GB)**, **4GB (4GB-2TB)**<br>Parentheses enclose the range of file system sizes that are appropriate for the file system division size that is written before the parentheses.<br>The file system division size appropriate to the capacity of the file system is displayed as the default.<br>The following are the specifiable sizes for the file system division, where *m* indicates the file system capacity, and <= means *is equal to or less than*. For details on the file system capacity, see section 4.10.3.<br>When 128 MB <= *m* < 256 MB:<br>You can specify 16 MB, 32 MB, 64 MB, or 128 MB. The size must be larger than the size specified in **Log file capacity**.<br>When 256 MB <= *m* < 512 MB:<br>You can specify 32 MB, 64 MB, 128 MB, or 256 MB. The size must be larger than the size specified in **Log file capacity**.<br>When 512 MB <= *m* < 1 GB:<br>You can specify 64 MB, 128 MB, 256 MB, or 512 MB. The size must be larger than the size specified in **Log file capacity**.<br>When 1 GB <= *m* < 2 GB:<br>You can specify 128 MB, 256 MB, 512 MB, or 1 GB. The size must be larger than the size specified in **Log file capacity**.<br>When 2 GB <= *m* < 4 GB:<br>You can specify 256 MB, 512 MB, 1 GB, or 2 GB.<br>When 4 GB <= *m* < 8 GB:<br>You can specify 512 MB, 1 GB, 2 GB, or 4 GB.<br>When 8 GB <= *m* < 16 GB:<br>You can specify 1 GB, 2 GB, or 4 GB.<br>When 16 GB <= *m* < 32 GB:<br>You can specify 2 GB or 4 GB.<br>When 32 GB <= *m* < 2 TB:<br>You can specify 4 GB. |
| **Device files for use** | Using the **List of selectable device files** list box, specify the device files to use in the file system. In this list box, the drive type and capacity are also displayed for each device file name. As the drive type, `FC` is displayed for an FC drive, and `SATA` is displayed for a SATA drive.<br>Up to 256 device files can be specified per file system. When **Use** is selected for **Volume manager**, specify a device file whose capacity is 65 MB or more.<br>Specify a file system capacity from 128 MB and up to (but not including) 2 TB. For details on the file system capacity, see section 4.10.3.<br>When you click the ▼ button, the device files selected in the **List of selectable device files** list box are added to the **Selected device files** list box. Only device files listed in the **Selected device files** list box are used in the file system.<br>The total capacity of the device files added to the **Selected device files** list box is displayed in **Total disk capacity**.<br>To delete a device file from the **Selected device files** list box, select the device file and click the ▲ button. |

| Item | Description |
| --- | --- |
| **Mount option** | Use a radio button to specify whether to mount the file system after creating it. Select **Mount** to mount the file system; otherwise, select **Do not Mount**. If you select **Mount**, you also need to select the following options:<br>**Access mode**<br>Use a radio button to select an access permission for the file system:<br>**Read only**<br>Read only permission.<br>**Read/Write**<br>Read/write permission.<br>**Last access time**<br>Use a radio button to specify whether to update the last access time at which the file system was accessed. The default is **Do not update**. If you unmount a file system once and then move to the **Edit Mount** window to remount it, **Last access time** returns to its default **Do not update**:<br>**Update**<br>Update the last access time according to the last i-node access time.<br>**Do not update**<br>Do not update the last access time.<br>**Quota**<br>Use a radio button to select whether to enable the quota functionality:<br>**On**<br>Enable the quota functionality.<br>**Off**<br>Disable the quota functionality. |

| Item | Description |
|---|---|
| **Default quota option** | Use the radio button to choose whether to set the default quota after creating a file system. If you want to set the default quota, choose **Set default quota**. If you do not want to set the default quota, choose **Do not set default quota**. If you choose **Set default quota**, specify the following items:<br>**Block limits**<br>Specify the block space available for each user.<br>This setting is applied when a user, for whom a quota for the file system has not been set, uses the file system created in this window for the first time (when the user creates a file).<br>**Soft limit**<br>Set the soft limit (units: MB).<br>Specify a value from 0 to 2,097,151. This value must not exceed the **Hard limit** setting.<br>The default is 0 (no soft limit).<br>**Hard limit**<br>Set the hard limit (units: MB).<br>Specify a value from 0 to 2,097,151.<br>The default is 0 (no hard limit).<br>**i-node limits**<br>Specify the number of i-nodes available for each user. This setting is applied when a user for which the quota has not been set uses the file system created in this window for the first time (when the user creates a file).<br>**Soft limit**<br>Set the soft limit.<br>Specify a value from 0 to 2,147,483,647. This value must not exceed the **Hard limit** setting.<br>The default is 0 (no soft limit).<br>**Hard limit**<br>Set the hard limit.<br>Specify a value from 0 to 2,147,483,647.<br>The default is 0 (no hard limit). |

### 4.10.5.2 Creating a File Share (After Creating a File System)

When creating a file system, you can move directly from the **Create New File System** window to a file share creation window (the **Create NFS Share** window or **Create CIFS File Share** window) if you want to create an NFS or CIFS share immediately after creating and mounting a file system and setting up the default quota.

When creating a share immediately after creating a file system in the NAS Modular system, while you are entering file share information in the **Create NFS File Share** window or **Create CIFS File Share** window, the processing to create and mount a file system and set the default quota runs concurrently in the background. This can reduce the time it takes you to create a file share.

The following figure shows the processing flow for creating a file share immediately after creating a file system:

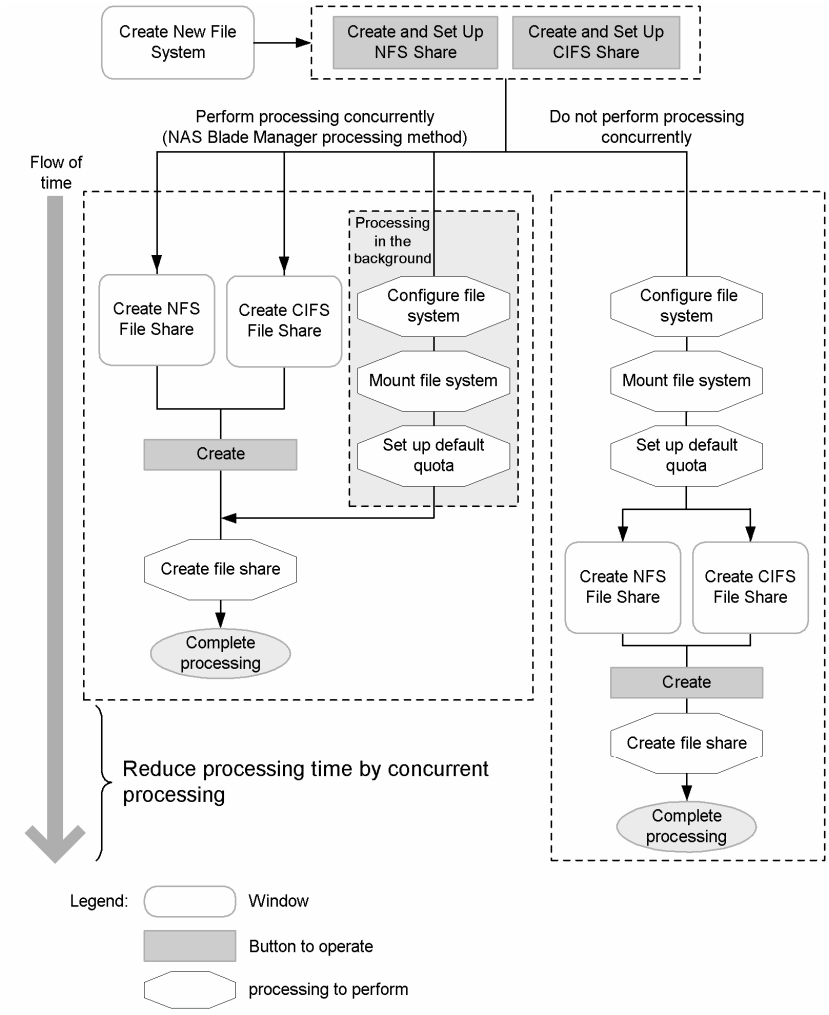



**Figure 4.85 Creating a File Share after Creating a File System**

If you perform the operations explained in this section in the **Create NFS File Share** window, **Create CIFS File Share** window, **Write Allowed Users / Groups** Setup window, or **Write Disallowed Users / Groups** Setup window, the status of processing (which is running concurrently in the background to create and mount a file system and to set the default quota) is checked. If the processing in the background finishes successfully, the next processing is performed.

Following are the operations, for each window, to check the status of background processing:

- In the **Create NFS File Share** window, click the **Create** or **Back** button.
- In the **Create CIFS File Share** window, click **Main Menu** or **Display**.
- In either the **Write Allowed Users / Groups** window or the **Write Disallowed Users / Groups** window, click **Main Menu** or **Display.**

The window transitions and actions to be taken when an error occurs in the processing to create and mount the file system and set the default quota that is running concurrently in the background are shown below:

- When an error occurs while creating the file system:

  After an error window appears, the **Create New File System** window also appears. Based on the message displayed in the error window, take the appropriate action, and try to create the file system again. For details on creating a file system, see section 4.10.5.

- When an error occurs while mounting the file system mount or setting the default quota:

  After an error window appears, the **List of File Systems** window also appears. Based on the message displayed in the error window, take the appropriate action, and then see the **List of File Systems** window to check whether the file system has been mounted. In addition, in the **List of File Systems** window, select the relevant file system, and then click the **Quota Setup** button to display the **List of Quota Information** window where you can determine whether the default quota has been set. Then, if required, mount the file system and set the default quota.

  For details on mounting a file system, see section 4.10.6. For details on setting the default quota, see section 4.12.4.

If you click **Close** to close the **Create NFS File Share** window, **Create CIFS File Share** window, **Write Allowed Users / Groups** window, or **Write Disallowed Users / Groups** window, a message is displayed indicating that background processing log data is output to the `management.log` file. If there is a possibility that an error has occurred in background processing, check the `management.log` file.

For details on viewing the `management.log`, see section 4.13.7.

### 4.10.6 Mounting a File System

You can use the **Edit Mount** window to mount a file system. The maximum number of file systems that can be mounted for one cluster is 256.

Differential-data snapshots that have been created using NAS Sync Image cannot be mounted. If you want to mount differential-data snapshots, see the manual *NAS Sync Image Modular User's Guide*.

File systems are mounted at the following mount point directory:

| /mnt/*file-system-name* |
|---|

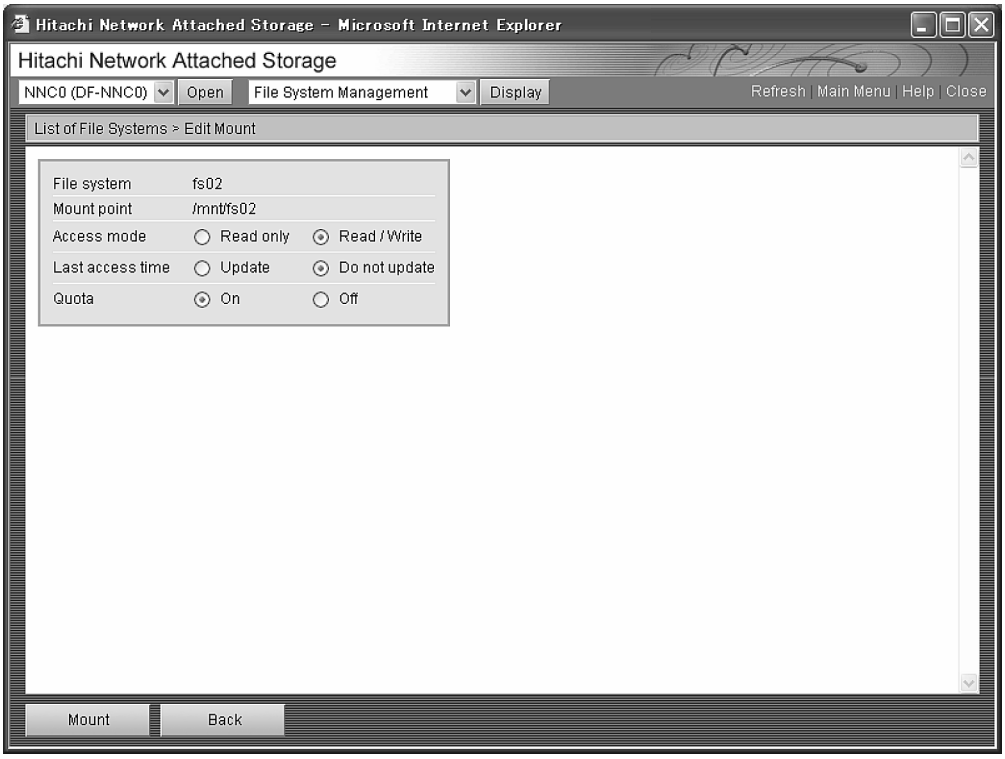



**Figure 4.86 Edit Mount Window**

The following snapshots cannot be mounted:

- Snapshots taken by NAS Backup Restore
- Differential-data snapshots created by using NAS Sync Image

The file system for which the copy device is defined cannot be mounted while NAS Backup Restore recovers the file system from the snapshot.

To mount the file systems or snapshots described above, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide* or *Hitachi AMS/WMS NAS Sync Image User's Guide*.

In a NAS Modular system, mount status is maintained even in the event of failover of the resource group providing the mounted file system services or restart of the services, because the mount information is saved on the disk array.

The NAS Modular system allows full-time access to the file system by maintaining the mount status.

**Before Mounting a File System**

When you change **Quota** in the **Edit Mount** window to **On** for a file system whose quota setting was **Off** the last time it was mounted, the file system takes a long time to finish re-mounting.

The larger the used capacity of the file system is, the longer it takes to mount the file system. We recommend that the Quota setting in the **Edit Mount** window should be **On** when a file system is first mounted.

To mount a file system:

1. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window appears again, and `Mounting` is displayed in **Operating status** in the window. For window details, see section 4.10.4.

2. Use a radio button to select the file system you want to mount, and then click the **Edit Mount** button.

   The **Edit Mount** window displays.

3. Enter the required information as described in Table 4.51, and then click the **Mount** button.

   The **List of File Systems** window appears again, and `Mounting` is displayed in **Operating status** in the window.

   The system administrator must click **Refresh** in the **List of File Systems** window to view the latest information displayed in **Operating status**. If nothing is displayed in **Operating status**, the task has terminated normally. If `Error` is displayed in **Operating status**, the task has terminated abnormally.

   The following table lists and describes the information to be specified in the **Edit Mount** window when mounting a file system.

**Table 4.51 Edit Mount Window at File System Mounting**

| Item | Description |
|---|---|
| **Access mode** | Use a radio button to select an access permission for the file system:<br>**Read only**<br>Read only permission.<br>**Read/Write**<br>Read/write permission. |
| **Last access time** | Use a radio button to specify whether to update the last access time at which the file system was accessed. The default is **Do not update**. When you unmount a file system once and then move to the **Edit Mount** window to remount it, **Last access time** returns to its default **Do not update**:<br>**Update**<br>Update the last access time according to the last i-node access time.<br>**Do not update**<br>Do not update the last access time. |
| **Quota** | Use a radio button to select whether to enable the quota functionality:<br>**On**<br>Enable the quota functionality.<br>**Off**<br>Disable the quota functionality. |

### 4.10.7 Unmounting a File System

Differential-data snapshots that have been created using NAS Sync Image cannot be unmounted. If you want to unmount differential-data snapshots, see the manual *Hitachi AMS/WMS NAS Sync Image User's Guide*.

**Before Unmounting a File System**

Before unmounting a file system, you must delete all NFS and CIFS shares. An error occurs if you attempt to unmount a file system without deleting NFS and CIFS shares. For details on deleting NFS and CIFS shares, see section 4.11.5 or section 4.11.12.

If a file system is unmounted, the service for that unmounted file system stops.

If the NAS Backup Restore license has been set up, make sure that neither backup nor restore is being performed. If you unmount a file system while a backup or restore is being performed, the backup or restore will fail, and an error will occur. Before unmounting a file system, view the connection between the NDMP server and the backup server, or between the NDMP server and the media server, to make sure that neither backup nor restore is being performed.

For details on how to check the connection between the NDMP server and the backup server, or between the NDMP server and the media server, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

To unmount a file system:

1. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window displays. For window details, see section 4.10.4.

2. Select a file system to unmount, and then click the **Edit Mount** button.

   The **Edit Mount** window displays.

3. Click the **Unmount** button.

   The file system is unmounted and the **List of File Systems** window re-displays.

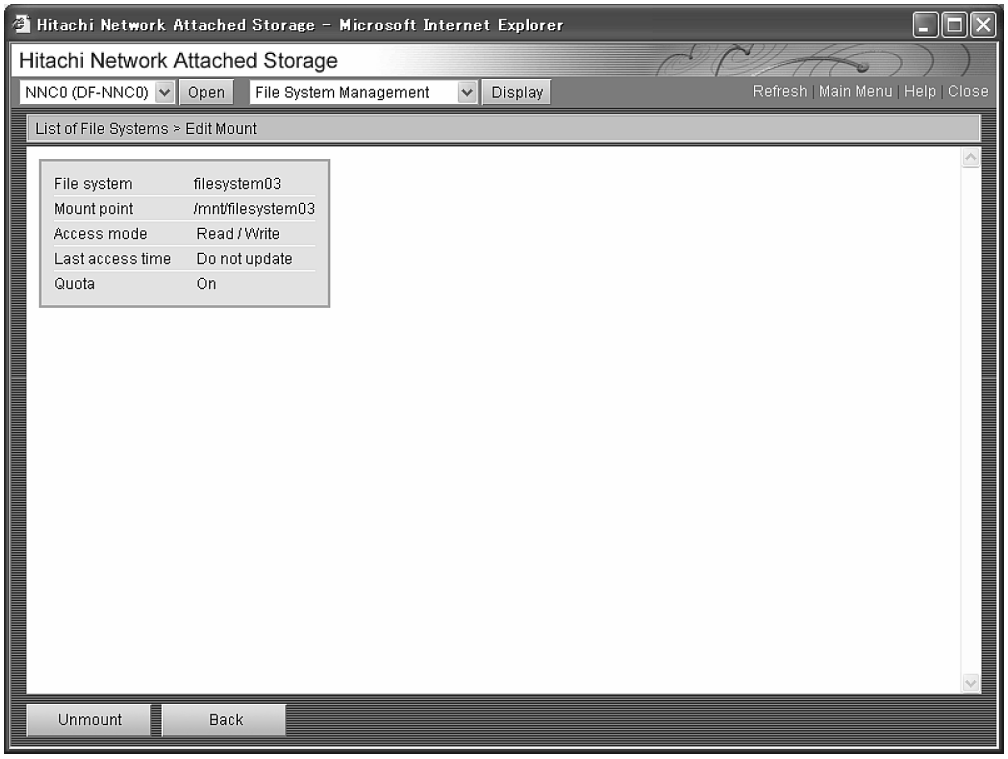



**Figure 4.87 Edit Mount Window (at unmounting)**

### 4.10.8 Expanding File System Capacity

The capacity of a file system can be expanded if you used a volume manager to create the file system. You can use the **Expand File System** window to expand the file system capacity by adding device files. A file system can be expanded as long as the file system capacity is less than 2 TB. However, the expandable size might be smaller depending on the file system division size when the file system was created.

The capacity of the file system for which differential-data snapshots and a differential-data storage device have been set (by using NAS Sync Image) cannot be expanded. For details on how to expand the file system, see the manual *NAS Sync Image Modular User's Guide*.

When the remote copy function of NAS Backup Restore is applied to the file system whose capacity you want to expand, reconfigure the remote copy pair after you expand the capacity. For details on using the remote copy functionality, see the manuals for ShadowImage.

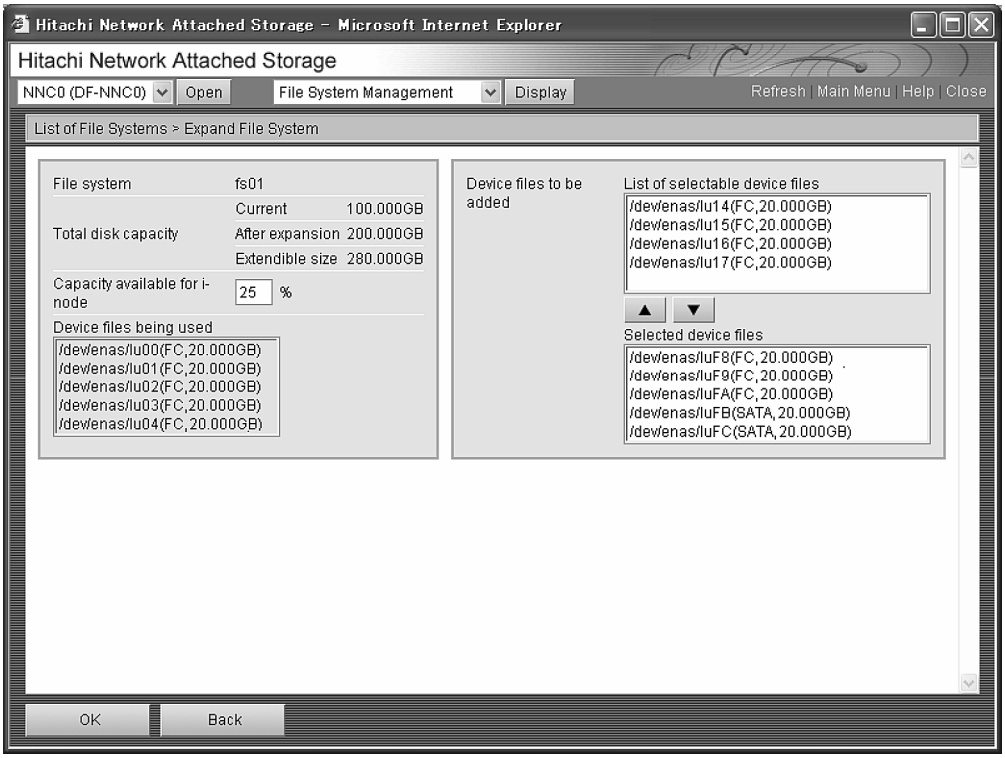



**Figure 4.88 Expand File System Window**

To expand the capacity of a file system:

1. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window displays. For window details, see section 4.10.4.

2. Use a radio button to select the file system you want to expand and click the **Expand** button.

   The **Expand File System** window displays. Following is information about the window's contents:

   - **Capacity available for i-node** Specify the maximum capacity available for i-nodes after file system expansion (units: %). When the window is opened, the maximum capacity that is set for the current file system is displayed as the initial value.
   - **Device files to be added** Using the **List of selectable device files** list box, select one or more device files to add to the file system. In this list box, the drive type and capacity are also displayed for each device file name. As the drive type, `FC` is displayed for an FC drive, and `SATA` is displayed for a SATA drive. The size of each device file must be 160 MB or greater. Up to 256 device files can be specified per file system.

     When you click the ▼ tif button, the device files selected in the **List of selectable device files** list box are added to the **Selected device files** list box. Only device files listed in the **Selected device files** list box will be added in the file system.

     The sum of the total capacity of the file systems added to the **Selected device files** list box, and the capacity of the device files already specified, is displayed in **After Expansion**, in **Total disk capacity**. Also, the capacity of the device files already specified is displayed in **Current**, in **Total disk capacity**.

     To delete a device file from the **Selected device files** list box, select the device file, then click the ▲ button.

3. Enter the required information, and then click the **OK** button.

   The file system is expanded and the **List of File Systems** window re-displays.

### 4.10.9 Deleting a File System

You can use the **List of File Systems** window to delete a file system. Deleting a file system frees the configured device files and makes them available for other purposes.

The file systems for which differential-data snapshots and a differential-data storage device have been set (by using NAS Sync Image) cannot be deleted. For details on how to delete the file systems and differential-data snapshots, see the manual *NAS Sync Image Modular User's Guide*.

#### Before Deleting a File System

Before deleting a file system, you must complete the following tasks; attempting to delete a file system without completing these tasks results in an error:

- Unmount the file system.
- Delete the copy-destination file system (delete the pair with ShadowImage).

- Remove the differential-data storage device settings.

- For details on unmounting a file system, see section 4.10.7.
- For details on deleting copy device definitions, see the *Hitachi AMS/WMS NAS Sync Image User's Guide*
- For details on deleting copy-destination file systems, see the *ShadowImage in-System Replication Software User's Guide*.
- For details on removing differential-data storage device settings, see the *Hitachi AMS/WMS NAS Sync Image User's Guide*.

**To delete a file system:**

1. Check the status of the nodes that make up the cluster and the status of the resource group:
   - Status of the nodes that make up the cluster

     In the **Browse Cluster Status** (Cluster / Node Status) window, make sure that the **Node status** is `UP`. If the **Node status** is other than `UP`, start the node.

     For details on how to start a node, see section 4.5.5.
   - Status of the resource group

     In the **Browse Cluster Status** (Resource Group Status) window, make sure that the **Resource group status** is either `Online / No error` or `Offline`.

   For details on how to check the status of the resource group, see section 4.5.7.
2. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window displays. For window details, see section 4.10.4.
3. Use a radio button to select the file system you want to delete, and then click the **Delete** button.

   A dialog box confirms that you want to delete the file system.
4. Click the **OK** button.

   The selected file system is deleted.

   ***Note:*** When the status of the resource group is `Offline` and you delete the shared file system, an NFS share is deleted, however, a CIFS share is not deleted. Change the status of the resource group to `Online`, then delete the CIFS share in the **List of File Shares** (List of CIFS File Shares) window. For details on how to delete CIFS shares, see section 4.11.12.

## 4.11 Managing File Shares

To enable access over a network to the data stored in a disk array, sharing of the file system and files based on the NFS or CIFS protocol must be set up. File shares allow the NAS Modular system to be used as network attached storage (NAS) so that users on heterogeneous operating systems such as UNIX® and Windows® can access file systems over their networks.

This section describes how you can **Create NFS Share**s and CIFS shares, and how to modify file share attributes.

### 4.11.1 Viewing NFS Share Information

You can use the **List of File Shares** (List of NFS File Shares) window to view information about NFS shares.

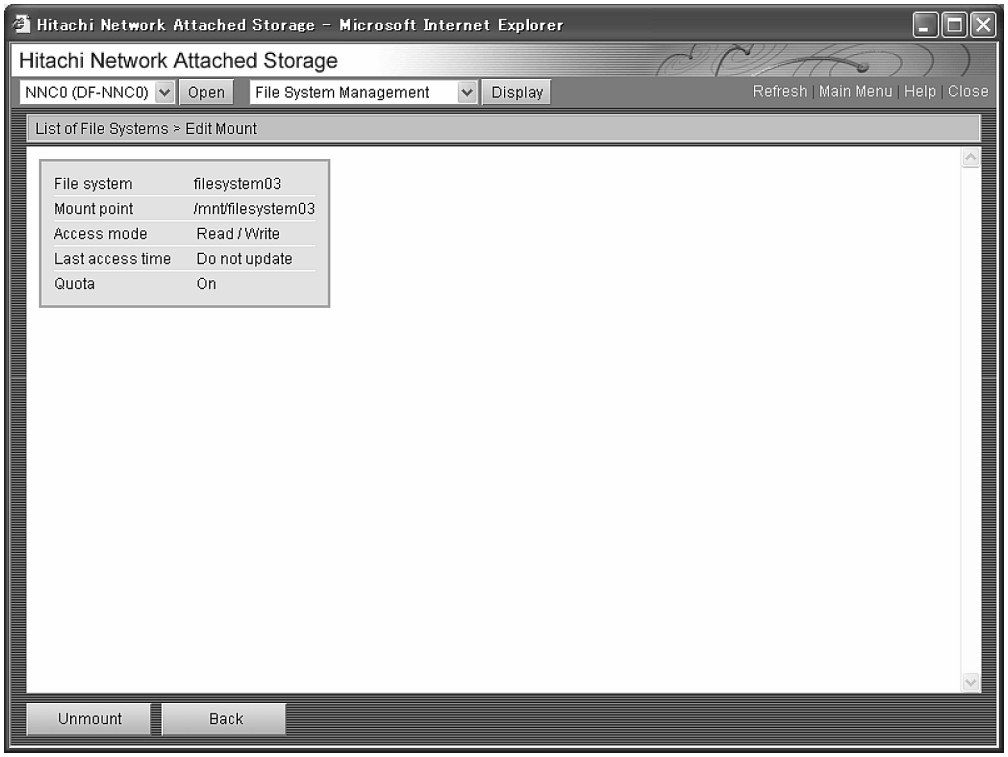



**Figure 4.89 List of File Shares Window**

The following table describes the information that is displayed in the **List of File Shares** (List of NFS File Shares) window:

**Table 4.52 List of File Shares Window**

| Item | Description |
|---|---|
| **Last update** | The date and time the information displayed in the window was last updated. |
| **Shared directory** | Absolute path of the NFS shared directory name. |
| **Public destination host/network** | Name of a host or network accessing the NFS share. |
| **Operating status** | The status of the creation of the NFS file share.<br>`Creating`<br>Creation of the NFS file share is waiting for execution or being executed.<br>`Error` |

| Item | Description |
|---|---|
| | The attempt to create the NFS file share terminated abnormally after it was queued. Take action.<br>If creation of the NFS file share has terminated normally, nothing is displayed. |
| **Permission mode** | Access permission for the NFS share:<br>`ro`<br>Read only permission.<br>`rw`<br>Read/write permission. |
| **Synchronous writing** | Synchronous write mode when write operations to the NFS share are permitted:<br>`sync`<br>Synchronous write without optimization.<br>`sync (optimized)`<br>Synchronous write with optimization. |
| **Anonymous mapping** | Users mapped as anonymous users:<br>`everyone`<br>All users are mapped as anonymous users.<br>`root only`<br>Only the root user is mapped as an anonymous user.<br>`none`<br>No users are mapped as anonymous users. |

To view information about NFS shares, click the **File Share Management** button from the **Main Menu** window.

The **List of File Shares** (List of NFS File Shares) window appears. If the **List of File Shares** (List of CIFS File Shares) window is active, select **List of NFS file shares** from the drop-down list, then click the **Display** button.

To check the latest status, click **Refresh**.

### 4.11.2 Creating an NFS Share

You can use the **Create NFS File Share** window to create an NFS share. Ensure that there are no more than 256 NFS shares per cluster.

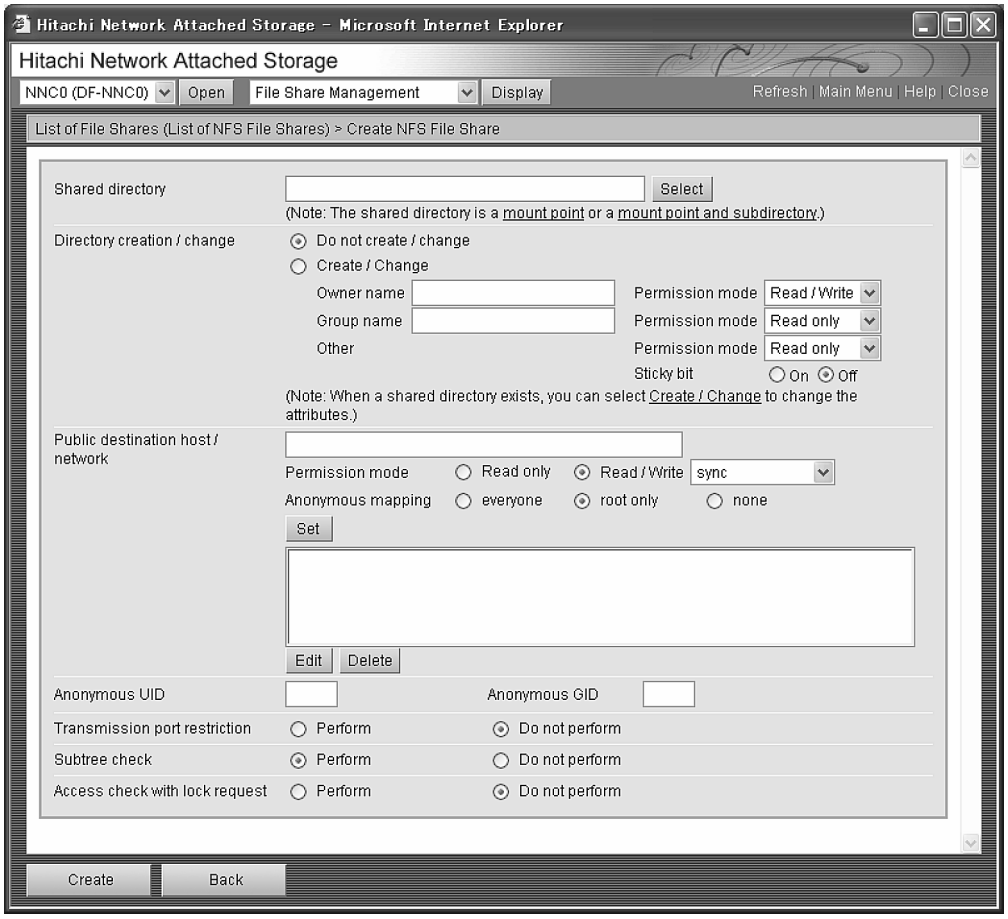



**Figure 4.90 Create NFS File Share Window**

If an error occurs during NFS share creation, the previous status is restored. The entered settings do not change if a resource group failover or restart occurs once the share is created.

When an automatic creation schedule is set up in NAS Sync Image for a file system for which an NFS share was created, if a file share is automatically created for a snapshot, that NFS share is created for the snapshot using the NFS share information created in this window.

To create an NFS share:

***Note:*** Clicking the **Create and Set Up NFS Share** button in the **Create New File System** window displays the **Create NFS File Share** window. In this case, skip steps 1 and 2 in the following procedure.

1. In the **Main Menu** window, click the **File Share Management** button.

   The **List of File Shares** (List of NFS File Shares) window displays. For window details, see section 4.11.1. If the **List of File Shares** (List of CIFS File Shares) window is active, select **List of NFS file shares** from the drop-down list, and then click the **Display** button.

2. Click the **Create a File Share** button.

   The **Create NFS File Share** window displays. Information about the window's contents is described in Table 4.53.

3. Enter the required information, and then click the **Create** button.

   The system administrator must click **Refresh** in the **List of File Shares** (List of NFS File Shares) window to check the latest information displayed in **Operating status**. It nothing is displayed in **Operating status**, the task has terminated normally. If `Error` is displayed in **Operating status**, the task terminated abnormally after it was queued.

   After an NFS share has been created, the **List of File Shares** (List of NFS File Shares) window displays.

**Table 4.53 Create NFS File Share Window**

| Item | Description |
|---|---|
| **Shared directory** | Specify the shared directory to be accessed as an NFS share. Clicking the **Select** button displays the **List of Mounted File Systems** window. In the List of Mounted Files Systems window, select a file system to be shared as an NFS share, or enter its name directly in the text box. For details on selecting a file system in the **List of Mounted File Systems** window for creating an NFS share, see section 4.11.3.<br>If you display this window by clicking the **Create and Set Up NFS Share** button in the **Create New File System** window, the file system mount point specified for **File system** in the **Create New File System** window is displayed. Create an NFS share under the displayed mount point. The **Select** button is not displayed.<br>Specify a unique name for an NFS directory within the cluster. Make sure that you use an absolute path to specify the directory.<br>Enter from 6 to 63 characters. If the NAS Sync Image automatic creation schedule (automatic creation of shares) was used, the NFS share directory can be a maximum of 48 characters.<br>You can use any alphanumeric character, hyphen (-), period (.), forward slash (/), and underscore (_). **Shared directory** is case-sensitive.<br>▪ When sharing a directory of the file system:<br>`/mnt/`*`name-of-mounted-file-system`*`/`*`path-name`*<br>***Example***: `/mnt/filesystem01/share1`<br>▪ When sharing the whole file system:<br>`/mnt/`*`name-of-mounted-file-system`*<br>***Example***: `/mnt/filesystem02` |

| Item | Description |
|---|---|
| **Directory creation / change** | Use a radio button to select whether to create a new directory if the directory specified in **Shared directory** does not exist. If the directory has been created and is not specified in **Shared directory** for a CIFS share, you can change properties for the specified directory.<br>The created directory will not be automatically deleted even if you delete the NFS share.<br>If the directory specified in **Shared directory** has already been created, and you want to inherit its attributes, select **Do not create / change**. To create a new directory, or to change the attributes of a directory already created, select **Create / Change**.<br>If you select **Create / Change**, select or enter the following items:<br>**Owner**<br>Specify the user name or user ID of the owner.<br>When specifying a user registered by the user mapping functionality, specify the user as follows:<br>*domain-name**user-name*<br>**Group**<br>Specify the group name or group ID of the owner group.<br>When specifying a group registered by the user mapping functionality, specify the group as follows:<br>*domain-name**group-name*<br>**Permission mode** From the drop-down list, select the access permission for the directory owner, owner's group, and others.<br>▪ **Read/Write** Select this mode to grant both read and write permissions. The directory execution permission is granted.<br>▪ **Read only** Select this mode to grant read permission only. The directory execution permission is granted.<br>▪ **None** Select this mode when neither the read and write permissions nor the directory execution permission is granted. This mode is available for **Group** and **Other**.<br>▪ **Sticky bit** Permit only owner of files or subdirectories under the directory to delete or rename them. Use a radio button to select whether to set a sticky bit for the directory. |
| **Public destination host / network** | In the text box, enter the name of a host or network accessing the NFS share. You may enter up to 255 characters. You cannot specify a hyphen (-) at the beginning of the character string. Although multiple names can be specified, hosts must not have duplicate names.<br>Besides host names and IP addresses, the following formats are also available for specifying the name of a public destination:<br>▪ Netgroup<br>Enter an NIS netgroup. For example, you can write `@group` to specify only the host of the netgroup members.<br>▪ IP network<br>To permit all hosts in a sub-network to access the shared directory, specify the IP address and netmask in the format *address*/*netmask*. You can specify the netmask in decimal numbers separated by periods, and can also specify a continued mask length.<br>For example, the setting `10.208.148.0/255.255.255.0` indicates that all hosts connected to `10.208.148` are permitted to access the directory.<br>To specify a netmask with a continued mask length, enter as follows: `10.208.148.0/24`.<br>▪ Wildcard<br>When specifying all hosts, an asterisk (*) can be used as a wildcard. |

| Item | Description |
|---|---|
| **Public destination host / network**<br>(continued) | If some or all of the NFS client machines have multiple network interfaces that are used to communicate with the NAS Modular system, specify all the host names corresponding to all the IP addresses (for those interfaces) for the NFS clients. If you specify a wildcard (*), IP network, or netgroup, NFS clients might not be able to access the NFS share.<br>In **Permission mode** and **Anonymous mapping**, select options for the public destination that is set in the text box and has permission to access the NFS share.<br>**Permission mode**<br>Use a radio button to select the appropriate access permission for the NFS share.<br>Select **Read only** to prohibit data writes, or select **Read/Write** to permit data writes.<br>For the **Read/Write** option, select a synchronous write mode from the drop-down list.<br>*Synchronous write mode optimization* (**sync (optimized)**) is a function that slightly delays the writing of write requests to disk when a related write request is currently executing or is expected from the NFS client. This optimization can enhance performance because multiple write requests are written to disk in a single operation.<br>If the data write requests received by the NFS server will generally be unrelated, optimization will reduce performance. In this case, select **sync**.<br>**sync**<br>Write synchronously without optimization.<br>**sync (optimized)**<br>Write synchronously with optimization.<br>**Anonymous mapping**<br>*Anonymous mapping* is a function that maps a client accessing an NFS share to an arbitrary user ID or group ID instead of using the client's own user ID or group ID.<br>Use a radio button to select the users who access the NAS Modular system from the NFS client host, and are to be mapped as anonymous users.<br>**everyone**<br>Select this when you map all users as anonymous users.<br>**root only**<br>Select this when you map only the root user as an anonymous user.<br>**none**<br>Select this when you do not want to map users as anonymous users. |
| | In **Permission mode** and **Anonymous mapping**, specify options for the public destination that is set in the text box and has permission to access the NFS share, then click the **Set** button to add the specified hosts or networks to the list box. Only the host and network names appearing in the list box will be set as hosts or networks accessing the NFS share.<br>The total length of the selected host names or network names (the length of each name + 4 bytes) must be less than 1,005 bytes. When the specified IP addresses can be resolved by using methods such as the hosts file or DNS, the total of the lengths calculated by using the host names that match the IP addresses (the length of each host name + 4 bytes) must also be less than 1,005 bytes.<br>To edit a host name or network name set in the list box, select the desired host name or network name and then click the **Edit** button.<br>The settings for the selected item appear in the text box, **Permission mode** setting, and **Anonymous mapping** setting. After editing an item, click the **Set** button to update the changed settings back to the list box.<br>To delete a name from the list box, select the host or network name and click the **Delete** button. |
| **Anonymous UID** | Specify the user ID to be used when accessing the NFS share as an anonymous user. Specify a value from 0 to 65,535.<br>If you do not enter any value, the anonymous UID is set to `65534`. |

| Item | Description |
|---|---|
| **Anonymous GID** | Specify the group ID to be used when accessing the NFS share as an anonymous user. Specify a value from 0 to 65,535.<br>If you do not enter any value, the anonymous GID is set to `65534`. |
| **Transmission port restriction** | Use a radio button to select whether to accept only the requests from internet port lower than 1,024.<br>Select **Do not perform** if machines that use internet port 1,024 or higher are to access the file system.<br>**Perform**<br>Restrict ports requesting access to the file system.<br>**Do not perform**<br>Do not restrict ports requesting access to the file system.<br>***Note:***<br>In AIX, internet port 1,024 or higher is used by default.<br>Select **Do not perform** when AIX is used as an NFS client host and you want to use the default internet port setting.<br>In HP-UX, internet port 1,024 or higher is used for locking a file.<br>Select **Do not perform** to use HP-UX as an NFS client host. |
| **Subtree check** | Use a radio button to select whether to check that not only do the file and directory to be accessed have access permission (`x` permission), but also, all directories (subtrees) from the shared directory to the directory in which the file and directories to be accessed exist have execute permission (`x` permission). This is a security measure when only subdirectories of the file system are shared, not the entire file system.<br>If performance is a priority, select **Do not perform**.<br>If you use, as an NFS client, a machine that does not send authentication information for a lock request (the machine OS is HP-UX or a machine on which the `rpcinfo -p` command displays `100020` in `program`), or a machine that sends authentication information of a user other than the user who makes a lock request (the machine OS is AIX), select **Do not perform**. If you select **Perform**, a lock might not be able to be obtained (a lock request might result in the ENOLCK error) when execution permissions (`x`) for directories from the parent directory of a lock target file to the NFS mounted directory are not granted for an anonymous user in the NAS Modular system.<br>▪ **Perform** Perform a subtree check.<br>▪ **Do not perform** Do not perform a subtree check. |

| Item | Description |
|---|---|
| **Access check with lock request** | Use a radio button to select whether to check permissions for a lock request.<br>If you use, as an NFS client, a machine that does not send authentication information for a lock request (the machine OS is HP-UX or a machine on which the `rpcinfo -p` command displays `100020` in `program`), or a machine that sends authentication information of a user other than the user who makes a lock request (the machine OS is AIX), select **Do not perform**.<br>If you select **Perform**, a lock might not be able to be obtained (a lock request might result in the ENOLCK error) when read permissions (r) for directories from the parent directory of a lock target file to the NFS mounted directory are not granted for an anonymous user in the NAS Modular system.<br>**Perform**<br>Check permissions for a lock request.<br>If anonymous mapping is not set for the user, permissions for the user who locked the files are checked. If anonymous mapping is set for the user, permissions for the anonymous user in the NAS Modular system are checked. The owner of the locked files can lock them without permissions. Also, if the user has read permissions, they can write lock the files.<br>**Do not perform**<br>Do not check permissions for a lock request.<br>Permissions for an anonymous user in the NAS Modular system are checked. |

### 4.11.3 Selecting a File System for Creating an NFS Share

In the **List of Mounted File Systems** window, the system administrator can select a file system to share as an NFS share. The **List of Mounted File Systems** window lists the following file systems and differential-data snapshots:

- File systems and differential-data snapshots that have already been mounted.
- File systems and differential-data snapshots for which the mount operation is waiting to be executed or is being executed.

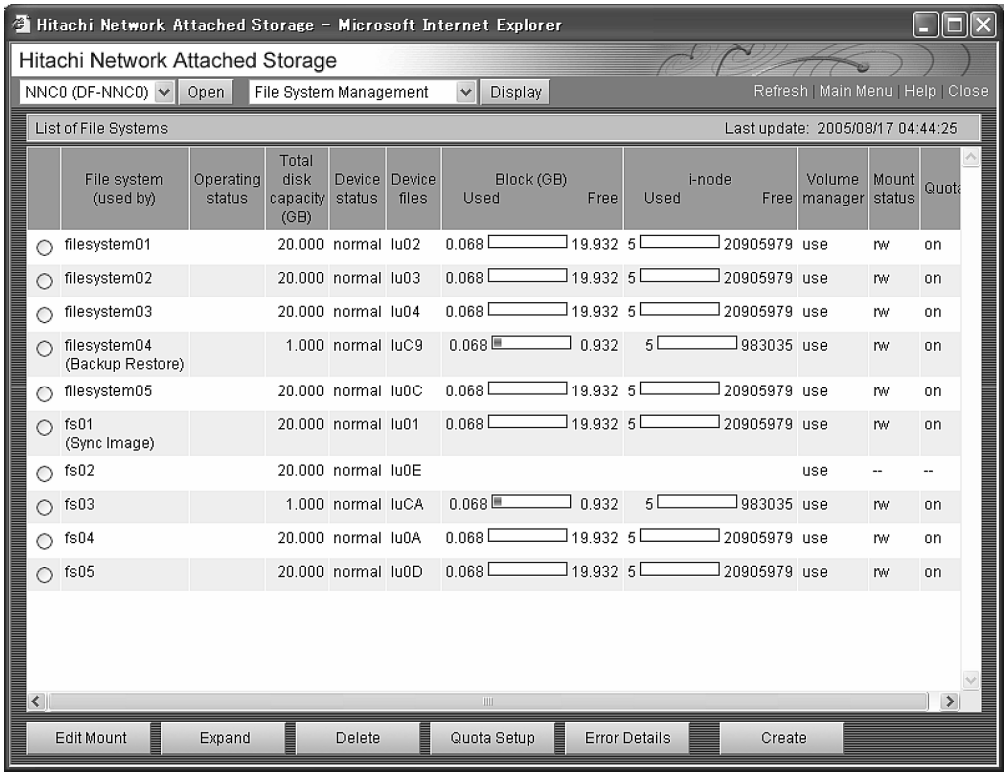



**Figure 4.91 List of Mounted File Systems Window**

To select a file system to share as an NFS share:

1. In the **Main Menu** window, click the **File Share Management** button.

   The **List of File Shares** (List of NFS File Shares) window displays. For window details, see section 4.11.1. If the **List of File Shares** (List of CIFS File Shares) window is active, select **List of NFS file shares** from the drop-down list, and then click the **Display** button.

2. Click the **Create a File Share** button.

   The **Create NFS File Share** window displays. For window details, see section 4.11.2.

3. To select, from a list of mount points, a mount point for a shared directory (mount point or subdirectories) to be accessed as an NFS share, click the **Select** button for **Shared directory**.

   The **List of Mounted File Systems** window displays.

4. From the **List of Mounted File Systems**, use a radio button to select the file system for which you want to create an NFS share, and then click the **OK** button.

   The **Create NFS File Share** window re-displays. In **Shared directory** of the **Create NFS File Share** window, the mount point of the selected file system is displayed. To allow access to directories under the file system, enter the directories following the displayed mount point.

### 4.11.4 Editing Information About an NFS Share

You can use the **Edit NFS File Share** window to edit information about an NFS share.

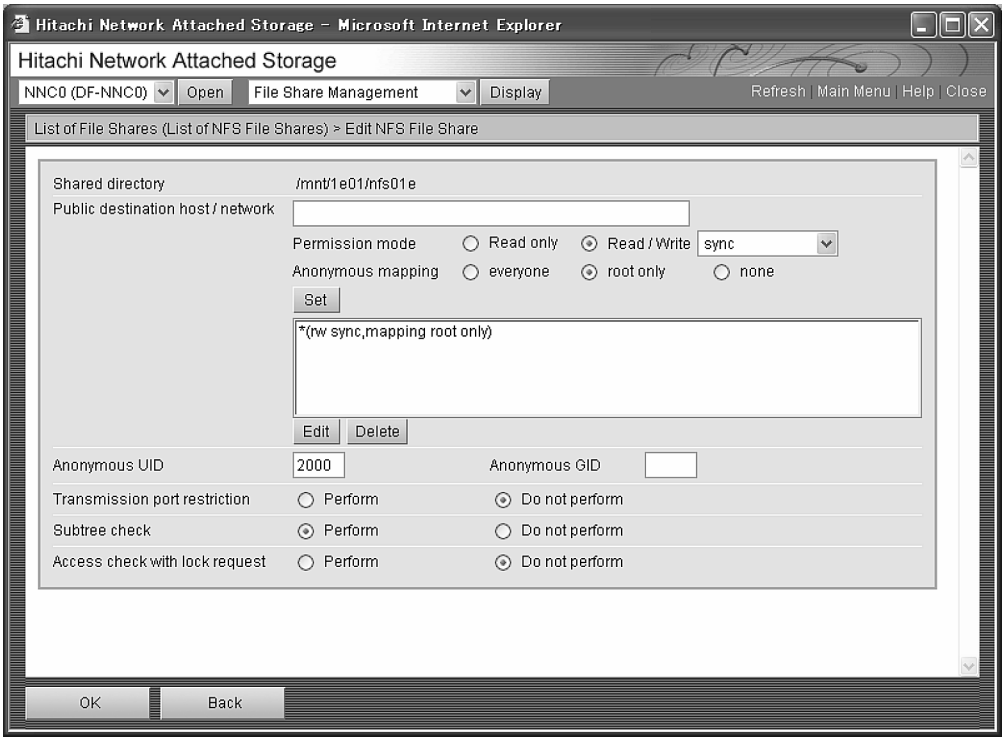



**Figure 4.92 Edit NFS File Share Window**

For unchanged items, the current settings will still apply after editing. If a failover or restart occurs during editing, the status is restored to the previous settings. When an automatic creation schedule is set up in NAS Sync Image for a file system for which an NFS share was created, if a file share is automatically created for a snapshot, that NFS share is created for the snapshot using the NFS share information edited in this window.

To edit information about an NFS share:

1. In the **Main Menu** window, click the **File Share Management** button.

   The **List of File Shares** (List of NFS File Shares) window displays. For window details, see section 4.11.1. If the **List of File Shares** (List of CIFS File Shares) window is active, select **List of NFS file shares** from the drop-down list, and then click the **Display** button.

2. Use a radio button to select the NFS share you want to edit, then click the **Edit** button.

   The **Edit NFS File Share** window displays. Information about the window's contents is described in Table 4.54.

3. Enter the required information, and then click the **OK** button.

   The NFS share settings are updated, and the **List of File Shares** (List of NFS File Shares) window re-displays.

**Table 4.54 Edit NFS File Share Window**

| Item | Description |
|---|---|
| **Public destination host / network** | In the text box, enter the name of a host or network accessing the NFS share. You may enter up to 255 characters. Although multiple names can be specified, hosts must not have duplicate names. Besides host names and IP addresses, the following formats are also available for specifying the name of a public destination:<br>▪ Netgroup<br>Enter an NIS netgroup.<br>For example, you can write `@group` to specify only the host of netgroup members.<br>▪ IP network<br>To permit all hosts in a sub-network to access the shared directory, specify the IP address and netmask in the format *address*/*netmask*. You can specify the netmask in decimal numbers separated by periods, and can also specify a continued mask length.<br>For example, the setting `10.208.148.0/255.255.255.0` indicates that all hosts connected to `10.208.148.0/24` are permitted to access the directory.<br>To specify a netmask with a continued mask length, enter as follows: `10.208.148.10/24`.<br>▪ Wildcard<br>When specifying all hosts, an asterisk (`*`) can be used as a wildcard.<br>If some or all of the NFS client machines have multiple network interfaces that are used to communicate with the NAS Modular system, specify all the host names corresponding to all the IP addresses (for those interfaces) for the NFS clients. If you specify a wildcard (`*`), IP network, or netgroup, NFS clients might not be able to access the NFS share.<br>In **Permission mode** and **Anonymous mapping**, select options for the public destination that is specified in the text box and has permission to access the NFS share.<br>**Permission mode**<br>Use a radio button to select the appropriate access permission for the NFS share.<br>Select **Read only** to prohibit data writes, or select **Read/Write** to permit data writes.<br>For the **Read/Write** option, select a synchronous write mode from the drop-down list.<br>*Synchronous write mode optimization* (**sync (optimized)**) is a function that delays slightly the writing of write requests to disk when a related write request is currently executing or is expected from the NFS client. This optimization can enhance performance because multiple write requests are written to disk in a single operation.<br>If the data write requests received by the NFS server will generally be unrelated, optimization will reduce performance. In this case, select **sync**.<br>**sync**<br>Write synchronously without optimization.<br>**sync (optimized)**<br>Write synchronously with optimization.<br>**Anonymous mapping**<br>*Anonymous mapping* is a function that maps a client accessing an NFS share to an arbitrary user ID or group ID instead of using the client's own user ID or group ID.<br>Use a radio button to select the users who access the NAS Modular system from the NFS client host, and are to be mapped as anonymous users.<br>▪ **everyone**<br>Select this when you map all users as anonymous users.<br>▪ **root only**<br>Select this when you map only the root user as an anonymous user.<br>**none**<br>Select this when you do not want to map users as anonymous users. |

| Item | Description |
|---|---|
| **Public destination host / network**<br>(continued) | In **Permission mode** and **Anonymous mapping**, specify options for the public destination that is set in the text box and has permission to access the NFS share, then click the **Set** button to add the specified host(s) or network(s) to the list box. Only the host and network names appearing in the list box will be set as hosts or networks accessing the NFS share.<br>The total length of the selected host names and network names (the length of each name + 4 bytes) must be less than 1,005 bytes. When the specified IP addresses can be resolved by using methods such as the hosts file or DNS, the total of the lengths calculated by using the host names that match the IP addresses (the length of each host name + 4 bytes) must also be less than 1,005 bytes.<br>To edit a host name or network name set in the list box, select the desired host name or network name and then click the **Edit** button. The settings for the selected item appear in the text box, **Permission mode** setting, and **Anonymous mapping** setting. After editing an item, click the **Set** button to update the changed settings back to the list box.<br>To delete a name from the list box, select the host or network name and click the **Delete** button. |
| **Anonymous UID** | Specify the user ID to be used when accessing the NFS share as an anonymous user.<br>Specify a value from 0 to 65,535.<br>If you do not enter any value, the anonymous UID is set to `65534`. |
| **Anonymous GID** | Specify the group ID to be used when accessing the NFS share as an anonymous user.<br>Specify a value from 0 to 65,535.<br>If you do not enter any value, the anonymous GID is set to `65534`. |
| **Transmission port restriction** | Use a radio button to select whether to accept only the requests from internet port lower than 1,024.<br>Select **Do not perform** if machines that use internet port 1,024 or higher are to access the file system.<br>**Perform**<br>Restrict ports requesting access to the file system.<br>**Do not perform**<br>Do not restrict ports requesting access to the file system.<br>***Note:***<br>In AIX, internet port 1,024 or higher is used by default.<br>Select **Do not perform** when AIX is used as an NFS client host and you want to use the default internet port setting.<br>In HP-UX, internet port 1,024 or higher is used for locking a file.<br>Select **Do not perform** to use HP-UX as an NFS client host. |

| Item | Description |
|---|---|
| **Subtree check** | Use a radio button to select whether to check that not only do the file and directory to be accessed have access permission (x permission), but also, all directories (subtrees) from the shared directory to the directory in which the file and directories to be accessed exist have execute permission (x permission). This is a security measure when only subdirectories of the file system are shared, not the entire file system.<br>If performance is a priority, select **Do not perform**.<br>If you use, as an NFS client, a machine that does not send authentication information for a lock request (the machine OS is HP-UX or a machine on which the `rpcinfo -p` command displays `100020` in `program`), or a machine that sends authentication information of a user other than the user who makes a lock request (the machine OS is AIX), select **Do not perform**. If you select **Perform**, a lock might not be able to be obtained (a lock request might result in the ENOLCK error) when execution permissions (x) for directories from the parent directory of a lock target file to the NFS mounted directory are not granted for an anonymous user in the NAS Modular system.<br>▪ **Perform** Perform a subtree check.<br>▪ **Do not perform** Do not perform a subtree check. |
| **Access check with lock request** | If you use, as an NFS client, a machine that does not send authentication information for a lock request (the machine OS is HP-UX or a machine on which the `rpcinfo -p` command displays `100020` in `program`) or a machine that sends authentication information of a user other than the user who makes a lock request (the machine OS is AIX), select **Do not perform**.<br>If you select **Perform**, a lock might not be able to be obtained (a lock request might result in the ENOLCK error) when read permissions (r) for directories from the parent directory of a lock target file to the NFS mounted directory are not granted for an anonymous user in the NAS Modular system.<br>▪ **Perform**<br>Check permissions for a lock request. If anonymous mapping is not set for the user, permissions for the user who locked the files are checked. If anonymous mapping is set for the user, permissions for the anonymous user in the NAS Modular system are checked. The owner of the locked files can lock them without permissions. Also, if the user has read permissions, they can write lock the files.<br>▪ **Do not perform**<br>Do not check accessibility at a lock request. Permissions for an anonymous user in the NAS Modular system are checked. |

### 4.11.5 Deleting an NFS Share

You can use the **List of File Shares** (List of NFS File Shares) window to delete an NFS share. If an error occurs while an NFS share is being deleted, a warning message is output, and the deletion process stops.

To delete an NFS share:

1. In the **Main Menu** window, click the **File Share Management** button.

   The **List of File Shares** (List of NFS File Shares) window displays. For window details, see section 4.11.1. If the **List of File Shares** (List of CIFS File Shares) window is active, select **List of NFS file shares** from the drop-down list, and then click the **Display** button.

2. Use a radio button to select the NFS share you want to delete, and then click the **Delete** button.

A dialog box confirms that you want to delete the shared directory and remove access settings for the hosts or networks that access the selected NFS share.

3. Click the **OK** button.

   The selected NFS share is deleted.

### 4.11.6 When Creating an NFS Share Fails

If an attempt to create an NFS file share fails, you must check and clear the error details, and then try to create the NFS file share again.

If you try to create an NFS file share for a file system right after creating or mounting a file system from the GUI, the error may be caused by the creation or mounting of the file system. After checking and clearing the error details on the creation of the NFS file share, check the results of creating or mounting the file system. For more information, see section 4.10.2.

To clear the error details:

1. In **Main Menu** window, click the **File Share Management** button.

   The **List of File Shares** (List of NFS File Shares) window appears. For details on this window, see section 4.11.1.

2. Use a radio button to select the NFS file share for which creation terminated abnormally, and then click the **Error Details** button.

   The **Error Details** window appears.

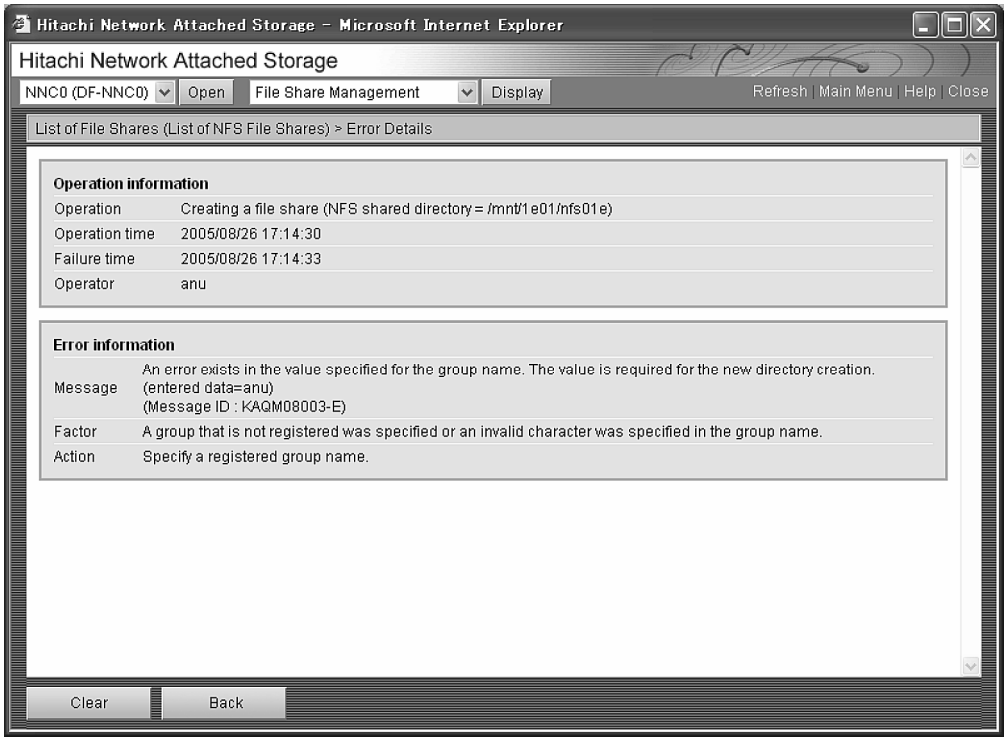



**Figure 4.93 Creating an NFS File Share Error Details Window**

3. Check the displayed information, such as the error message and information on the cause of the error, and the action to be taken. Then, click the **Clear** button.

   A dialog box appears asking you to confirm that the error details can be cleared.

   The following table describes the information displayed in the **Error Details** window:

**Table 4.55 Creating an NFS File Share Error Details Window**

| Item | Description |
|---|---|
| **Operation** | Displays the information on the operation that terminated abnormally, in the following format: `Creating a file share (NFS shared directory = shared-directory-name-for-the-NFS-file-share)` |
| **Operation Time** | Displays the date and time the operation was performed. |
| **Failure Time** | Displays the date and time the operation failed. |
| **Operator** | Displays the user name of the system administrator who tried to run the operation. |
| **Message** | Displays the error message and message ID. |
| **Factor** | Displays the cause of the error. |
| **Action** | Displays corrective action. |

4. Click the **OK** button.

   The error details are cleared and the **List of File Shares** (List of NFS File Shares) window appears again.

5. Take action according to the error details that you checked.

After the action finishes, try to create the NFS file share again. For details on how to do this, see section 4.11.2.

### 4.11.7 Viewing CIFS Share Information

You can use the **List of File Shares** (List of CIFS File Shares) window to view information about CIFS shares.

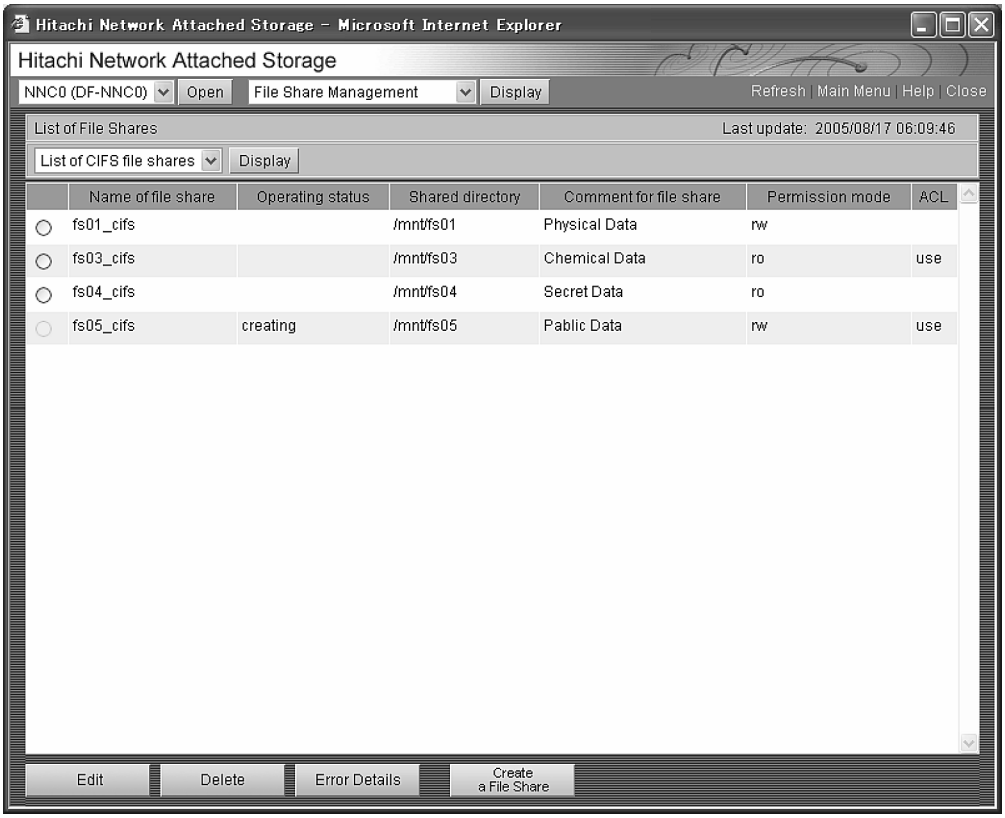



**Figure 4.94 List of File Shares (List of CIFS File Shares) Window**

#### 4.11.7.1 Before Managing CIFS Shares

Note the following points before managing CIFS shares:

- In the following environments, you cannot use the GUI to set write permissions on CIFS shares for each user or group:
  - An environment in which the total number of users registered by NAS Manager, the NIS server, and the LDAP server for user authentication exceeds 10,000
  - An environment in which the total number of groups registered by NAS Manager, the NIS server, and the LDAP server for user authentication exceeds 10,000
  - An environment operating in command operation mode
  - An environment that uses user mapping

Use the `enas_cifscreate` or `enas_cifsedit` command. For details on how to use a command to manage CIFS shares, see 5.6.2.

- We recommend that you enable recording of the file creation time in the file system before creating a CIFS share. When recording of the file creation time in the file system is enabled by a system administrator, CIFS clients can check the creation times of files in the file system.

.To change the setting for recording the file creation time for an existing file system, see 5.5.9.

Table 4.56 describes the information that is displayed in the window.

**Table 4.56 CIFS Shares Data Displayed in List of File Shares Window**

| Item | Description |
|---|---|
| **Last Update** | The date and time the information displayed in the window was last updated. |
| **Name of file share** | Name of a CIFS share that can be viewed from a client |
| **Operating Status** | The status of the creation of the CIFS file share.<br>**Creating** Creation of the CIFS file share is waiting to be used or is being used.<br>**Error** The attempt to create the CIFS file share terminated abnormally after it was queued. Take action, following the procedure in 4.11.2(7) Action to take if creation of a CIFS file share has terminated abnormally.<br>If creation of the CIFS file share has terminated normally, nothing is displayed. |
| **Shared directory** | Name of the shared directory |
| **Comment for file share** | Comment for the CIFS share that can be viewed from a client. |
| **Permission mode** | Access permission for the CIFS share:<br>▪ `ro` Read only permission<br>▪ `rw` Read/write permission |
| **ACL** | When youview or set the ACL from the client, `Use` is displayed. |

To view information about CIFS shares:

1. In the **Main Menu** window, click the **File Share Management** button.

   The **List of File Shares** (List of NFS File Shares) window displays. For window details, see section 4.11.1.

2. Select **List of CIFS file shares** from the drop-down list, and then click the **Display** button.

   The **List of File Shares** (List of CIFS File Shares) window displays.

### 4.11.8 Creating a CIFS Share

You can use the **Create CIFS File Share** window to create a CIFS share. Make sure that there are no more than 256 CIFS shares per cluster.

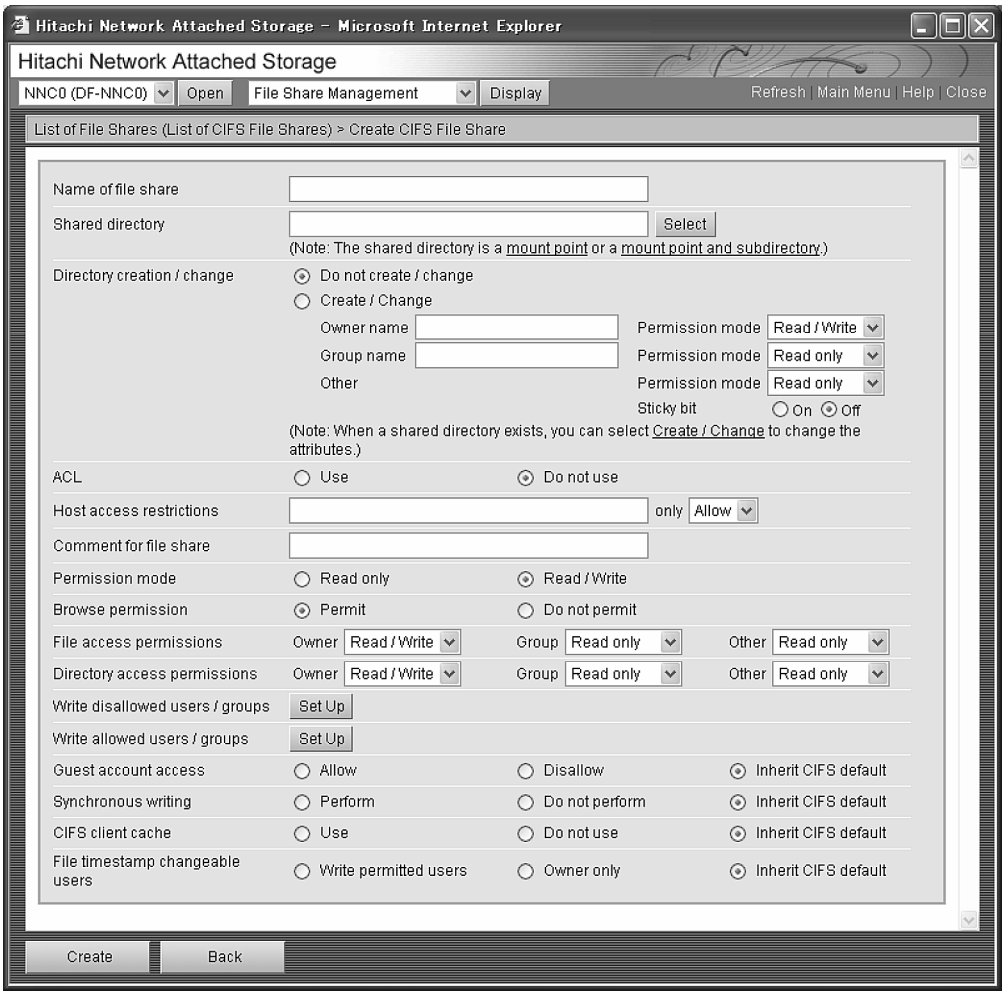



**Figure 4.95 Create CIFS File Share Window**

If an error occurs during CIFS share creation, the previous status is restored. If a resource group failover or restart occurs after the share is created, the entered settings do not change.

When an automatic creation schedule is set up in NAS Sync Image for a file system for which a CIFS share was created, if a file share is automatically created for a snapshot, that CIFS share is created for the snapshot using the CIFS share information created in this window.

To create a CIFS share:

1. In the **Main Menu** window, click the **File Share Management** button.

   The **List of File Shares** (List of NFS File Shares) window displays. For window details, see section 4.11.1.

2. Select **List of CIFS file shares** from the drop-down list, and then click the **Display** button.

   The **List of File Shares** (List of CIFS File Shares) window displays.

3. Click the **Create a File Share** button.

   The **Create CIFS File Share** window displays. Information about the window's contents is described in Table 4.57.

4. Enter the required information, and then click the **Create** button.

   The **List of File Shares** (List of CIFS File Shares) window appears again, and `Creating` is displayed in **Operating status** in the window.

   The system administrator must click **Refresh** in the **List of File Shares** (List of CIFS File Shares) window to check the latest information displayed in **Operating status**. If nothing is displayed in **Operating status**, the task has terminated normally. If `Error` is displayed in **Operating status**, the task terminated abnormally after it was queued.

   The CIFS share is created and the **List of File Shares** (List of CIFS File Shares) window re-displays.

**Table 4.57 Create CIFS File Share Window**

| Item | Description |
|---|---|
| **Name of file share** | Enter the name of the CIFS share that can be viewed from a client. Specify a unique name for the CIFS share within a node.<br>Enter a maximum of 80 characters. If the NAS Sync Image automatic creation schedule (automatic creation of shares) was used, the CIFS share name can be a maximum of 69 characters.<br>You can use any alphanumeric character, left parenthesis ( `(`), right parenthesis (`)` ), hyphen (`-`), period (`.`), at mark (`@`), and underscore (`_`). However, you cannot specify a name that consists only of a single or double period (`.` or `..`). You also cannot specify a period (`.`) at the end of the entry (for example, "`Abc.`").<br>In Windows, the entered value is not case sensitive. Specify a name that is unique regardless of whether upper-case or lower-case alphabetic characters are used.<br>You cannot specify `global`, `homes`, and `printers` for a CIFS share name. |

| Item | Description |
|---|---|
| **Shared directory** | Specify the full path of the shared directory. Clicking the **Select** button displays the **List of Mounted File Systems** window. In the List of Mounted Files Systems window, select a file system to be shared as a CIFS share, or enter its name directly in the text box. To select a file system in the **List of Mounted File Systems** window for creating a CIFS share, see section 4.11.9.<br>If you display this window by clicking the **Create and Set Up CIFS Share** button in the **Create New File System** window, the mount point specified for **File system** in the **Create New File System** window is displayed. Create a CIFS share under the displayed mount point. The **Select** button is not displayed.<br>Specify a unique name for the CIFS directory within the cluster. Make sure that you use an absolute path to specify the directory.<br>Enter from 6 to 256 characters. If the NAS Sync Image automatic creation schedule (automatic creation of shares) was used, the CIFS share directory can be a maximum of 241 characters.<br>You can use any alphanumeric character, hyphen (-), period (.), forward slash (/), and underscore (_). **Shared directory** is case-sensitive.<br>▪ When sharing a directory of the file system:<br>/mnt/*name-of-mounted-file-system*/*path-name*<br>***Example***: /mnt/filesystem01/share1<br>▪ When sharing the whole file system:<br>/mnt/*name-of-mounted-file-system*<br>***Example***: /mnt/filesystem02 |

| Item | Description |
|---|---|
| **Directory creation / change** | Use a radio button to select whether to create a new directory if the directory you set in **Shared directory** does not exist. If the directory has been created and is not specified in **Shared directory** for an NFS share, you can change properties for the specified directory.<br>The created directory will not be automatically deleted even if you delete the CIFS share.<br>If the directory specified in **Shared directory** has already been created, and you want to inherit its attributes, select **Do not create / change**. To create a new directory, or to change the attributes of a directory already created, select **Create / Change**. If you select **Create / Change**, select or enter the following items:<br>▪ **Owner**<br>Specify the name or user ID of the directory owner. When specifying a user registered by user mapping, specify the user as follows:<br>*domain-name**user-name*<br>▪ **Group**<br>Specify the name or group ID of the owner's group. When specifying a group registered by user mapping, specify the group as follows:<br>*domain-name**group-name*<br>***Note:*** When the authentication mode assigned to the CIFS service is Active Directoryauthentication, set the value specified in **Domain name (NetBIOS)** in the Active Directory Authentication window as the domain name used for **Owner** or **Group**.<br>▪ **Permission mode**<br>From the drop-down list, select an access permission for the directory owner, owner's group, and others.<br>**Read/Write**<br>Select this mode to grant both read and write permissions. The directory execution permission is granted.<br>**Read only**<br>Select this mode to grant read permission only. The directory execution permission is granted.<br>**None**<br>Select this mode when neither read and write permissions nor the directory execution permission is granted. This mode is available for **Group** and **Other**.<br>▪ **Sticky bit**<br>Permit only owner of files or subdirectories under the directory to delete or rename them. Use a radio button to select whether to set a sticky bit for the directory.<br>The attributes of directories for the mount point of a file system are:<br>▪ The owner of the directory is `root` and has `Read/Write` permission.<br>▪ The owner group of the directory is `root` and has `Read Only` permission.<br>▪ Others: `Read Only` permission<br>Therefore, if a CIFS share directory is specified for the mount point, change the permissions to enable users to use the CIFS share directory. |
| **ACL** | Use a radio button to select whether the ACL settings are to be viewed or specified from a client.<br>An ACL cannot be set for the guest account (`nobody`).<br>**Use**<br>Specify this if you want to view or set ACLs from the client.<br>**Do not use**<br>Specify this if you do not want to view or set ACLs from the client.<br>If **Use** is selected when a CIFS share is created, this item cannot be changed to **Do not use** even when you are not using ACLs after the creation of the CIFS share. |

| Item | Description |
|---|---|
| **Host access restrictions**<br>See ***Note 1*** | Enter this item when you want to limit access by CIFS client hosts or networks to CIFS shares. You can use a maximum of 1,023 characters. If this item is omitted, all hosts are allowed access to the CIFS shares.<br>If you want to limit access to a CIFS share, enter the host name or network address in the text box and select whether to allow access to CIFS shared files from the drop-down list. Multiple host names or network addresses must be separated by commas ( , )<br>See ***Note 2, 3,*** and ***4***<br>**Allow** Allow the specified hosts or networks to access CIFS shared files.<br>**Deny** Do not allow the specified hosts or networks to access CIFS shared files. |
| **Comment for file share** | Enter a comment for the CIFS share that can be viewed from a client.<br>Enter a maximum of 256 characters.<br>You can use any alphanumeric character, exclamation mark ( ! ), number sign (#), dollar sign ($), ampersand (&), apostrophe ( ' ), left parenthesis ( ( ), right parenthesis ( ) ), asterisk (*), plus sign (+), comma ( , ), hyphen (-), period ( . ), forward slash (/), colon ( : ), left angle bracket (<), right angle bracket (>), question mark (?), at mark (@), left bracket ( [ ), backslash (\), right bracket ( ] ), circumflex (^), underscore (_), grave accent (`), left brace ( { ), vertical bar ( \| ), right brace ( } ), and tilde (~). You can also specify spaces, but not at the beginning or end of the character string. A backslash (\) cannot be used at the end of the entry.<br>This item is optional. |
| **Permission mode** | Use a radio button to select the access permission for the CIFS share. Users or groups for which the access permission specified here applies must match the settings for **Permission mode**, in **Directory creation / change.** If you do not have write permission for the shared file system, select **Read only**. In this case, even if you select **Read/Write**, **Read only** will be set:<br>▪ **Read/Write**<br>Read/write permission.<br>▪ **Read only**<br>Read only permission. |
| **Browse permission** | Use a radio button to select whether to display a CIFS share name in the CIFS share name list, in the CIFS client environment:<br>**Permit**<br>Select this if you want to display a share name in the CIFS share name list.<br>**Do not permit**<br>Select this if you do not want to display a share name in the CIFS share name list. |
| **File access permissions** | If you selected the **Read/Write** radio button in **Permission mode**, from the drop-down list select an access permission for creating files in the CIFS share for the owner, the owner's group, and others. Set the access permissions separately for **Owner**, **Group**, and **Other**.<br>You can select any of the following:<br>▪ **Read/Write**<br>Select this to grant both read and write permissions.<br>▪ **Read only**<br>Select this to grant read permission only.<br>▪ **None**<br>Select this to grant neither read nor write permission<br>If a file is updated when **None** is set for **Group** and an item other than **None** is set for **Other**, the owner group's access permissions set for the file may be removed. When you set **None** for **Group**, also set **None** for **Other**. |

| Item | Description |
|---|---|
| **Directory access permissions** | If you selected the **Read/Write** radio button in **Permission mode**, from the drop-down list select an access permission for creating directories in the CIFS share for the owner, the owner's group, and others. Set the access permission separately for **Owner**, **Group**, and **Other**.<br>▪ **Read/Write**<br>Select this to grant both read and write permissions.<br>▪ **Read only**<br>Select this to grant read permission only.<br>▪ **None**<br>Select this to grant neither read nor write permission. Only search permission is granted. |
| **Write disallowed users / groups** | Specify the users or groups who will have read-only access to the CIFS share. The users and groups registered by user mapping cannot be specified.<br>This setting only takes effect when the **Permission mode** is set to **Read/Write**.<br>When you click the **Set Up** button, the **Write Disallowed Users / Groups Setup** window appears. For details on setting the access permission for CIFS shares for a user or group, see section 4.11.10. |
| **Write allowed users / groups** | Specify the users or groups who will have read-write access to the CIFS share. The users and groups registered by user mapping cannot be specified.<br>This setting only takes effect when the **Permission mode** is set to **Read only**.<br>Specify users or groups for which **Directory creation / change** is set to **Read/Write**. Even if you specify users or groups for which **Read/Write** is not set, file writes are not permitted.<br>If you do not have write permission for the shared file system and specify a user or group that has write permission, the setting will not take effect.<br>When you click the **Set Up** button, the **Write Allowed Users / Groups Setup** window appears. For details on setting the access permission for CIFS shares for a user or group, see section 4.11.10. |
| **Guest account access**<br>See ***Note 5*** | Specify access permissions for guest account users.<br>▪ **Allow**<br>Select this to allow guest account users to access CIFS share.<br>▪ **Disallow**<br>Select this to disallow guest account users to access CIFS share.<br>▪ **Inherit CIFS default**<br>Select this to inherit the CIFS default that was set in the configuration definition for the CIFS service.<br>See ***Note 6*** |

| Item | Description |
|---|---|
| **Synchronous writing** | Specify whether to perform synchronous control for writing when a write request is issued from the CIFS client to the CIFS share folder.<br>If **Perform** is selected, data reliability improves when an error occurs in the network or the CIFS client, because a flush to disk is performed each time the CIFS client issues a write request. However, performance might deteriorate because a flush to disk occurs each time a write request is issued.<br>Regardless of the setting for this item, data can be saved to the disk when there is a flush to the file to be updated, or when the file is closed.<br>▪ **Perform**<br>Select this to perform synchronous control when a write request is issued from a client.<br>▪ **Do not perform**<br>Select this to not perform synchronous control when a write request is issued from a client.<br>▪ **Inherit CIFS default**<br>Select this to inherit the CIFS default that was set in the configuration definition for the CIFS service.<br>See ***Note 6*** |
| **CIFS client cache** | Specify whether the updated data in the CIFS share file is to be cached on the client.<br>If **Use** is selected, performance improves when the updated data in the CIFS share file is cached on the client. However, when an error occurs in the network or CIFS client, data reliability might deteriorate.<br>▪ **Use**<br>Select this if the updated data in the CIFS share file is to be cached on the client.<br>▪ **Do not use**<br>Select this if the updated data in the CIFS share file is not to be cached on the client.<br>▪ **Inherit CIFS default**<br>Select this to inherit the CIFS default that was set in the configuration definition for the CIFS service.<br>See ***Note 6*** |
| **File timestamp changeable users** | Select the users for whom you want to allow updating of the CIFS share file timestamp. Select **Write permitted users** if the file is only shared by the CIFS service.<br>▪ **Write permitted users**<br>Select this to permit timestamp updating for all users who are permitted to write to the file.<br>▪ **Owner only**<br>Select this if you want to restrict timestamp updating to the file owner.<br>▪ **Inherit CIFS default**<br>Select this to inherit the CIFS default that was set in the configuration definition for the CIFS service. See ***Note 6*** |

***Note 1:*** If you set **Host access restrictions** in the **CIFS Service Management** window, the settings in the **CIFS Service Management** window are applied to all CIFS shares regardless of the settings in the **Create CIFS File Share** window or **Edit CIFS File Share** window. If you want to set **Host access restrictions** for each CIFS share, set **Host access restrictions** in the **Create CIFS File Share** window or **Edit CIFS File Share** window, and do not set **Host access restrictions** in the **CIFS Service Management** window.

***Note 2:*** The user authentication of a CIFS client is performed even though access to the CIFS share is permitted in **Host access restrictions.**

***Note 3:*** When you specify the host name in **Host access restrictions**, edit the `/etc/hosts` file in the **Edit System File** window to add the names and IP addresses of all hosts that are specified in **Host access restrictions**. If the host names are not added to the `/etc/hosts` file, the specified information might be invalid when access to the CIFS share is permitted or denied in **Host access restrictions**. For details on how to edit the `/etc/hosts` file, see section 4.7.11:

- If **Allow** is selected, in the `/etc/hosts` file add the names and IP addresses of all hosts to which you want to grant access permissions.
- If **Deny** is selected, add all host names to the `/etc/hosts` file so that hosts that can access the CIFS share are distinguished from hosts that cannot access the CIFS share.

***Note 4:*** Specify the network in the following format:

- When specifying a network address, specify an IP address:

  (***example***: `10.203.15.0`)

- When specifying a network range by using a netmask, use the following format:

  *`network-address`*`/`*`netmask`* (***example***: `10.203.15.0/255.255.255.0`)

***Note 5:*** In **Guest account access**, access permissions can be specified for each CIFS share for guest account users. The guest account is regarded as `nobody` (user ID: `65534`) regardless of the CIFS service authentication mode. Therefore, allow access permissions in the CIFS share that guest account users can access as `nobody`. An ACL cannot be set for the guest account.

When access to the CIFS service by guest account users is not permitted (**Never** is specified in **Mapping to guest account** in the **CIFS Service Management** window), the guest account setup for each CIFS share is not applied.

***Note 6:*** When **Inherit CIFS default** is specified, the configuration definitions that have been applied for the CIFS service are used. Even though the configuration definitions are set in the **CIFS Service Management** window, the configuration definitions for the CIFS service are not applied until the service restarts. You can check the current configuration definitions for the CIFS service in the **CIFS Service Maintenance** window.

For details on the **CIFS Service Management** window, see section 4.6.3.1. For details on the **CIFS Service Maintenance** window, see section 4.6.4.1.

### 4.11.9 Selecting a File System for Creating a CIFS Share

In the **List of Mounted File Systems** window, the system administrator can select a file system to be shared as a CIFS share. The **List of Mounted File Systems** window lists the following file systems and differential-data snapshots:

- File systems and differential-data snapshots that have already been mounted.
- File systems and differential-data snapshots for which the mount operation is waiting for execution or being executed.

To select a file system to share as a CIFS share:

1. In the **Main Menu** window, click the **File Share Management** button.

   The **List of File Shares** (List of NFS File Shares) window displays. For window details, see section 4.11.1.

2. Select **List of CIFS file shares** from the drop-down list, and then click the **Display** button.

   The **List of File Shares** (List of CIFS File Shares) window displays. For window details, see section 4.11.7.

3. Click the **Create a File Share** button.

   The **Create CIFS File Share** window displays. For window details, see section 4.11.8.

4. To select from a list of mount points a mount point for a shared directory (mount point or mount point and subdirectories) to be accessed as a CIFS share, click the **Select** button for **Shared directory**.

   The **List of Mounted File Systems** window displays.

5. From the **List of Mounted File Systems**, use a radio button to select a file system for which you want to create a CIFS share, and then click the **OK** button.

   The **Create CIFS File Share** window re-displays. In **Shared directory** of the **Create CIFS File Share** window, the mount point of the selected file system is displayed. Enter the directories following the displayed mount point.

### 4.11.10 Setting User and Group Access Permissions

You can use the **Write Disallowed Users/Groups Setup** window and **Write Allowed Users/Groups Setup** window to set user and group access permissions for CIFS shares.

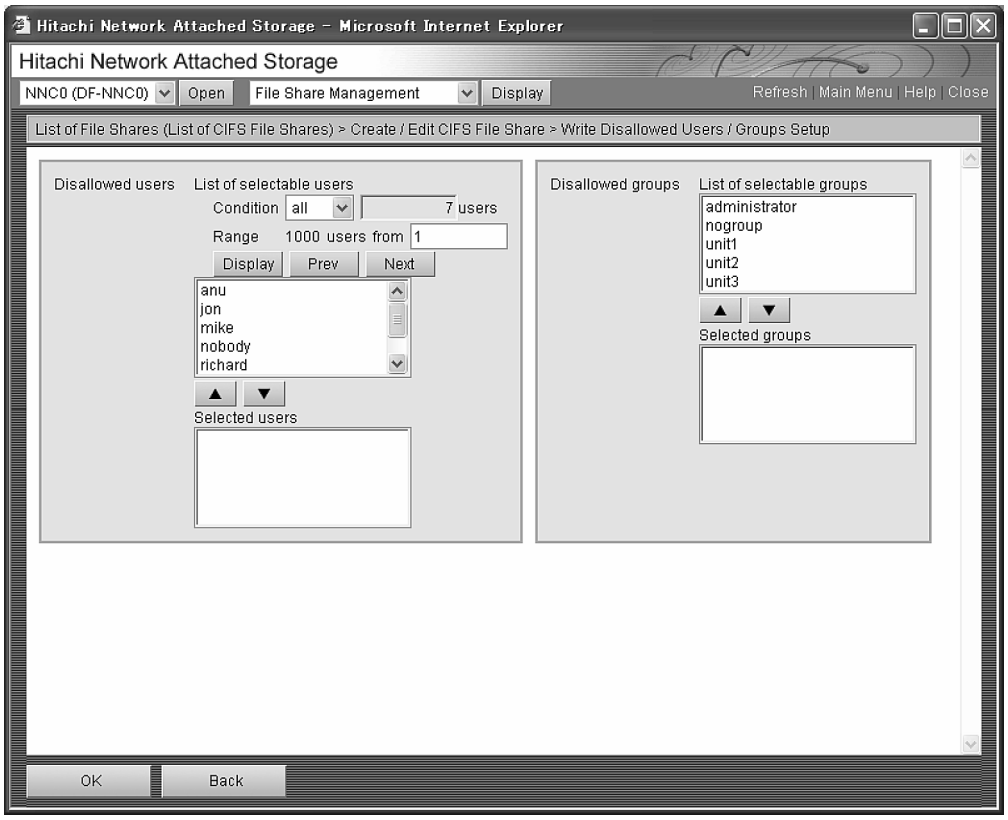



**Figure 4.96 Write Disallowed Users / Groups Setup Window**

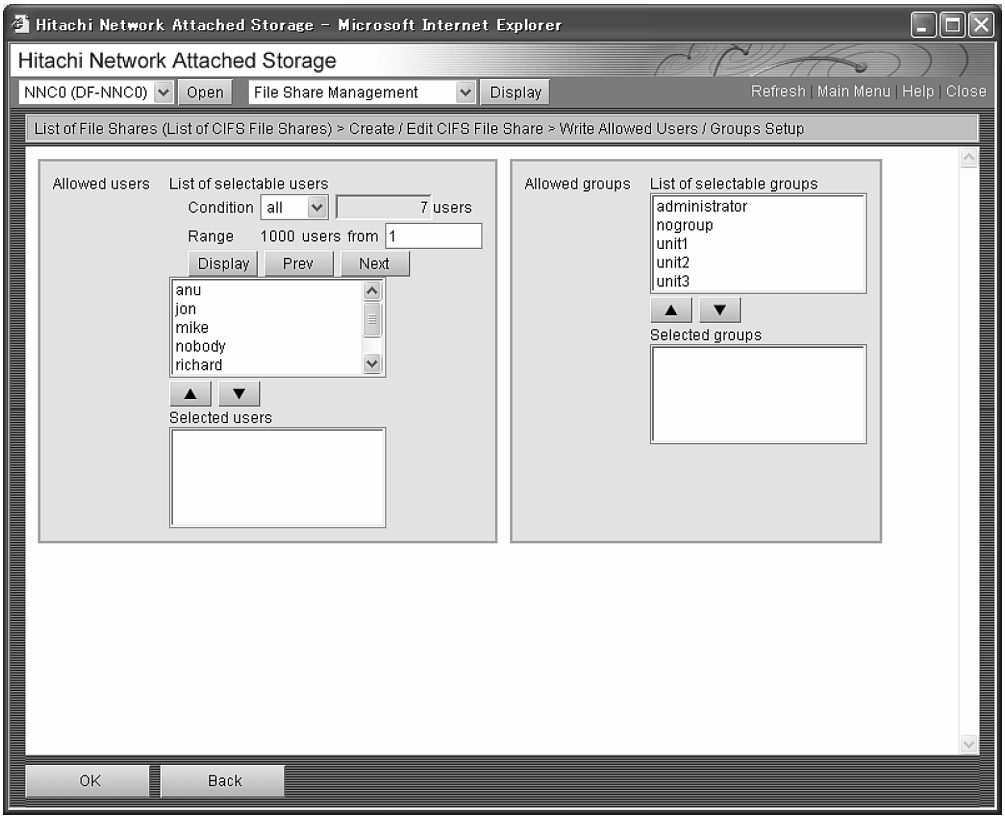



**Figure 4.97 Write Allowed Users / Groups Setup Window**

To set an access permission for a CIFS share for a user or group:

1. In the **Main Menu** window, click the **File Share Management** button.

   The **List of File Shares** (List of NFS File Shares) window displays. For window details, see section 4.11.1.

2. Select **List of CIFS file shares** from the drop-down list, and then click the **Display** button.

   The **List of File Shares** (List of CIFS File Shares) window displays. For window details, see section 4.11.7.

3. Click the **Create a File Share** button, or use a radio button to select the CIFS share and then click the **Edit** button.

   When you click the **Create a File Share** button, the **Create CIFS File Share** window displays. For window details, see section 4.11.8.

   When you use a radio button to select the CIFS share whose settings you want to change and click the **Edit** button, the **Edit CIFS File Share** window displays. For window details, see section 4.11.11.

4. To set the users and groups that will be prohibited from writing to the CIFS share, in the **Write disallowed users / groups** area, click the **Set Up** button.

   The **Write Disallowed Allowed Users/Groups Setup** window displays.

To set the users and groups that will be permitted to write to the CIFS share, in the **Write allowed users / groups** area, click the **Set Up** button to display the **Write Allowed Users/Groups Setup** window.

5. Enter the required information, and then click the **OK** button.

   Write permissions are set on the CIFS share on a user or group basis. When you transit from the **Create CIFS File Share** window, the **Create CIFS File Share** re-displays. When you transit from the **Edit CIFS File Share** window, the **Edit CIFS File Share** window re-displays.

**Table 4.58 Write Disallowed and Write Allowed Users / Groups Setup Window**

| Item | Description |
|---|---|
| **Allowed users** or **Disallowed users** | In the **List of selectable users** list box, select a user to grant read-only permission or read/write permission. If you do not have write permission for the shared file system and specify a user who has write permission, the setting will not take effect. If the same user is selected in **Allowed users** and **Disallowed users**, the **Allowed users** setting will take effect.<br>To filter the displayed users, select a filter from the **Condition** drop-down list, then click the **Display** button.<br>▪ **All** Displays all user names.<br>▪ **a** to **z**, **A** to **Z**, or **0** to **9** Displays user names that begin with the selected alphanumeric character.<br>▪ **Other** Displays user names that begin with a character other than an alphanumeric.<br>The total number of filtered users is shown on the right side of the **Condition** drop-down list. A maximum of 1,000 users can be displayed at the same time in the **List of selectable users** list box. If the number of users exceeds 1,000, you can use the following methods to specify the users to be displayed.<br>▪ **Range** text box Displays initially the sequence number of the user who is displayed at the beginning of the **List of selectable users** list box.<br>Specify a value equal to or less than the total number of filtered users, then click the **Display** button. This displays 1,000 users, beginning with the user whose sequence number you specified.<br>If you then select a different filter from the **Condition** drop-down list and click the **Display** button, the value specified in the **Range** text box is ignored and users are displayed beginning with the first user.<br>▪ **Prev** button Clicking this button displays in sequential order the users preceding the user displayed at the beginning of the **List of selected users** list box. If the user displayed at the beginning of the **List of selected users** list box is the first user, or if the total number of filtered users is 0, an error message appears when you click the **Prev** button.<br>▪ **Next** button Clicking this button displays in sequential order the users following the user displayed at the end of the **List of selected users** list box. If the user displayed at the end of the **List of selected users** list box is the last user, or if the total number of filtered users is 0, an error message appears when you click the **Next** button.<br>Make sure that there are no more than 100 users and groups who are granted read-only permission or read/write permission per file share. See ***Note.***<br>When you click the ▼ button, the users selected in the **List of selectable users** list box are added to the **Selected users** list box.<br>Only users listed in the **Selected users** list box will be set as users with the designated access permission.<br>To delete a user from the **Selected users** list box, select the user and click the ▲ button. |

| Item | Description |
|---|---|
| **Allowed groups** or **Disallowed groups** | In the **List of selectable groups** list box, select a group to grant read-only permission or read/write permission. If you do not have write permission for the shared file system and specify a group that has write permission, the setting will not take effect. If the same group is selected in **Allowed groups** and **Disallowed groups**, the **Allowed groups** setting will take effect.<br>Make sure that there are no more than 100 users and groups who are granted read-only permission or read/write permission per file share. See ***Note.***<br>When you click the ▼ button, the users selected in the **List of selectable users** list box are added to the **Selected users** list box. Only groups listed in the **Selected groups** list box will be set as groups with the designated access permission.<br>To delete a group from the **Selected groups** list box, select the group and click the ▲ button. |

***Note:*** The following formula must be satisfied, where *u* is the number of users, *g* is the number of groups, *n* is the number of characters used for all user names, and *m* is the number of characters used for all group names: $u+2g+n+m < 1024$

## 4.11.11 Editing Information About a CIFS Share

You can use the **Edit CIFS File Share** window to modify information about a CIFS share.

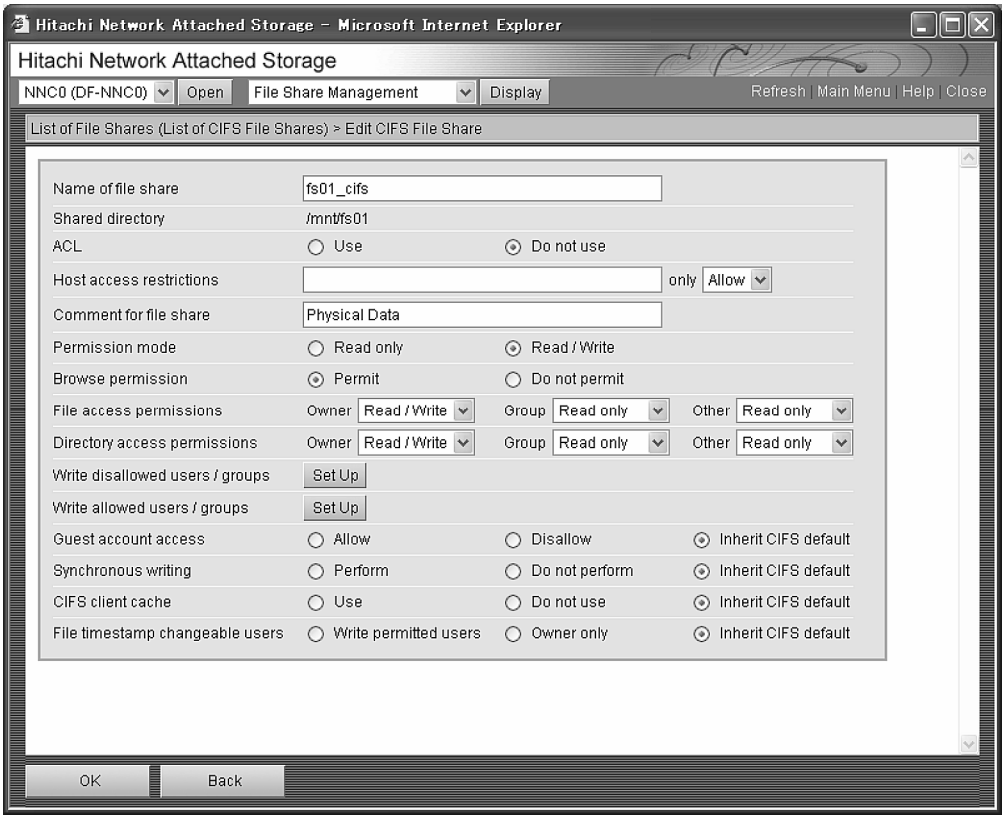



**Figure 4.98 Edit CIFS File Share Window**

For unchanged items, the current settings still apply after editing. If a failover or restart occurs during editing, the status is restored to the previous settings. When an automatic creation schedule is set up in NAS Sync Image for a file system for which a CIFS share was created, if a file share is automatically created for a snapshot, that CIFS share is created for the snapshot using the CIFS share information edited in this window.

To edit information about a CIFS share:

1. In the **Main Menu** window, click the **File Share Management** button.

   The **List of File Shares** (List of NFS File Shares) window displays. For window details, see section 4.11.1.

2. Select **List of CIFS file shares** from the drop-down list, and then click the **Display** button.

   The **List of File Shares** (List of CIFS File Shares) window displays. For window details, see section 4.11.7.

3. Use a radio button to select the CIFS share you want to edit, and then click the **Edit** button.

   The **Edit CIFS File Share** window displays. Information about the window's contents is described in Table 4.59.

4. Enter the required information, and then click the **OK** button.

   The CIFS share settings are updated, and the **List of File Shares** (List of CIFS File Shares) window re-displays.

**Table 4.59 Edit CIFS File Share Window**

| Item | Description |
|---|---|
| **Name of file share** | Enter the name of the CIFS share that can be viewed from a client. Enter a maximum of 80 characters. If the NAS Sync Image automatic creation schedule (automatic creation of shares) was used, the CIFS share name can be a maximum of 69 characters. |
| **ACL** | A radio button is used to select whether the ACL is to be viewed or set from the client.<br>An ACL cannot be set for the guest account (`nobody`).<br>▪ **Use**<br>Specify this button to view or set the ACL from the client.<br>▪ **Do not use**<br>Specify this button if you do not want to view or set the ACL from the client.<br>If **Use** was selected when the CIFS share was created, **Use** is displayed. In this case, this item cannot be changed to **Do not use**, even when you are not using the ACL. |
| **Host access restrictions**<br>See ***Note 1*** | Enter this item when you want to limit access by CIFS client hosts or networks to CIFS shares. You can use a maximum of 1,023 characters. If this item is omitted, all hosts are allowed access to the CIFS shares.<br>If you want to limit access to CIFS shares, enter the host name or network address in the text box and select whether to allow access to CIFS shared files from the drop-down list. Multiple host names or network addresses must be separated by commas ( **,** ). See ***Note 2, 3,*** and ***4***.<br>▪ **Allow**<br>Allow the specified hosts or networks to access CIFS shared files.<br>▪ **Deny**<br>Do not allow the specified hosts or networks to access CIFS shared files. |

| Item | Description |
|---|---|
| **Comment for file share** | Enter a comment for the CIFS share that can be viewed from a client. |
| **Permission mode** | Use a radio button to select an access permission for the CIFS share. Users or groups for which the access permission specified here applies must match the settings for **Permission mode**, in **Directory creation / change**, which were set when the CIFS share was created in the **Create CIFS File Share** window. If you do not have write permission for the shared file system, select **Read only**. In this case, even if you select **Read/Write**, **Read only** will be set:<br>▪ **Read/Write**<br>Read/write permission.<br>▪ **Read only**<br>Read only permission. |
| **Browse permission** | Use a radio button to select whether to display a CIFS share name in the CIFS share name list, in the CIFS client environment:<br>▪ **Permit**<br>Select this if you want to display a share name in the CIFS share name list.<br>▪ **Do not permit**<br>Select this if you do not want to display a share name in the CIFS share name list. |
| **File access permissions** | If you selected the **Read/Write** radio button in **Permission mode**, from the drop-down list select an access permission for creating files in the CIFS share for the owner, the owner's group, and others. Set the access permission separately for **Owner**, **Group**, and **Other**.<br>You can select either of the following:<br>▪ **Read/Write**<br>Read/write permission.<br>▪ **Read only**<br>Read only permission.<br>▪ **None**<br>Neither read or write permission.<br>If a file is updated when **None** is set for **Group** and an item other than **None** is set for **Other**, the owner group's access permissions set for the file might be removed. When you set **None** for **Group**, also set **None** for **Other**. |
| **Directory access permissions** | If you selected the **Read/Write** radio button in **Permission mode**, from the drop-down list select an access permission for creating directories in the CIFS share for the owner, the owner's group, and others. Set the access permission separately for **Owner**, **Group**, and **Other**.<br>▪ **Read/Write**<br>Read/write permission.<br>▪ **Read only**<br>Read only permission.<br>▪ **None**<br>Neither read or write permission. |
| **Write disallowed users / groups** | Specify the users or groups who will have read-only access to the CIFS share. The users and groups registered by user mapping cannot be specified.<br>This setting only takes effect when the **Permission mode** is set to **Read/Write**.<br>When you click the **Set Up** button, the **Write Disallowed Users / Groups Setup** window appears. For details on setting the access permission for CIFS shares for a user or group, see section 4.11.10. |

| Item | Description |
|---|---|
| **Write allowed users / groups** | Specify the users or groups who will have read-write access to the CIFS share. The users and groups registered by user mapping cannot be specified.<br>This setting only takes effect when the **Permission mode** is set to **Read only**.<br>Specify users and groups for which **Directory creation/change** is set to **Read/Write**. Even if you specify users and groups for which **Read/Write** is not set, file writes are not permitted. If you do not have write permission for the shared file system and specify a user or group that has write permission, the setting will not take effect.<br>When you click the **Set Up** button, the **Write Allowed Users / Groups Setup** window appears. |
| **Guest account access**<br>See ***Note 5*** | Specify access permissions for guest account users.<br>▪ **Allow**<br>Select this to allow guest account users access to the CIFS share.<br>▪ **Disallow**<br>Select this to disallow guest account users access to the CIFS share.<br>▪ **Inherit CIFS default**<br>Select this to inherit the CIFS default that was set in the configuration definition for the CIFS service.<br>See ***Note 6***. |
| **Synchronous writing** | Specify whether to perform synchronous control for writing when a write request is issued from the client to the CIFS share.<br>If **Perform** is selected, data reliability improves when an error occurs in the network or the CIFS client, because a flush to disk is performed each time the CIFS client issues a write request. However, performance might deteriorate because a flush to disk occurs each time a write request is issued.<br>Regardless of the setting for this item, data can be saved to the disk when there is a flush to the file to be updated, or when the file is closed.<br>▪ **Perform**<br>Select this to perform synchronous control when a write request is issued from a client.<br>▪ **Do not perform**<br>Select this to not perform synchronous control when a write request is issued from a client.<br>▪ **Inherit CIFS default**<br>Select this to inherit the CIFS default that was set in the configuration definition for the CIFS service.<br>See ***Note 6***. |
| **CIFS client cache** | Specify whether the updated data in the CIFS share file is to be cached on the client.<br>If **Use** is selected, performance enhances when the updated data in the CIFS share file is cached on the client. However, when an error occurs in the network or CIFS client, data reliability might deteriorate.<br>▪ **Use**<br>Select this if the updated data in the CIFS share file is to be cached on the client.<br>▪ **Do not use**<br>Select this if the updated data in the CIFS share file is not to be cached on the client.<br>▪ **Inherit CIFS default**<br>Select this to inherit the CIFS default that was set in the configuration definition for the CIFS service.<br>See ***Note 6***. |

| Item | Description |
|---|---|
| **File timestamp changeable users** | Select the users for whom you want to allow updating of the CIFS share file timestamp. Select **Write permitted users** if the file is only shared by the CIFS service.<br>▪ **Write permitted users**<br>Select this if you want to permit updating of the CIFS share file timestamp for all users who are permitted to write to this file.<br>▪ **Owner only**<br>Select this if you want to restrict timestamp updating to the file owner.<br>▪ **Inherit CIFS default**<br>Select this to inherit the CIFS default that was set in the configuration definition for the CIFS service.<br>See ***Note 6.*** |

***Note 1:*** If you set **Host access restrictions** in the **CIFS Service Management** window, the settings in the **CIFS Service Management** window are applied to all CIFS shares regardless of the settings in the **Create CIFS File Share** window or **Edit CIFS File Share** window. If you want to set **Host access restrictions** for each CIFS share, set **Host access restrictions** in the **Create CIFS File Share** window or **Edit CIFS File Share** window, and do not set **Host access restrictions** in the **CIFS Service Management** window.

***Note 2:*** The user authentication of a CIFS client is performed even though access to the CIFS share is permitted in **Host access restrictions**.

- ***Note 3:*** When you specify the host name in **Host access restrictions**, edit the `/etc/hosts` file in the **Edit System File** window to add the names and IP addresses of all hosts that are specified in **Host access restrictions**. If the host names are not added to the `/etc/hosts` file, the specified information might be invalid when access to the CIFS share is permitted or denied in **Host access restrictions**.

***Note 4:*** Specify the network in the following format:

- When specifying a network address, specify an IP address:

  (***example***: `10.203.15.0`)

- When specifying a network range by using a netmask, use the following format:

  *network-address*/*netmask* (***example***: `10.203.15.0/255.255.255.0`)

***Note 5:*** In **Guest account access**, access permissions can be specified for each CIFS share for guest account users. The guest account is regarded as `nobody` (user ID: `65534`) regardless of the CIFS service authentication mode. Therefore, allow access permissions in the CIFS share that guest account users can access as `nobody`. An ACL cannot be set for the guest account.

When access to the CIFS service by guest account users is not permitted (**Never** is specified in **Mapping to guest account** in the **CIFS Service Management** window), the guest account setup for each CIFS share is not applied.

***Note 6:*** When **Inherit CIFS default** is specified, the configuration definitions that have been applied for the CIFS service are used. Even though the configuration definitions are set in the **CIFS Service Management** window, the configuration definitions for the CIFS service are not applied until the service restarts. You can check the current configuration definitions for the CIFS service in the **CIFS Service Maintenance** window.

For details on the **CIFS Service Management** window, see section 4.6.3.1. For details on the **CIFS Service Maintenance** window, see section 4.6.4.1.

### 4.11.12 Deleting a CIFS Share

You can use the **List of File Shares** (List of CIFS File Shares) window to delete a CIFS share. If an error occurs while a CIFS share is being deleted, a warning message is output, and the deletion process stops.

To delete a CIFS share:

1. In the **Main Menu** window, click the **File Share Management** button.

   The **List of File Shares** (List of NFS File Shares) window displays. For window details, see section 4.11.1.

2. Select **List of CIFS file shares** from the drop-down list, and then click the **Display** button.

   The **List of File Shares** (List of CIFS File Shares) window displays. For window details, see section 4.11.7.

3. Use a radio button to select the CIFS share you want to delete, and then click the **Delete** button.

   A dialog box confirms that you want to delete the selected CIFS share.

4. Click the **OK** button.

   The selected CIFS share is deleted.

### 4.11.13 When a Creating a CIFS Share Fails

If you try to create an CIFS file share and it fails, check and clear the error message and try again. If you try to create an CIFS file share for a file system right after creating or mounting a file system, the error may be related to the creation or mounting of the file system. Check and clear any related messages. For more information, see section 4.10.2.

To clear the error message:

1. In **Main Menu** window, click the **File Share** Management button.
2. The **List of File Shares** (List of CIFS File Shares) window appears. For details on this window, see section 4.11.1.
3. Use a radio button to select the CIFS file share for which creation terminated abnormally, and then click the **Error Details** button.

   The **Error Details** window appears.

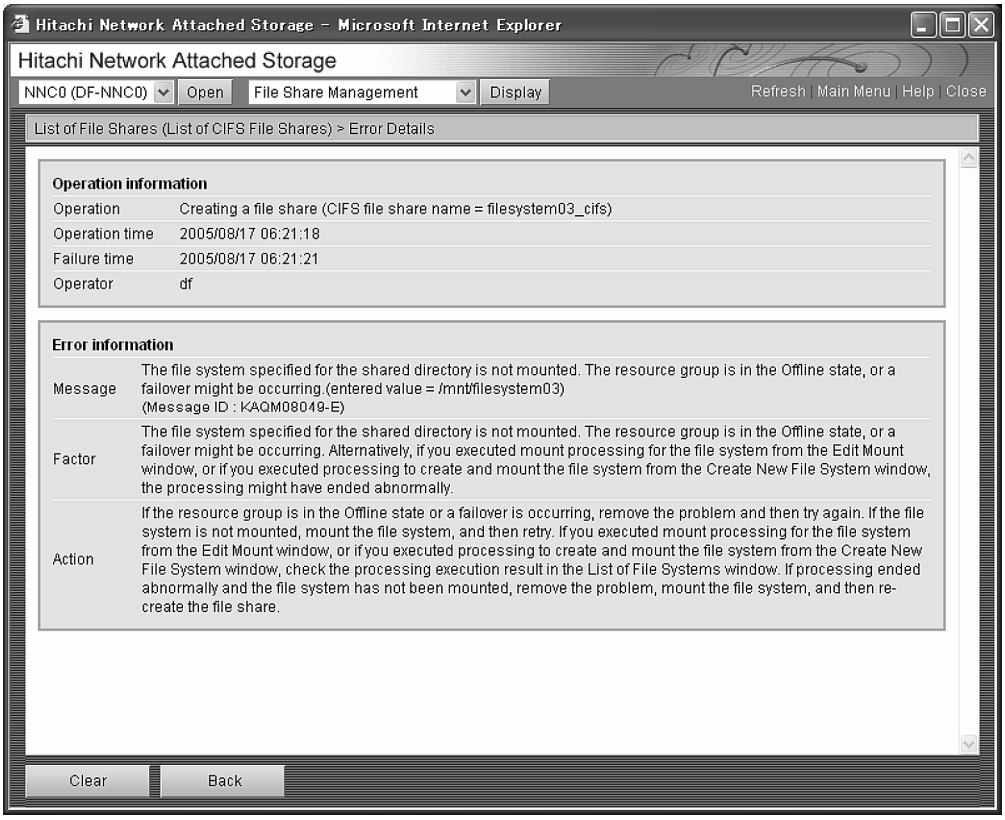



**Figure 4.99 Creating CIFS File Share Error Details Window**

4. Check the displayed information, such as the error message and information on the cause of the error, and the action to be taken. Then, click the **Clear** button.

   A dialog box appears asking you to confirm that the error details can be cleared.

   The following table describes the information displayed in the **Error Details** window:

**Table 4.60 Creating CIFS File Share Error Details Window (Information Displayed)**

| Item | Description |
|---|---|
| **Operation** | Displays the information on the operation that terminated abnormally, in the following format: `Creating a file share (CIFS shared directory = shared-directory-name-for-the-CIFS-file-share)` |
| **Operation Time** | Displays the date and time the operation was performed. |
| **Failure Time** | Displays the date and time the operation failed. |
| **Operator** | Displays the user name of the system administrator who tried to perform the operation. |
| **Message** | Displays the error message and message ID. |
| **Factor** | Displays the cause of the error. |
| **Action** | Displays corrective action. |

5. Click the **OK** button.

   The error details are cleared and the **List of File Shares** (List of CIFS File Shares) window appears again.

6. Take action according to the error details that you checked.

   After the action finishes, try to create the CIFS file share again. For details on how to do this, see section 4.11.1.

## 4.12 Managing Quotas

To prevent specific users from monopolizing space in a file system, you can use quota management functionality to set the upper limit for space that can be used.

The NAS Modular system allows you to manage quotas for each file system, or to manage subtree quotas for each directory immediately under the mount point. The following table shows information that can be set for each management method.

**Table 4.61 Information set for the quota management functionality**

| Information to be set | Managing quotas for each file system | | Managing subtree quotas | |
|---|---|---|---|---|
| | GUI | Command | GUI | Command |
| Quota for each user | Settable | Settable | Not settable | Settable |
| Quota for each group | Settable | Settable | Not settable | Settable |
| Quota for each directory | Not settable | Not settable | Not settable | Settable |
| Default quota | Settable | Settable | Not settable | Settable |
| Grace period | Settable | Settable | Not settable | Settable |
| Quota monitoring method | Settable | Settable | Not settable | Not settable |
| Disabling quotas set for a directory | Not settable | Not settable | Not settable | Settable |

The following explains information that can be set for quota management:

Setting the quota for each user, group, or directory

The quota can be set for each user or group. When subtree quotas are being managed, a quota can also be set for each directory.

You can use *quota management* to prevent excessive disk space usage by setting the upper limit of the disk space that is available to users.

The following settings can be entered for quota management:

- **Quota settings for each user or group**

  The quota can be set for each user or group:

  - **Hard limit**

You can set an upper limit (*hard limit*) on the block space and the number of i-nodes available to individual users or specific groups. The user or group cannot create files in excess of the quota setting as a hard limit.

- **Soft limit**

  You can set a warning value (*soft limit*) on the block space and the number of i-nodes available to individual users or specific groups. The user or group cannot create or update files once a fixed duration (*grace period*) has elapsed after the quota setting as a soft limit is exceeded. However, files can be updated, as long as block usage does not increase.

  When a user or group is no longer able to create or update files, by deleting files until block and i-node usage falls below the soft limits, files can again be created or updated.

  The soft limit must not exceed the quota setting as a hard limit.

- **Default quota setting**

  The default quota prevents excessive usage of block space and i-nodes in a file system when a quota has not been explicitly set for each user. The hard and soft limits can be set for each user or group using the same method as that used for setting the quota.

  The value set for the default quota is applied when a user, for whom a quota has not been set, uses the file system or directory with the default quota assigned for the first time (when the user creates the file).

  The default quota is applied to all users, including users registered by user mapping.

- **Grace period**

  You can set a fixed duration (*grace period*) to allow file creation and updating after the quota setting as a soft limit is exceeded.

- **Setting the quota monitoring method**

  When managing the quota for each file system, NAS Manager monitors quota information at specified times. Information about users or groups who have exceeded their soft limit or grace period is reported by using an SNMP trap or the `management.log` file.

  The quota monitoring times and the SNMP trap notification mode (when users or groups exceeding the soft limit or grace period are detected) can be set for each file system. There are two SNMP trap notification modes:

  - Summary notification mode (recommended)

    In this mode, NAS Manager reports only the number of users or groups whose soft limit or grace period has been exceeded when it detects such users or groups.

  - Individual notification mode

    In this mode, NAS Manager returns a quota information message for each user or group whose soft limit or grace period has been exceeded when it detects such users or groups. If the number of users or groups exceeds 100, NAS Manager stops notification in this mode and reports only the number of users or groups to the SNMP manager.

***Note:***

Individual notification mode has been set for the file systems whose quota monitoring times were set using NAS Manager 04-00. For these file systems, change the mode setting as needed.

The `management.log` file stores the same information as that reported in summary notification mode.

The following table lists the information items reported if an exceeded soft limit or grace period is detected.

**Table 4.62 Information reported if an exceeded soft limit or grace period is detected**

| Item | Summary notification | Individual notification | | |
|---|---|---|---|---|
| | | When a soft limit is exceeded | When a grace period is exceeded | When individual notification mode is suppressed |
| Notification time | Yes | Yes | Yes | Yes |
| NNC name | Yes | Yes | Yes | Yes |
| NNC number | Yes | Yes | Yes | Yes |
| Device identification number | Yes | Yes | Yes | Yes |
| File system name | Yes | Yes | Yes | Yes |
| User type (user/group) | -- | Yes | Yes | Yes |
| User name or group name | -- | Yes | Yes | -- |
| User ID or group ID | -- | Yes | Yes | -- |
| Type of limit exceeded (block/inode) | -- | Yes | Yes | -- |
| Current usage (unit of block usage: KB) | -- | Yes | Yes | -- |
| Soft limit value (unit of block usage: KB) | -- | Yes | Yes | -- |
| Hard limit value (unit of block usage: KB) | -- | Yes | Yes | -- |
| Remaining grace period (unit: seconds) | -- | Yes | -- | -- |
| Grace period (unit: days) | -- | -- | Yes | -- |
| Number of users or groups exceeding the soft limit for block usage | Yes | -- | -- | Yes |

| Item | Summary notification | Individual notification | | |
|---|---|---|---|---|
| | | When a soft limit is exceeded | When a grace period is exceeded | When individual notification mode is suppressed |
| Number of users or groups exceeding the grace period for block usage | Yes | -- | -- | Yes |
| Number of users or groups exceeding the soft limit for i-node usage | Yes | -- | -- | Yes |
| Number of users or groups exceeding the grace period for i-node usage | Yes | -- | -- | Yes |

Legend:

Yes: Reported, --: Not reported

When quota management is running, the disk usage is always monitored regardless of the quota monitoring time.

Block spaces are managed by the file system and used in units of 4 KB. Therefore, even if the total file size is less than the soft limit for a block space, the block space might exceed the soft limit.

When quotas are set for a specific user and for the group to which that user belongs, the smaller setting applies.

The following table shows an example of user quota settings:

**Table 4.63 User Quota Settings**

| User Name | Quota Setting for User | Primary Group | User's Groups |
|---|---|---|---|
| User A | 20 MB | Group 1 | Group 1 |
| User B | 20 MB | Group 1 | Group 1 |
| User C | 20 MB | Group 1 | Group 1 |
| User D | 30 MB | Group 2 | Group 1 and Group 2 |

Following is an explanation of the quota setting based on this example, where the available block space for Group 1 is 25 MB:

- A quota of 20 MB is set for users A, B, and C. That is, users A, B, and C can use 20 MB of block space in total. So, if user A is using 20 MB, users B and C will have 5 MB available between them.

- User D can use up to 30 MB of block space if no quota is set for user D's primary group (Group 2). However, if user D updates Group 1 files under the group's execution permission, user D will be restricted to use 25 MB.

### 4.12.1 Before Managing Quotas

Quotas are managed per file system. By managing quotas, you can restrict the block space and the number of i-nodes available to users or groups accessing a particular file system. The following are points that you must note before starting quota management:

- To manage quotas, you must enable the quota management functionality when you mount a target file system.

  For details on how to enable the quota functionality in the **Create New File System** window when using the GUI to create a file system.

- To start quota management for a file system being mounted, unmount the file system, and then re-mount the file system with the quota functionality enabled.

- When NAS Manager is in GUI operation mode, the system administrator cannot display the **List of Quota Information** window in the following environments. Place NAS Manager in command operation mode or use commands to perform quota management.

  - An environment in which the total number of users registered by NAS Manager, the NIS server, and the LDAP server for user authentication exceeds 10,000
  - An environment in which the total number of groups registered by NAS Manager, the NIS server, and the LDAP server for user authentication exceeds 10,000

  For details on how to switch to command operation mode, see 4.7.14. For details on how to use commands to manage quotas, see 5.7.

- When NAS Manager is in command operation mode, the system administrator cannot use the GUI to perform the following operations:

  - Viewing quota information of a user or group
  - Setting a user-based or group-based quota

  Instead of using the GUI, use commands to perform the above operations. For details on how to use commands to manage quotas, see 5.7.

- Use commands to manage quotas of users and groups registered by user mapping. For details on using commands for quota management, see 5.7.

- If you set a quota for users registered by user mapping, we recommend that you set the quota monitoring times.

- You can also issue a *get* request from the SNMP manager to view the quota information about users and groups for a file system. For details on the quota information that you can view by using a *get* request, see *B.1 MIB objects for responding to SNMP get requests*.

- The system administrator can view the quota information set for a file system. Also, a system administrator can directly edit the `/etc/snmp/snmpd.conf` file to set the threshold for the number of responses to the SNMP manager.

- To start managing the **Quota** of a file system that has been mounted, unmount the file system, set **Quota** to **On**, and re-mount the file system. Even though the file system is mounted, if the capacity of the file system is insufficient for the **Quota** management, Quota management will not be available. You must either expand the capacity of the file system or delete unnecessary files from it so as to increase free space, then re-mount the file system. For details on expanding the capacity of a file system, see section 4.10.8.
- When starting to manage the Quota of a file system that has been mounted, because internal system checks will take place when the file system is mounted next, the larger the used capacity of the file system is, the longer it takes to process the file system.

### 4.12.2 Viewing User Quota Information

The system administrator can view user quota information in the **List of Quota Information** (User) window. The following figure shows the **List of Quota Information** (User) window.

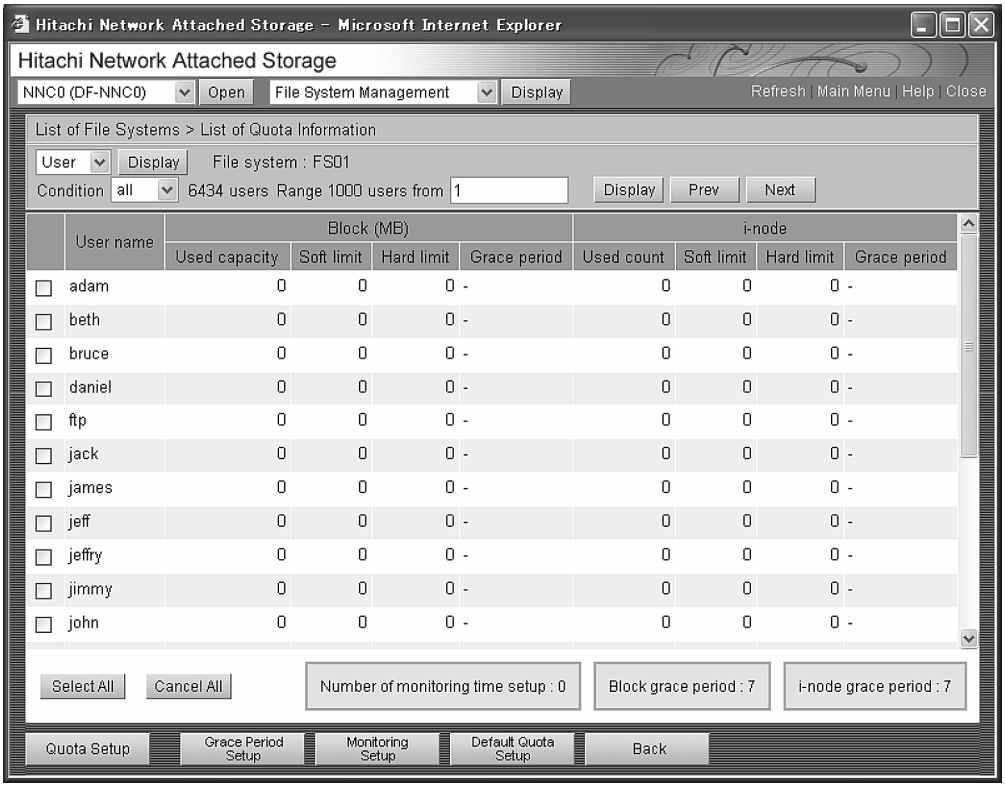



**Figure 4.100 List of Quota Information (User) Window**

***Note:*** When NAS Manager is in command operation mode, a message is displayed instead of a list of user quota information. The following table describes the information that is displayed in the window:

**Table 4.64 List of Quota Information (User) Window**

| Item | Description |
|---|---|

| Item | Description |
|---|---|
| **User name** | User name |
| **Block (MB)** | Block usage by individual user:<br>▪ **Used capacity**<br>Block space used (units: MB). Displayed in red if the block space used exceeds the value set as the soft limit or reaches the hard limit.<br>▪ **Soft limit**<br>Soft limit for block usage (units: MB) See ***Note***.<br>▪ **Hard limit**<br>Hard limit for block usage (units: MB) See ***Note***.<br>▪ **Grace period**<br>Remaining grace time until files can no longer be created after the user's block usage exceeds the soft limit. Displayed in one of the following formats:<br>*n* `days` The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.<br>*n* `hours` The remaining grace time is less than 24 hours. The value is shown in orange. For example, `0 hours` appears if less than 1 hour remains.<br>`Over` Either the grace period has expired or block usage has reached the hard limit. `over` is displayed in red.<br>**-** The user's block usage is within the soft limit. |
| **i-node** | i-node usage by individual user:<br>▪ **Used count**<br>Number of i-nodes used. Displayed in red if the number of i-nodes used exceeds the value set as the soft limit or reaches the hard limit.<br>▪ **Soft limit**<br>Soft limit for i-node usage. See ***Note.***<br>▪ **Hard limit**<br>Hard limit for i-node usage. See ***Note.***<br>▪ **Grace period**<br>Remaining grace time until files can no longer be created after the user's i-node usage exceeds the soft limit. Displayed in one of the following formats:<br>*n* `days` The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.<br>*n* `hours` The remaining grace time is less than 24 hours. The value is shown in orange. For example, `0 hours` appears if less than 1 hour remains.<br>`Over` Either the grace period has expired or i-node usage has reached the hard limit. `over` is displayed in red.<br>**-** The user's i-node usage is within the soft limit. |
| **Number of monitoring time setup** | Number of times per day that NAS Manager checks quotas. |
| **Block grace period** | Grace period until files can no longer be created or updated after block usage exceeds the soft limit. |
| **i-node grace period** | Grace period until files can no longer be created after i-node usage exceeds the soft limit. |

***Note:*** #1: If the default quota is set for the file system, the default quota values are applied to users for whom quota information has not been set.

To display user quota information:

1. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window displays. For window details, see section 4.10.4.

2. Use a radio button to select the file system whose quota information you want to view, and then click the **Quota Setup** button.

   The **List of Quota Information** (User) window displays. If the **List of Quota Information** (Group) window is active, select **User** from the drop-down list, and then click the **Display** button.

   To filter the users displayed in the **List of Quota Information** (User) window, select a filter from the **Condition** drop down list, and then click the **Display** button:

   - **All**

     Displays quota information for all users.

   - **a** to **z**, **A** to **Z**, or **0** to **9**

     Displays quota information for users whose names begin with the selected alphanumeric character.

   - **Other**

     Displays quota information for users whose names begin with a character other than an alphanumeric character.

     A maximum of 1,000 users can be displayed at the same time in the **List of Quota Information** (User) window. If the number of users exceeds 1,000, you can use the following methods to specify the users to be displayed.

   - **Range** text box

     Initially displays the sequence number of the user who is displayed at the beginning of the **List of Quota Information** (User) window.

     Specify a value equal to or less than the total number of filtered users, then click the **Display** button. This displays 1,000 users, beginning with the user whose sequence number you specified.

     If you then select a different filter from the **Condition** drop-down list and click the **Display** button, the value specified in the **Range** text box is ignored and users are displayed beginning with the first user.

– **Prev** button

  Clicking this button displays in sequential order the 1,000 users preceding the users currently displayed in the **List of Quota Information** (User) window. If there are fewer than 1,000 users preceding the user displayed at the beginning of the **List of Quota Information** (User) window, clicking the **Prev** button displays 1,000 users beginning with the first user. If the user displayed at the beginning of the **List of Quota Information** (User) window is the first user, or if the total number of filtered users is 0, an error message appears when you click the **Prev** button.

– **Next** button

  Clicking this button displays in sequential order the 1,000 users following the users currently displayed in the **List of Quota Information** (User) window. If the user displayed at the end of the **List of Quota Information** (User) window is the last user, or if the total number of filtered users is 0, an error message appears when you click the **Next** button.

### 4.12.3 Viewing Group Quota Information

The system administrator can view group quota information in the **List of Quota Information** (Group) window. The following figure shows the **List of Quota Information** (Group) window.

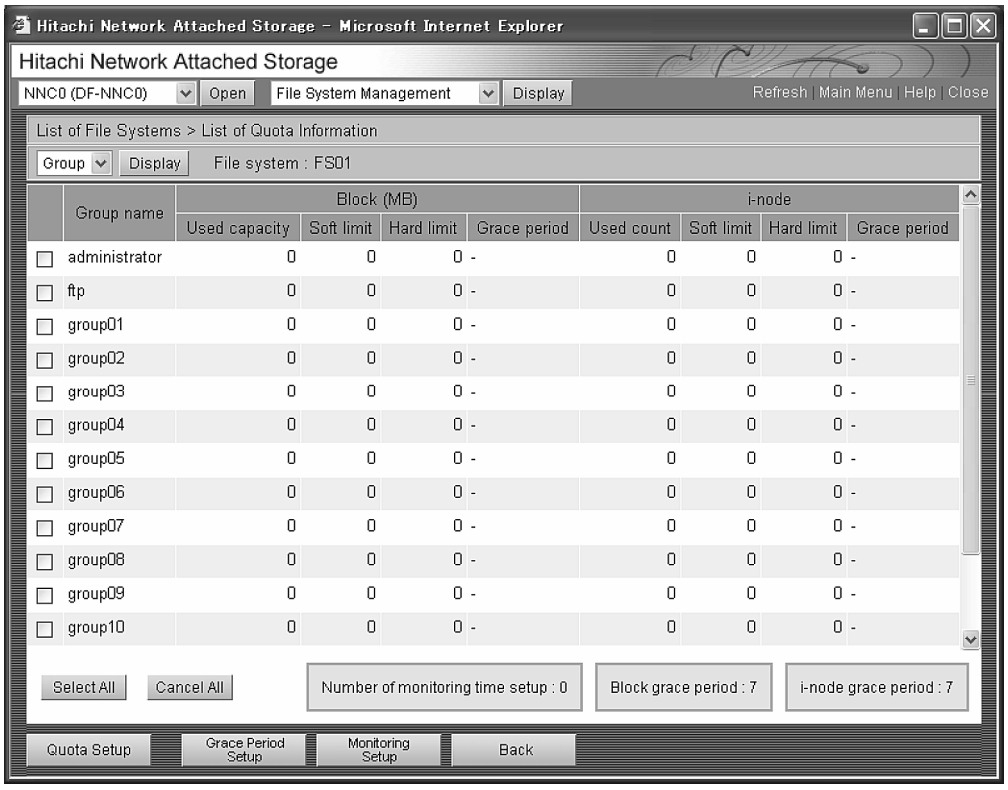



**Figure 4.101 List of Quota Information (Group) Window**

***Note:*** When NAS Manager is in command operation mode, a message is displayed instead of a list of group quota information.

The following table describes the information displayed in the window:

**Table 4.65 List of Quota Information (Group) Window**

| Item | Description |
|---|---|
| **Group name** | Group name |
| **Block (MB)** | Block usage by individual group:<br>▪ **Used capacity**<br>Block space used (units: MB). Displayed in red if the block space used exceeds the value set as the soft limit or reaches the hard limit.<br>▪ **Soft limit**<br>Soft limit for block usage (units: MB)<br>▪ **Hard limit**<br>Hard limit for block usage (units: MB)<br>▪ **Grace period**<br>Remaining grace time until files can no longer be created after the group's block usage exceeds the soft limit. Displayed in one of the following formats:<br>*n* `days` The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.<br>*n* `hours` The remaining grace time is less than 24 hours. The value is shown in orange. For example, `0 hours` appears if less than 1 hour remains.<br>`Over` Either the grace period has expired or block usage has reached the hard limit. `over` is displayed in red.<br>– The group's block usage is within the soft limit. |
| **i-node** | i-node usage by individual group:<br>▪ **Used count**<br>Number of i-nodes used. Displayed in red if the number of i-nodes used exceeds the value set as the soft limit or reaches the hard limit.<br>▪ **Soft limit**[1]<br>Soft limit for i-node usage.<br>▪ **Hard limit**[1]<br>Hard limit for i-node usage.<br>▪ **Grace period**<br>Remaining grace time until files can no longer be created after the group's i-node usage exceeds the soft limit. Displayed in one of the following formats:<br>*n* `days` The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.<br>*n* `hours` The remaining grace time is less than 24 hours. The value is shown in orange. For example, `0 hours` appears if less than 1 hour remains.<br>`Over` Either the grace period has expired or i-node usage has reached the hard limit. `over` is displayed in red.<br>– The group's i-node usage is within the soft limit. |
| **Number of monitoring time setup** | Number of times per day that NAS Manager checks quotas |
| **Block grace period** | Grace period until files can no longer be created or updated after block usage exceeds the soft limit. |
| **i-node grace period** | Grace period until files can no longer be created after i-node usage exceeds the soft limit. |

To display group quota information:

1. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window displays. For window details, see section 4.10.4.

2. Use a radio button to select the file system whose quota information you want to view, and then click the **Quota Setup** button.

   The **List of Quota Information** (User) window displays. For window details, see section 4.12.2.

3. Select **Group** from the drop-down list, and then click the **Display** button.

   The **List of Quota Information** (Group) window displays.

### 4.12.4 Setting Quotas

In the Quota Setup window, the system administrator can set a user or group quota for a file system.

Note the following when setting a user or group quota for a file system.

The default quota set for a file system does not apply to users for whom a quota has been set.

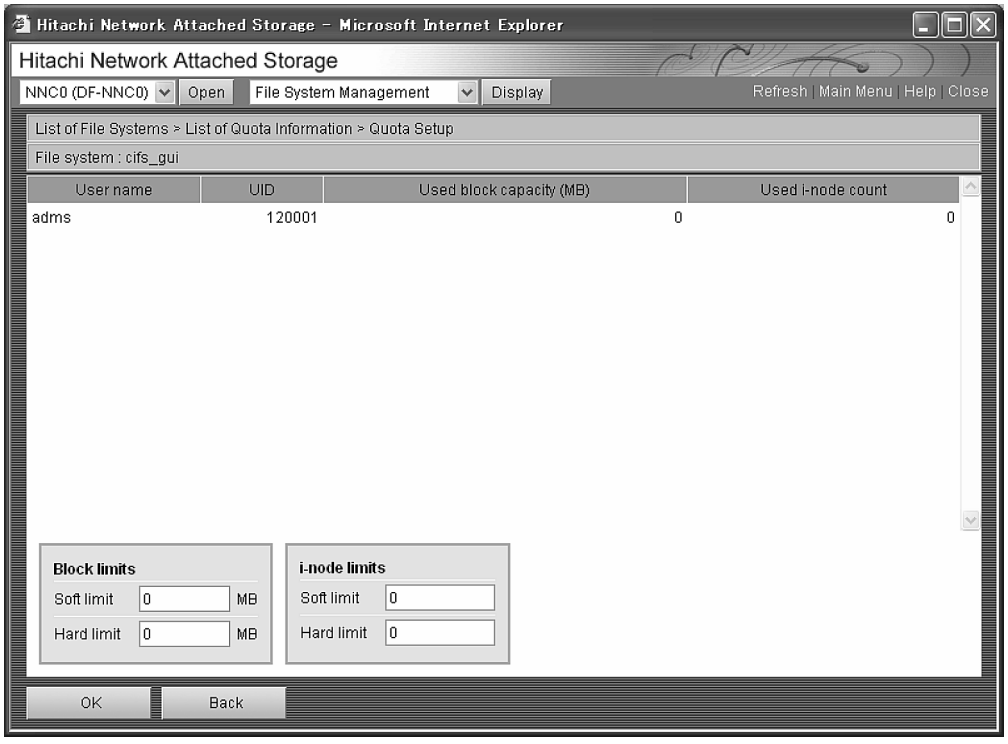



**Figure 4.102 Quota Setup Window**

Quotas cannot be set for the following snapshots:

- Snapshots taken by NAS Backup Restore
- Differential-data snapshots created with NAS Sync Image

While NAS Backup Restore recovers the file system from a snapshot, quotas cannot be set for file systems for which a copy device is defined.

To set a quota for a user or group:

1. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window displays. For window details, see section 4.10.4.

2. Use a radio button to select the file system whose quota information you want to set, and then click the **Quota Setup** button.

   The **List of Quota Information** (User) window displays. For window details, see section 4.12.2.

   To set a group quota, select **Group** from the drop-down list, and then click the **Display** button. The **List of Quota Information** (Group) window displays. For window details, see section 4.12.3.

3. Use the check boxes to select one or more users or groups for which a quota is to be set, and then click the **Quota Setup** button.

   The Quota Setup window displays for the selected users or groups. Information about the window's contents is described in Table 4.43.

4. Enter the required information, and then click the **OK** button.

   The quota is set and the **List of Quota Information** (User) window or **List of Quota Information** (Group) window re-displays. If you selected multiple users or groups, the same quota information is set for all of them.

**Table 4.66 Quota Setup Window**

| Item | Description |
|---|---|
| **Block limits** | Specify the block space available to the user(s) or group(s):<br>▪ **Soft limit**<br>Set the soft limit (units: MB). See ***Note.***<br>Specify a value from 0 to 2,097,151. This value must not exceed the **Hard limit** setting. The default is 0 (no soft limit).<br>▪ **Hard limit**<br>Set the hard limit (units: MB). You cannot set a smaller value than already used. Specify a value from 0 to 2,097,151. The default is 0 (no hard limit). See ***Note.*** |
| **i-node limits** | Specify the number of i-nodes available to the user(s) or group(s):<br>▪ **Soft limit**<br>Set the soft limit. See ***Note.***<br>Specify a value from 0 to 2,147,483,647. This value must not exceed the **Hard limit** setting. The default is 0 (no soft limit).<br>▪ **Hard limit**<br>Set the hard limit. You cannot set a smaller value than already used. Specify a value from 0 to |

| Item | Description |
|---|---|
| | 2,147,483,647. The default is 0 (no hard limit). See ***Note.*** |

***Note:*** If you specify one user in the **List of Quota Information** (User) window, or specify one group in the **List of Quota Information** (Group) window, the initial values displayed in **Soft limit** and **Hard limit** vary depending on whether a quota for the selected user or group has been set for a file system.

- When a quota for the selected user or group has been set for the file system:

  The quota that has been set is displayed.

- When a quota for the selected user or group has not been set for the file system:

  If you specify a user, and the default quota has been set for the file system, the default quota is displayed.

  If you specify a user and the default quota has not been set, 0 is displayed.

  If you specify a group, 0 is displayed.

If you specify multiple users or groups, no value is initially displayed.

### 4.12.5 Setting Default Quotas

The system administrator can set the default quota for a file system in the Default Quota Setup window. If a default quota is set for a file system, it is applied when a user for which a quota has not been set uses the file system. This prevents excessive disk space usage when a quota is not set for each user. In the same way as for quota setup for each user or group, specify the block space and the number of i-nodes available.

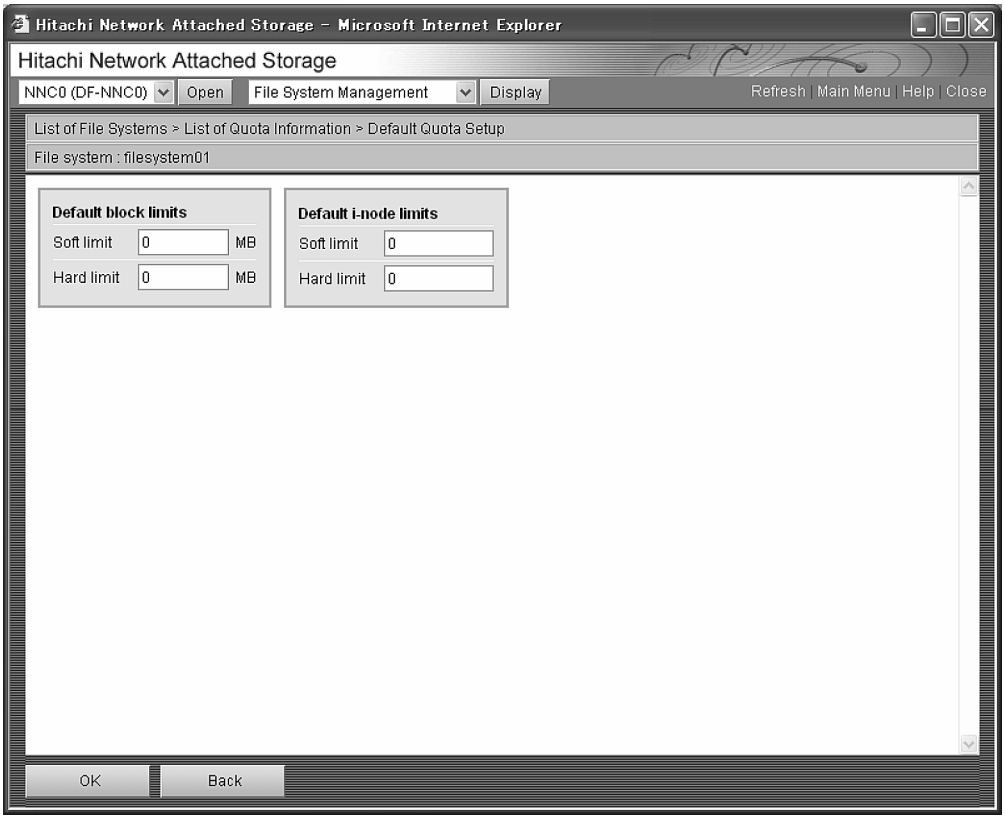



**Figure 4.103 Default Quota Setup Window**

Default quotas cannot be set for the following snapshots:

- Snapshots taken by NAS Backup Restore
- Differential-data snapshots created with NAS Sync Image

While NAS Backup Restore recovers the file system from a snapshot, default quotas cannot be set for file systems for which a copy device is defined.

To set the default quota for a file system:

1. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window appears. For details on this window, see section 4.10.3.

2. Select the radio button of the file system for which you want to set the default quota and click the **Quota Setup** button.

   The **List of Quota Information** (User) window appears. For details on this window, see section 4.12.2.

3. Click the **Default Quota Setup** button.

   The Default Quota Setup window appears.

4. Enter the required information, and then click the **OK** button.

   The default quota is set and the **List of Quota Information** (User) window reappears. In the **List of Quota Information** (User) window, the default quota information is displayed for users for which quota information has not been set.

The following sections describe the information to be specified in the **Default Quota Setup** window.

You can specify the following information in the Default Quota Setup window:

- **Default block limits**

  Use to specify the block space that is available to users.

  - Soft limit:

    Set the soft limit (units: MB). Specify a value from 0 to 2,097,151. This value must not exceed the Hard limit setting.

    The default is 0 (no soft limit).

  - Hard limit:

    Set the hard limit (units: MB). Specify a value from 0 to 2,097,151.

    The default is 0 (no hard limit).

- **Default i-node limits**

  Use to specify the number of i-node available to the users. This setting is applied when a user for which quota has not been set creates a file:

  - Soft limit:

    Set the soft limit. Specify a value from 0 to 2,147,483,647. This value must not exceed the Hard limit setting.

    The default is 0 (no soft limit).

  - Hard limit:

    Set the hard limit. Specify a value from 0 to 2,147,483,647.

    The default is 0 (no hard limit).

### 4.12.6 Setting a Grace Period

In the **Grace Period Setup** window, the system administrator can set a grace period for the quotas for a file system. The grace period applies to all users and groups using the file system.

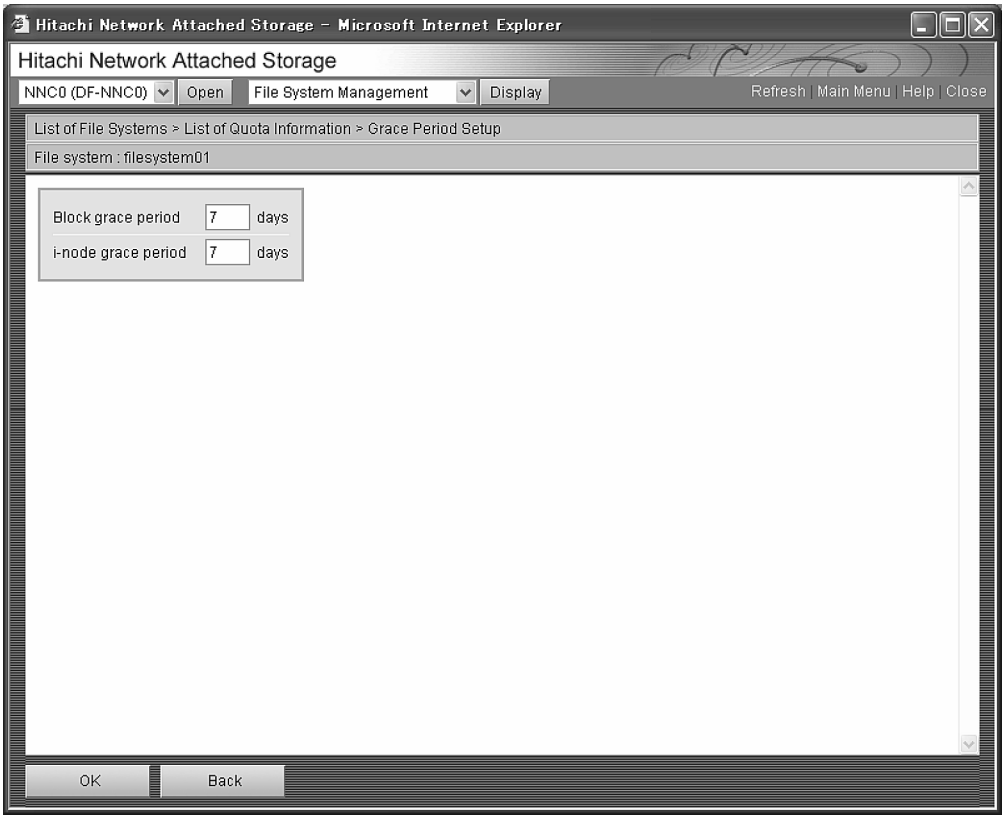



**Figure 4.104 Grace Period Setup Window**

Even if you change the current grace period, the new setting does not apply to the users or groups whose disk usage exceeds the soft limit and who are in the grace period. For example, if you change the grace period to 10 days for a file system used by a user whose remaining grace time is 5 days, the remaining grace time for that user will not change.

To set a grace period for the quotas for a file system:

1. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window displays. For window details, see section 4.10.4.

2. Use a radio button to select the file system for which you want to set a grace period, and then click the **Quota Setup** button.

   The **List of Quota Information** (User) window displays. For window details, see section 4.12.2.

3. Click the **Grace Period Setup** button.

   If the **List of Quota Information** (Group) window is active, click the **Grace Period Setup** button in that window.

The **Grace Period Setup** window displays. Following is information about the window's contents:

- **Block grace period**

  Specify a grace period until files can no longer be created or updated after block usage exceeds the soft limit (units: days). Set a value from 1 to 9,999 (the default is 7).

- **i-node grace period**

  Specify a grace period until files can no longer be created or updated after i-node usage exceeds the soft limit (units: days). Set a value from 1 to 9,999 (the default is 7).

4. Enter the required information, and then click the **OK** button.

   The grace period is set and the **List of Quota Information** (User) window re-displays.

### 4.12.7 Setting Quota Monitoring Times

You can use the **Monitoring Time Setup** window to set times each day at which quota information set for a file system is monitored (quota monitoring times). The system administrator can also use the window to set the SNMP trap notification mode when users or groups that have exceeded the soft limit or grace period for the file system are detected.

To set the monitoring method for quotas set for a file system:

1. In the **Main Menu** window, click the **File System Management** button.

   The **List of File Systems** window displays. For window details, see section 4.10.4.

2. Select the file system for which you want to set quota monitoring times, and then click the **Quota Setup** button.

   The **List of Quota Information** (User) window displays. For window details, see section 4.12.2.

3. Click the **Monitoring Setup** button.

   If the **List of Quota Information** (Group) window is active, click the **Monitoring Setup** button in that window. The **Monitoring Setup** window displays.

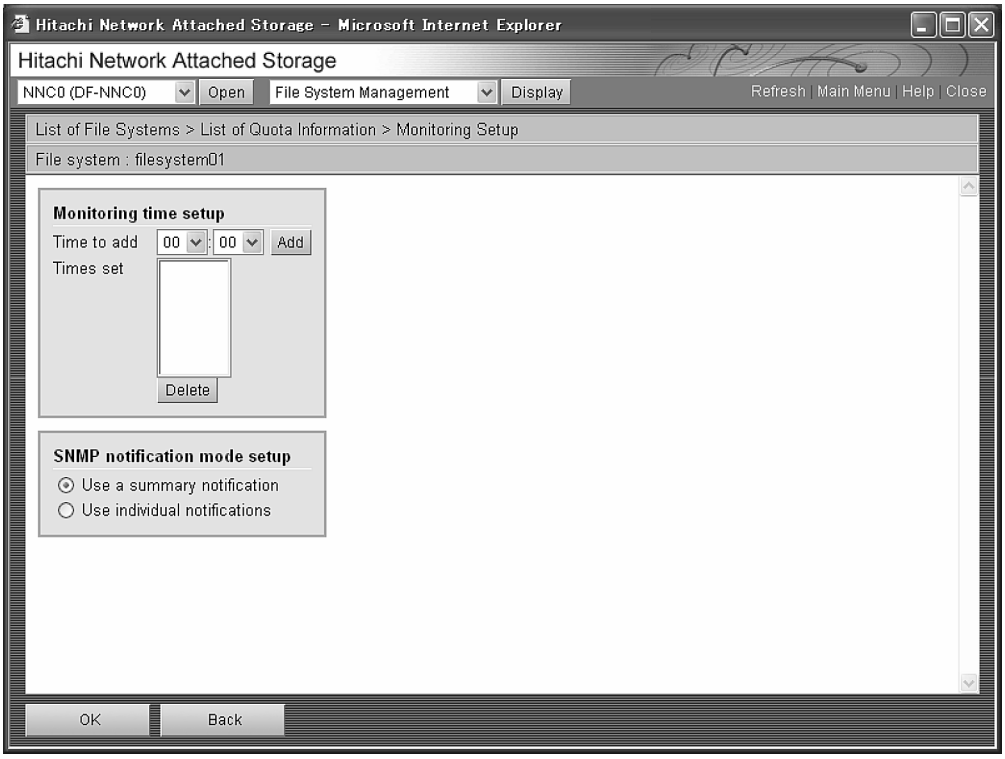



**Figure 4.105 Monitoring Setup Window**

4. Enter the required information, and then click the **OK** button.

   The quota monitoring method is set, and the **List of Quota Information** (User) window or the **List of Quota Information** (Group) window reappears.

   The following table lists and describes the information to be specified in the Monitoring Setup window.

**Table 4.67 Information specified in the Monitoring Setup window**

| Item | Description |
|---|---|
| **Monitoring time setup** | From the **Time to add** drop-down list, select a time at which NAS Manager polls for quota information (by hour and minute).<br>You can specify the time in 5-minute units, in the range from 00:00 to 23:55.<br>Click the **Add** button to add the selected time to the **Times set** list box. Only the times appearing in this list box will be set as quota monitoring times.<br>To delete a time from the list box, select the time and click the **Delete** button.<br>You can set from 0 to 48 daily monitoring times.<br>If omitted, quota monitoring will not be performed. |
| **SNMP notification mode setup** | Use a radio button to select the SNMP trap notification mode when users or groups that have exceeded the soft limit or grace period are detected.<br>**Use a summary notification**<br>Select this item to set summary notification mode.<br>**Use individual notifications**<br>Select this item to set individual notification mode. |

## 4.13 Managing Error Information

You can complete the following tasks to manage error information in the NAS Modular system:

- Investigate and deal with errors as they occur, referring to error information.
- Download error information and contact your HDS representative if a problem cannot be resolved.
- Regularly purge old error information that is no longer required, thereby preventing the NAS OS LU from filling up.

You can use the NAS Manager to display, download, and delete error information. You can download each log file, all the log data, or log files for each log group in a **Batch Operation**. For details on how to download log files in a **Batch Operation**, see section 4.13.10.

The following table lists such error information:

**Table 4.68 Error Information that can be Displayed, Downloaded, and Deleted**

| Type of Information | Description |
|---|---|
| System messages | Important NAS Modular system messages |
| System logs | System logs of the NAS OS |
| **Other logs:** | |
| /var/log/dmesg | Startup messages |
| /var/log/kern.log | Kernel log |
| /var/log/messages | OS messages |
| /var/log/daemon.log | Daemon log |
| /var/log/auth.log | User authentication log |
| /var/log/user.log | User log |
| /var/log/apache/error.log | Web server log |
| /var/log/apache/access.log | Web server log |
| /var/log/lvm | LVM log |
| /var/log/samba/log.smbd | CIFS log |
| /var/log/samba/log.nmbd | CIFS log |
| /var/log/samba/log.winbindd | CIFS log |
| /var/log/failsafe/crsd_*channel-adapter-name* | Cluster log |
| /var/log/failsafe/cmsd_*channel-adapter-name* | Cluster log |
| /var/log/failsafe/failsafe_*channel-adapter-name* | Cluster log |
| /var/log/failsafe/gcd_*channel-adapter-name* | Cluster log |
| **Other logs:** | |

| Type of Information | Description |
|---|---|
| /var/log/failsafe/ifd_*channel-adapter-name* | Cluster log |
| /var/log/failsafe/srmd_*channel-adapter-name* | Cluster log |
| /var/log/failsafe/script_*channel-adapter-name* | Cluster log |
| /var/log/failsafe/cli_*channel-adapter-name* | Cluster log |
| /var/log/failsafe/cmond_*channel-adapter-name* | Cluster log |
| /var/log/failsafe/cdbd_*channel-adapter-name* | Cluster log |
| /var/log/failsafe/clusterinfo.log | Cluster information |
| /enas/log/ebr_alertfile | Backup Restore log<br>See ***Note 1*** |
| /enas/log/backuprestore.trace | Backup Restore trace log<br>See ***Note 1*** |
| /enas/log/ndmpserver.log | NDMP server log<br>See ***Note 1*** |
| /enas/log/ndmptar.log | NDMP archiver log<br>See ***Note 1*** |
| /enas/log/management.log | Management log |
| /enas/log/management.trace | Management trace log |
| /enas/log/antivirus.log | Anti Virus Agent log<br>See ***Note 2*** |
| /enas/log/syncimage.log | Sync Image log<br>See ***Note 3*** |
| /enas/log/syncimage.trace | Sync Image trace log<br>See ***Note 3*** |
| core | Core files for all applications running on the NAS OS and dump files for the NAS OS |

***Note 1:*** Messages are logged to this file only when a license is set for NAS Backup Restore. For details on license setup, see the *Hitachi AMS/WMS Graphical User Interface (GUI) User's Guide* (MK-95DF711) and/or the *Hitachi AMS/WMS Storage Navigator Modular Command Line Interface (CLI)* (MK-95DF712).

***Note 2:*** Messages are logged to this file only when a license is set for NAS Anti Virus Agent. For details on license setup, see the *Hitachi AMS/WMS Storage Navigator Modular Graphical User Interface (GUI) User's Guide* (MK-95DF711) and/or the *Hitachi AMS/WMS Navigator Modular Command Line Interface (CLI)* (MK-95DF712).

***Note 3:*** Messages are logged to this file only when a license is set for NAS Sync Image.

For some types of error information (log files), it is possible to enter system settings about the number of log files to be kept and their size. For details on system settings, see section 4.7.9.

### 4.13.1 Viewing System Messages

*System messages* are important messages regarding effects on the entire NAS Modular system. You can use the **List of RAS Information** (List of Messages) window to view system messages.

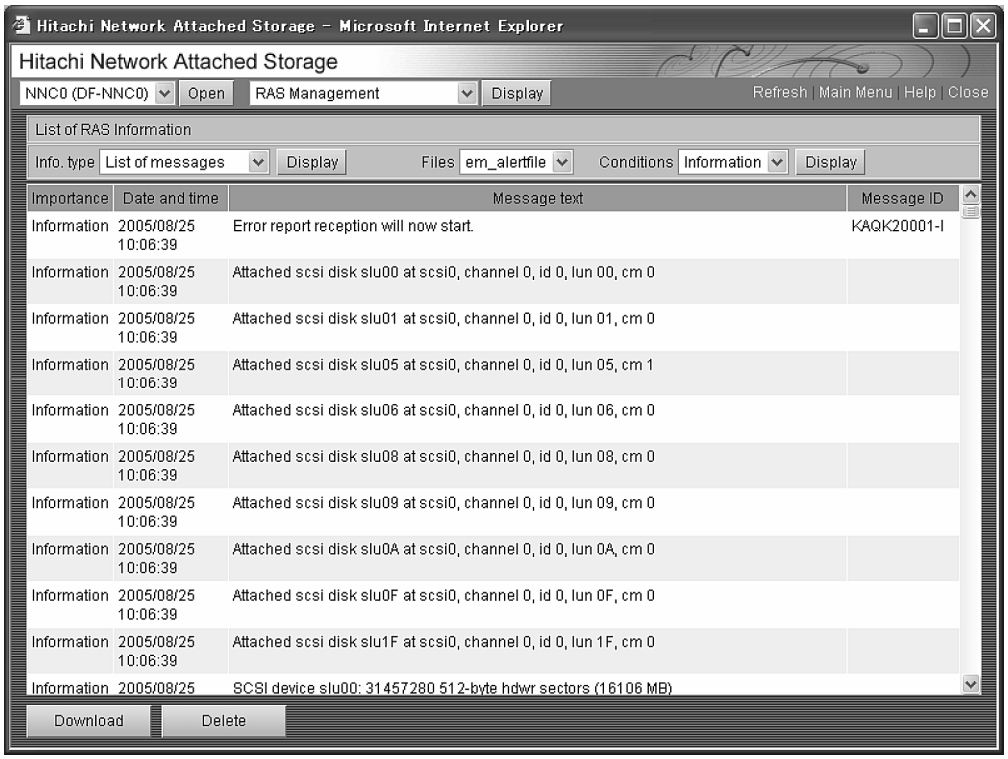



**Figure 4.106 List of RAS Information (List of Messages) Window**

The following table describes the information that is displayed in the window:

**Table 4.69 List of RAS Information (List of Messages) Window**

| Item | Description |
|---|---|
| **Importance** | Message severity level:<br>▪ `Information`<br>The message is at the *Information* level.<br>▪ `Warning`<br>The message is at the *Warning* level.<br>▪ `Error`<br>The message is at the *Error* level.<br>▪ `Fatal error` |

| Item | Description |
|---|---|
| | The message is at the *Fatal error* level. |
| **Date and time** | Date and time at which the message was output. |
| **Message text** | Message text. |
| **Message ID** | Message ID.<br>The message ID takes the following format:<br>KA*X*¹*X*²*Y*¹*Y*²*Y*³*Y*⁴*Y*⁵-*Z*<br>The variable portions indicate the source, type, and severity level of the message.<br>*X*¹*X*²<br>Symbol representing the program that produced the message.<br>The following shows the symbols that may be displayed and what they represent:<br>QB: NAS Backup Restore<br>QG: NAS File Sharing<br>QK: NAS Data Control<br>QM: NAS Manager<br>QS: NAS Sync Image<br>QV: NAS Anti Virus Agent<br>*Y*¹*Y*²*Y*³*Y*⁴*Y*⁵<br>Number representing the message type.<br>*Z*<br>Symbol representing the message severity level.<br>The following shows the symbols that may be displayed and what they represent:<br>E: Error message<br>I: Information message<br>W: Warning message<br>Q: Question message |

To view system messages:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. By default, the most recent messages are listed. When the **List of RAS Information** (List of Messages) window is not displayed, select **List of messages** from the **Info. type** drop-down list, and then click the **Display** button.

2. To view past system messages, select the required file from the **Files** drop-down list, and then click the **Display** button on the right side of the window:

   - **em_alertfile** Select this item to display the most recent system messages file. This item is selected by default.
   - **em_alertfile.***n* Select this item to display a file of past system messages. You can select the saved system message files such as **em_alertfile.1** and **em_alertfile.2**, where *n* indicates the generation number. The higher the number, the older the system messages file. Depending on the system status, **0** may be output for the file suffix *n*.

   A listing of the selected system messages displays.

3. To view messages by message severity level, select a severity level from the **Conditions** drop-down list, and then click the **Display** button:
   - **Information**

     Select to view all messages from information to fatal error messages.
   - **Warning**

     Select to view warning, error, and fatal error messages.
   - **Error**

     Select to view error and fatal error messages.
   - **Fatal error**

     Select to view fatal error messages only.

   Messages with the selected severity level or higher severity level are listed.

### 4.13.2 Downloading System Messages

To download system messages:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1. By default, the most recent messages are listed. When the window is not displayed, select **List of messages** from the **Info. type** drop-down list, and then click the **Display** button.
2. From the **Files** drop-down list, select the system messages file that you want to download, and then click the **Display** button.

   The list of system messages for the selected file is displayed.
3. Click the **Download** button.

   A download window and a Web browser download dialog box displays.
4. In the dialog box, specify where to download the file.

   The displayed system messages file will be downloaded to the specified location.
5. Click the **Close** button in the download window.

   The download window closes.

### 4.13.3 Deleting System Messages

To delete system messages:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1. By default, the most recent messages are listed. When the window is not displayed, select **List of messages** from the **Info. type** drop-down list, and then click the **Display** button.

2. From the **Files** drop-down list, select the system messages file you want to delete, and then click the **Display** button to show the list of selected system messages.
3. Click the **Delete** button.

   A dialog box confirms that you want to delete the system messages file.
4. Click the **OK** button to delete the displayed system messages file.

### 4.13.4 Viewing System Logs

You can use the **List of RAS Information** (List of System Logs) window to view system logs.

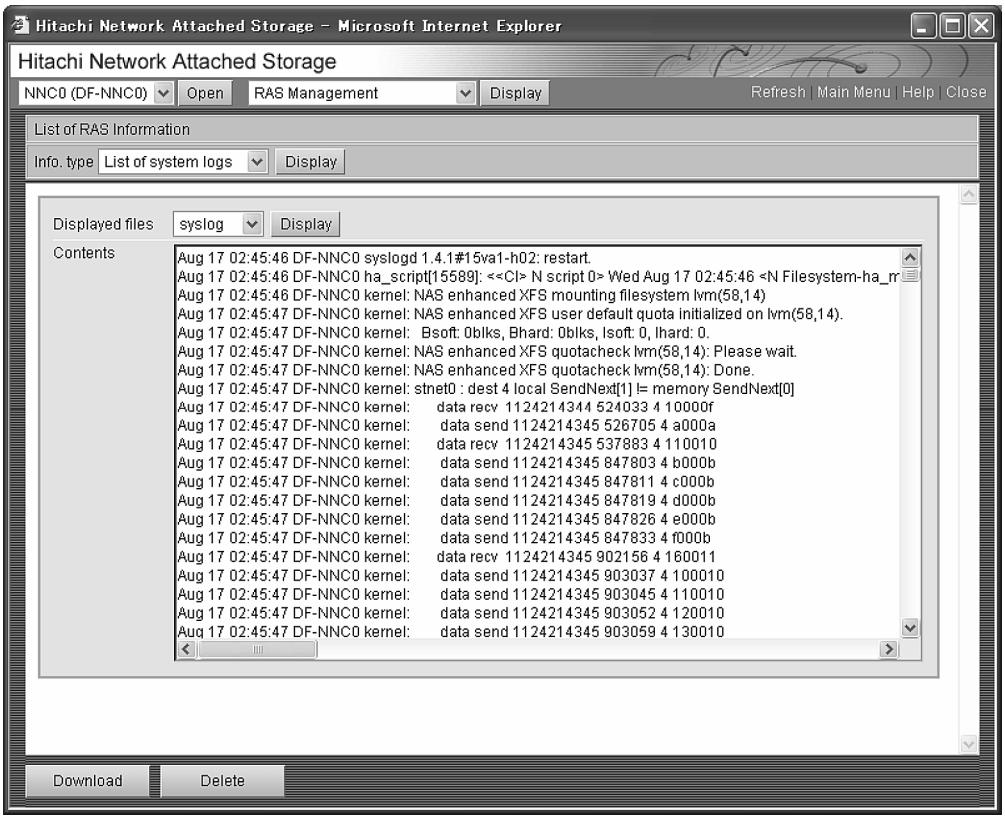



**Figure 4.107 List of RAS Information (List of System Logs) Window**

To view system logs:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1.
2. Select **List of system logs** from the **Info. type** drop-down list, and then click the **Display** button.

   The **List of RAS Information** (List of System Logs) window displays.

3. Select the required file from the **Displayed files** drop-down list, and then click the **Display** button:
   - **syslog**

     Select this item to display the most recent system logs file. This item is selected by default.
   - **syslog.*n***

     Select this item to display a file of past system logs. You can select the saved system log files, such as **syslog.1** and **syslog.2**, where *n* indicates the generation number. The higher the number, the older the system log file. Depending on the system status, **0** may be output for the file suffix *n*.

   The messages in the selected system log are displayed.

### 4.13.5 Downloading a System Log

To download a system log:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1.
2. Select **List of system logs** from the **Info. type** drop-down list, and then click the **Display** button.

   The **List of RAS Information** (List of System Logs) window displays. For window details, see section 4.13.4.
3. From the **Displayed files** drop-down list, select the system log file you want to download, and then click the **Display** button.

   The content of the selected system log file is displayed.
4. Click the **Download** button.

   A download window and a Web browser download dialog box display.
5. In the dialog box, specify where to download the file.

   The system log file being displayed is downloaded to the specified location.
6. Click the **Close** button in the download window.

   The download window closes.

### 4.13.6 Deleting a System Log

To delete a system log:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1.

2. Select **List of system logs** from the **Info. type** drop-down list, and then click the **Display** button.

   The **List of RAS Information** (List of System Logs) window displays. For window details, see section 4.13.4.

3. From the **Displayed files** drop-down list, select the system log file you want to delete, and then click the **Display** button.

   The content of the selected system log file is displayed.

4. Click the **Delete** button.

   A dialog box confirms that you want to delete the system log file.

5. Click the **OK** button.

   The system log file being displayed is deleted.

### 4.13.7 Viewing Other Log File Types

You can use the **List of RAS Information** (List of Other Log Files) window to view log files other than system messages and system logs.

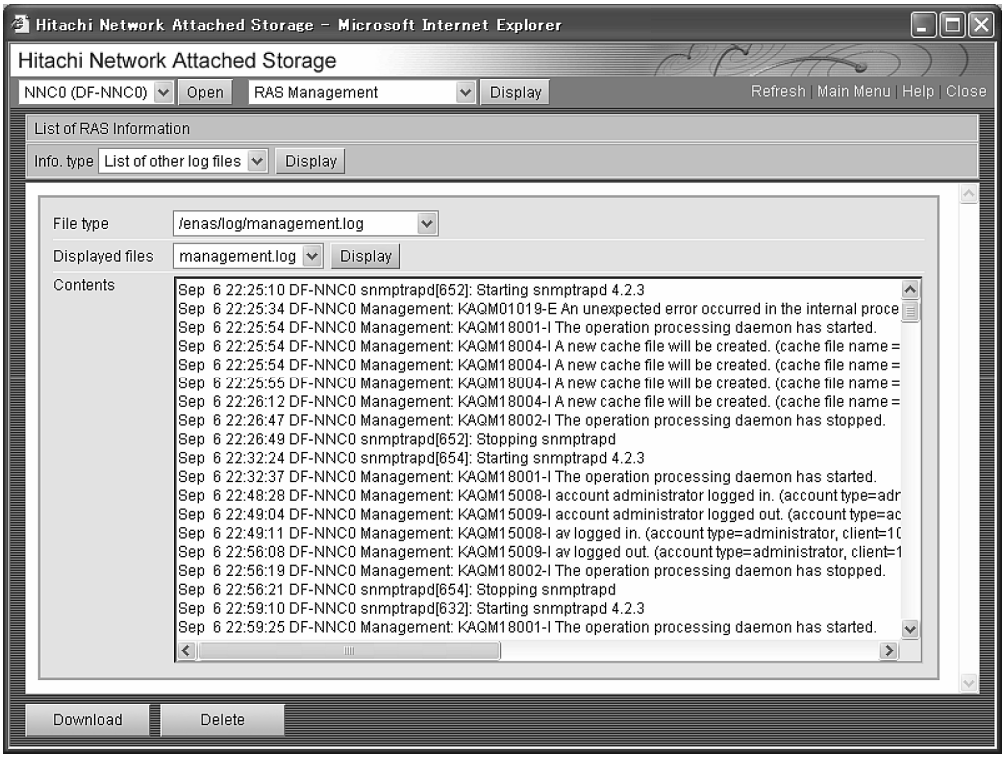



**Figure 4.108 List of RAS Information (List of Other Log Files) Window**

To view log files other than system messages and system logs:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1.

2. Select **List of other log files** from the **Info. type** drop-down list, and then click the **Display** button.

   The **List of RAS Information** (List of Other Log Files) window displays.

3. In the **File type** drop-down list, select the type of log file to be listed (see Table 4.70 after step 4).

   The listing in the **Displayed files** drop-down list is refreshed according to the file type you selected.

4. From the **Displayed files** drop-down list, select the log file to be displayed, and then click the **Display** button:

   - *name-of-selected-type-of-log-file*

     Select this item to display the most recent log file of the type you selected in the **File type** drop-down list. This item is selected by default.

   - *name-of-selected-type-of-log-file*.*n*

     Select this item to display a past log file of the type you selected in the **File type** drop-down list. You can select a saved log file, such as *name-of-selected-type-of-log-file*.**1**, *name-of-selected-type-of-log-file*.**2**, where *n* indicates the generation number. The higher the number, the older the log. Depending on the system status, **0** may be output for the file suffix *n*.

   The messages in the selected log file are displayed.

**Table 4.70 Log File Types in File Type Drop-Down List**

| Log File Type | Displays when Selected |
|---|---|
| /var/log/dmesg | startup messages |
| /var/log/kern.log | kernel log |
| /var/log/messages | OS messages |
| **/var/log/xfs/xfslog** | Select this item to display XFS log. |
| **/var/log/nfs/nfsinform.log** | Select this item to display NFS notification log. |
| /var/log/daemon.log | daemon log |
| /var/log/auth.log | user authentication log |
| /var/log/user.log | user log |
| /var/log/apache/error.log | Web server log |
| /var/log/apache/access.log | Web server log |
| /var/log/lvm | LVM log |
| /var/log/samba/log.smbd | CIFS log |
| /var/log/samba/log.nmbd | CIFS log |

| Log File Type | Displays when Selected |
|---|---|
| /var/log/samba/log.winbindd | CIFS log |
| **/var/log/snmpd.log** | Select this item to display SNMP daemon log. |
| /var/log/failsafe/crsd_NNC-name | cluster log |
| /var/log/failsafe/cmsd_ NNC-name | cluster log |
| /var/log/failsafe/failsafe_ NNC-name | cluster log |
| /var/log/failsafe/gcd_ NNC-name | cluster log |
| /var/log/failsafe/ifd_ NNC-name | cluster log |
| /var/log/failsafe/srmd_ NNC-name | cluster log |
| /var/log/failsafe/script_ NNC-name | cluster log |
| /var/log/failsafe/cli_ NNC-name | cluster log |
| /var/log/failsafe/cmond_ NNC-name | cluster log |
| /var/log/failsafe/cdbd_ NNC-name | cluster log |
| /var/log/failsafe/clusterinfo.log | cluster information |
| /enas/log/ebr_alertfile<br>See ***Note 1*** | Backup Restore log |
| /enas/log/backuprestore.trace<br>See ***Note 1*** | Backup Restore trace log |
| /enas/log/ndmpserver.log<br>See ***Note 1*** | NDMP server log |
| /enas/log/ndmptar.log<br>See ***Note 1*** | NDMP archiver log |
| /enas/log/management.log | Management log |
| /enas/log/management.trace | Management trace log |
| /enas/log/antivirus.log<br>See ***Note 2*** | Anti-Virus Agent log |
| /enas/log/syncimage.log<br>See ***Note 3*** | Sync Image log |
| /enas/log/syncimage.trace<br>See ***Note 3*** | Sync Image trace log |

***Note 1:*** Log information is written to this file only when a license is set for NAS Backup Restore. For details on license setup, see the *Hitachi AMS/WMS Storage Navigator Modular Graphical User Interface (GUI) User's Guide* (MK-95DF711) and/or the *Hitachi AMS/WMS Storage Navigator Modular Command Line Interface (CLI)* (MK-95DF712).

***Note 2:*** Log information is written to this file only when a license is set for NAS Anti Virus Agent. For details on license setup, see the *Storage Navigator Modular User's Guide*.

***Note 3:*** Log information is written to this file only when a license is set for NAS Sync Image.

### 4.13.8 Downloading Other Log File Types

To download log files other than system messages and system logs:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1.

2. From the **Info. type** drop-down list, select **List of other log files**, and then click the **Display** button.

   The **List of RAS Information** (List of Other Log Files) window displays. For window details, see section 4.13.7.

3. From the **File type** drop-down list, select the type of log file you want to download.

   The listing in the **Displayed files** drop-down list is refreshed according to the file type you selected.

4. From the **Displayed files** drop-down list, select the log file you want to download, and then click the **Display** button.

   The content of the selected log file is displayed.

5. Click the **Download** button.

   A download window and a Web browser download dialog box display.

6. In the dialog box, specify where to download the file.

   The log file being displayed is downloaded to the specified location.

7. Click the **Close** button in the download window.

   The download window closes.

### 4.13.9 Deleting Other Log File Types

To delete log files other than system messages and system logs:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1.

2. From the **Info. type** drop-down list, select **List of other log files**, and then click the **Display** button.

   The **List of RAS Information** (List of Other Log Files) window displays. For window details, see section 4.13.7.

3. From the **File type** drop-down list, select the type of the log files you want to delete.

   The listing in the **Displayed files** drop-down list is refreshed according to the file type you selected.

4. From the **Displayed files** drop-down list, select the log file you want to delete, and then click the **Display** button.

   The content of the selected log file is displayed.

5. Click the **Delete** button.

   A dialog box confirms that you want to delete the log file.

6. Click the **OK** button.

   The log file being displayed is deleted.

### 4.13.10 Downloading Log Files in a Batch Operation

To discover the cause of an error in a NAS Modular system, more than one log file may be required. In the **List of RAS Information** (Batch-download) window, you can download log files (system messages, system logs, and other log files) necessary for error analysis in units of log groups according to the error location.

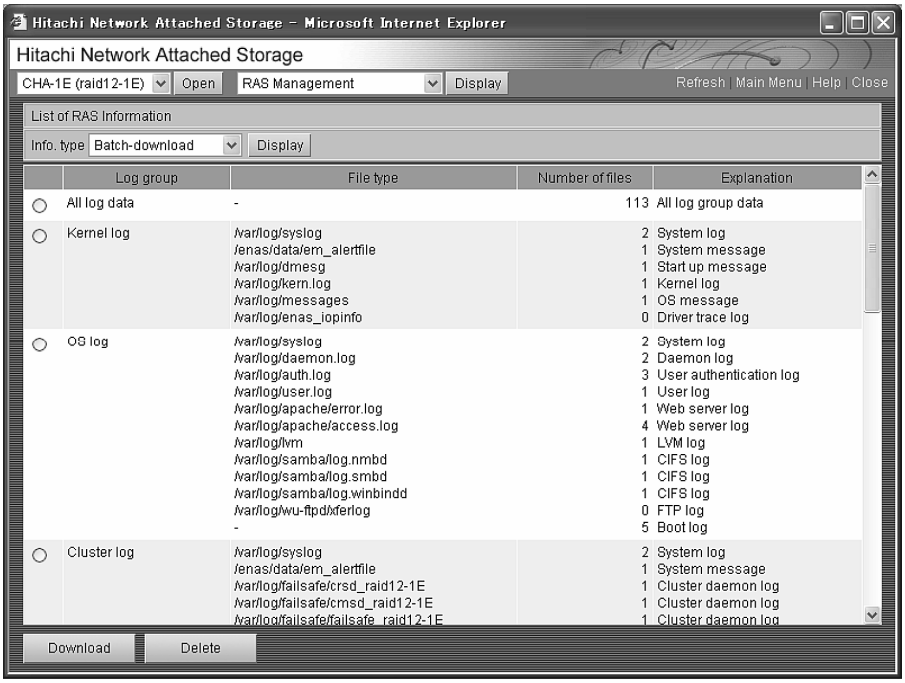



**Figure 4.109 List of RAS Information (Batch-Download) Window**

You can also delete log files for each log group in batches (see section 4.13.11). The following table lists log groups:

**Table 4.71 List of Log Groups**

| Log Group | File Type | Description |
|---|---|---|
| All log data<br>See ***Note 1*** | — | All log group data (except the log group *user mapping information* and *System activity data*) |
| Kernel log | /var/log/syslog | System log |
| | /enas/data/em_alertfile | System messages |
| | /var/log/dmesg | Startup messages |

| Log Group | File Type | Description |
|---|---|---|
| | /var/log/kern.log | Kernel log |
| | /var/log/messages | OS messages |
| | /var/log/xfs/xfslog | XFS log |
| | /var/log/xfs/xfsclilog | XFS command log |
| | /var/log/nfs/nfsinform.log | NFS notification log |
| | /var/log/enas_iopinfo | Driver internal information |
| OS log | /var/log/syslog | System log |
| | /var/log/daemon.log | Daemon log |
| OS log | /var/log/auth.log | User authentication log |
| | /var/log/user.log | User log |
| | /var/log/apache/access.log | Web server log |
| | /var/log/apache/error.log | Web server log |
| | /var/log/lvm | LVM log |
| | /var/log/samba/log.nmbd | CIFS log |
| | /var/log/samba/log.smbd | CIFS log |
| | /var/log/wu-ftpd/xferlog | FTP log |
| | /var/log/snmpd.log | SNMP daemon log |
| | - | Other OS log |
| Cluster log | /var/log/syslog | System log |
| | /enas/data/em_alertfile | System messages |
| | /var/log/failsafe/clusterinfo.log | Cluster information |
| | /var/log/failsafe/crsd_ *NNC-name* | Cluster log |
| | /var/log/failsafe/cmsd_ *NNC-name* | Cluster log |
| | /var/log/failsafe/failsafe__ *NNC-name* | Cluster log |
| | /var/log/failsafe/gcd_ *NNC-name* | Cluster log |
| | /var/log/failsafe/ifd_ *NNC-name* | Cluster log |
| | /var/log/failsafe/srmd_ *NNC-name* | Cluster log |
| | /var/log/failsafe/script_ *NNC-name* | Cluster log |
| | /var/log/failsafe/cli_ *NNC-name* | Cluster log |
| | /var/log/failsafe/cmond_ *NNC-name* | Cluster log |
| | /var/log/failsafe/cdbd_ *NNC-name* | Cluster log |
| Management log | /var/log/syslog | System log |
| | /enas/data/em_alertfile | System messages |
| | /enas/log/management.log | Management log |

| Log Group | File Type | Description |
|---|---|---|
| | /enas/log/management.trace | Management trace log |
| | /enas/log/clusterconf.log | Cluster definition information file |
| Anti Virus Agent log<br>See ***Note 2*** | /var/log/syslog | System log |
| | /enas/data/em_alertfile | System messages |
| | /enas/log/antivirus.log | Anti Virus Agent log |
| Anti Virus Agent log<br>See ***Note 2*** | /enas/log/antiviruslib.trace | Anti Virus Agent library trace log |
| | /enas/log/antivirusgui.trace | Anti Virus Agent GUI operation log |
| Backup Restore log | /var/log/syslog | System log |
| | /enas/data/em_alertfile | System messages |
| Backup Restore log<br>(continued)<br>See ***Note 3*** | /var/log/kern.log | Kernel log |
| | /var/log/messages | OS messages |
| | /var/log/lvm | LVM log |
| | /enas/log/management.log | Management log |
| | /enas/log/management.trace | Management trace log |
| | /enas/data/em_alertfile | System messages |
| | /enas/log/ebr_alertfile | Backup Restore log |
| | /enas/log/backuprestore.trace | Backup Restore trace log |
| | /enas/log/syncimage.log | Sync Image log |
| | /enas/log/syncimage.trace | Sync Image trace log |
| | /enas/log/ndmpserver.log | NDMP server log |
| | /enas/log/ndmptar.log | NDMP archiver log |
| | — | Remote Copy log |
| Sync Image log<br>See ***Note 4*** | /var/log/syslog | System log |
| | /enas/data/em_alertfile | System messages |
| | /var/log/kern.log | Kernel log |
| | /var/log/messages | OS messages |
| | /var/log/lvm | LVM log |
| | /enas/log/management.log | Management log |
| | /enas/log/management.trace | Management trace log |
| | /enas/log/ebr_alertfile | Backup Restore log<br>See ***Note 3*** |
| | /enas/log/backuprestore.trace | Backup Restore trace log<br>See ***Note 3*** |
| | /enas/log/syncimage.log | Sync Image log |

| Log Group | File Type | Description |
|---|---|---|
| | /enas/log/syncimage.trace | Sync Image trace log |
| Driver status<br>See ***Note 1*** | — | Various configuration information about driver status |
| LVM status[#1] | /var/log/syslog | System log |
| | /var/log/kern.log | Kernel log |
| | /var/log/user.log | User log |
| | /var/log/lvm | LVM log |
| | - | LVM status |
| Program info.<br>See ***Note 1*** | — | Installation information |
| NFS status<br>See ***Note 1*** | /var/log/syslog | System log |
| | /var/log/daemon.log | Daemon log |
| | /var/log/kern.log | Kernel log |
| | /var/log/messages | OS messages |
| | /var/log/nfs/nfsinform.log | NFS notification log |
| NFS status<br>(continued)<br>See ***Note 1*** | — | Various configuration information about NFS status |
| Setting file<br>See ***Note 1*** | — | Information on various configuration files |
| Network Info<br>See ***Note 1*** and ***4*** | — | Network information |
| User mapping information<br>See ***Note 5*** | /var/log/samba/userlist.csv | User information (using LDAP) |
| | /var/log/samba/grouplist.csv | Group information (using LDAP) |
| | /var/log/samba/idmap.ldif | LDIF information (LDAP) |
| System activity data<br>See ***Note 1*** | — | System activity data |

***Note 1:*** Can be batch downloaded only; cannot be deleted.

***Note 2:*** This information is displayed only when a license is set for NAS Anti Virus Agent. For details on license setup, see the *Storage Navigator Modular User's Guide*.

***Note 3:*** This information is displayed only when a license is set for NAS Backup Restore. For details on license setup, see the *Storage Navigator Modular User's Guide*.

***Note 4:*** This information is used to check the routing order and the connection between the NAS Unit and an external server. For details on the output contents of the network information, see Appendix D.

***Note 5:*** When user mapping using LDAP is not used, or when user mapping using LDAP is used but the CIFS service is inactive, a 0-byte file is archived and downloaded.

Batch download and batch deletion downloads and deletes the log files of all generations of files in the selected log group. To download system message files, system log files, and other log files in a **Batch Operation**:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1.

2. From the **Info. type** drop-down list, select **Batch-download**, and then click the **Display** button:

   - **Log group**

     Names of log groups.

   - **File type**

     Type of log files that belong to the log group.

   - **Number of files**

     Total number of log files currently saved in the NAS OS LU (the total number of the most recent and past log files).

   - **Explanation**

     Explanation of the log file.

   The **List of RAS Information** (Batch-download) window displays.

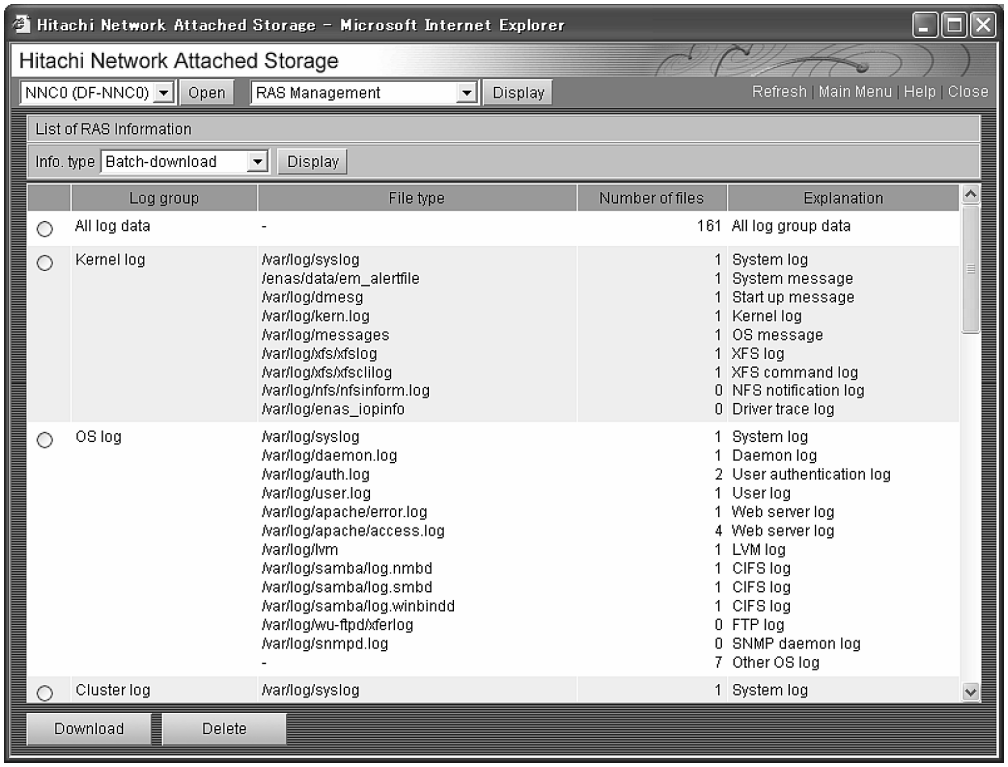



**Figure 4.110 List of RAS Information (Batch-download Window)**

3. Use a radio button to select the log group you want to download, and then click the **Download** button.

   A download window and a Web browser download dialog box display.

4. In the dialog box specify where to download the file.

   The log files that belong to the selected log group are archived by `tar` and compressed by `gzip`, and downloaded to the specified destination.

5. Click the **Close** button in the download window.

   The download window closes.

## 4.13.11 Deleting Log Files in a Batch Operation

To delete system message files, system log files, and other log files in a **Batch Operation**:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1.

2. From the **Info. type** drop-down list, select **Batch-download**, and then click the **Display** button.

   The **List of RAS Information** (Batch-download) window displays. For window details, see section 4.13.10.

3. Use a radio button to select the log group of the files you want to delete in a **Batch Operation**, and then click the **Delete** button.

A dialog box confirms that you want to delete the log group.

4. Click the **OK** button.

   All the log files that belong to the selected log group are deleted.

## 4.14 Managing Core Files

This section describes how you can use the **List of RAS Information** (List of Core Files) window to list core files and download or delete a core file.

### 4.14.1 Viewing a List of Core Files

You can use the **List of RAS Information** (List of Core Files) window to list core files.

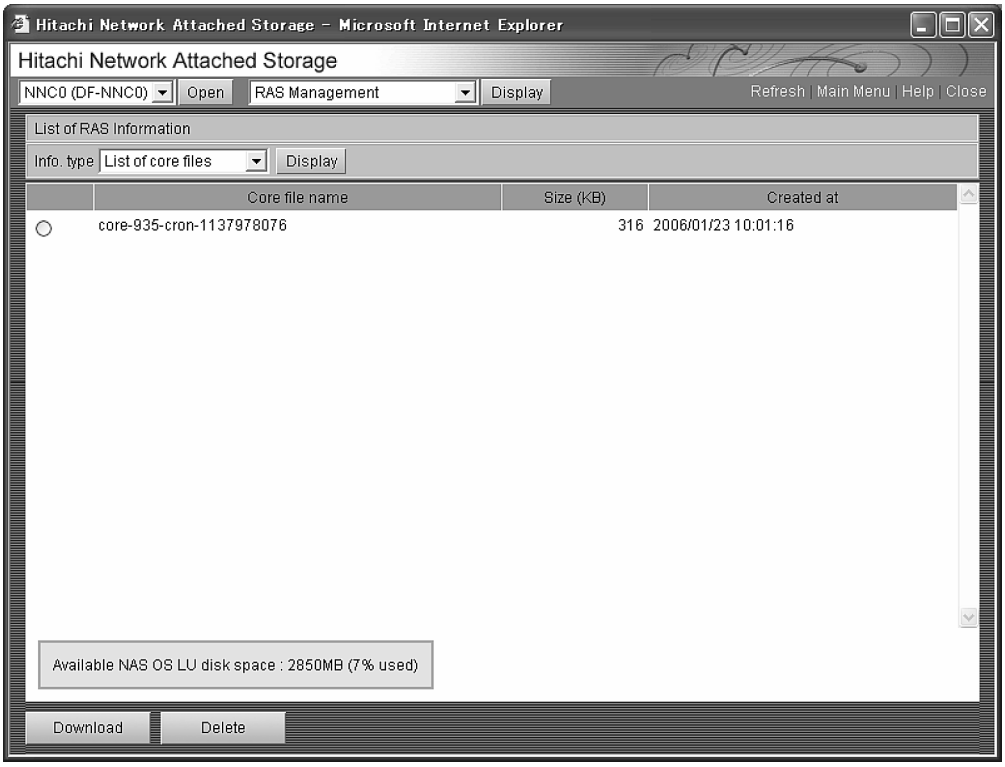



**Figure 4.111 List of RAS Information (List of Core Files) Window**

The following table describes the information that is displayed in the window:

**Table 4.72 Contents of List of RAS Information (List of Core Files) Window**

| Item | Description |
|---|---|
| **Core file name** | Name of the core file. |
| **Size (KB)** | Size of the core file. |
| **Created at** | Date and time at which the core file was output. |
| **Available NAS OS LU disk space** | Amount of free space (units: MB) and used space (units: %) in the NAS OS LU.<br>If the NAS OS LU has little free space, delete unneeded old core files and downloaded core files. |

***Note:*** If dump files are output, dump files, along with core files, are listed. Since only one generation of a dump file is stored in the space other than the space containing core files in the NAS OS LU, you do not need to delete this file for space management.

A dump file is required only when the vendor requests you to collect dump files. In such a case, download dump files and then contact maintenance personnel.

Dump files range from level 1 to level 4. The names of dump files contain a string such as the following:

`lv`*dump-file-level (1 to 4)*

Maintenance personnel can obtain level 1 and level 2 files, but cannot obtain level 3 or level 4 files because they contain access data for the file system (NFS services and CIFS services). Level 1 and level 2 files can be obtained by your HDS representative. Level 3 and level 4 files cannot be obtained by your HDS representative since they contain access data for the file system (NFS services and CIFS services). Depending upon the error level, you may be asked by your HDS representative to collect dump files, but since level 3 and level 4 dump files contain user information, be especially careful when managing these files.

To list core files:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1.

2. Select **List of core files** from the **Info. type** drop-down list, and then click the **Display** button.

   The **List of RAS Information** (List of Core Files) window displays.

### 4.14.2 Downloading a Core File

To download a core file:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1.

2. Select **List of core files** from the **Info. type** drop-down list, and then click the **Display** button.

   The **List of RAS Information** (List of Core Files) window displays. For window details, see section 4.14.

3. Use a radio button to select the file to be downloaded, and then click the **Download** button.

   A download window and a Web browser download dialog box display.

4. In the dialog box, specify where to download the file.

   The selected file is downloaded to the specified location.

5. Click the **Close** button in the download window.

   The download window closes.

### 4.14.3 Deleting a Core File

The system automatically deletes core files that exceed the set storage period. Therefore, periodically check whether a new core file has been created so that core files necessary for troubleshooting will not be deleted automatically. If a core file has been created, download it and send it to your HDS representative. Manually delete downloaded core files to increase the amount of free space in the NAS OS LU. For details on how to set a storage period for core files, see section 4.7.10.

To manually delete a core file:

1. In the **Main Menu** window, click the **RAS Management** button.

   The **List of RAS Information** (List of Messages) window displays. For window details, see section 4.13.1.

2. Select **List of core files** from the **Info. type** drop-down list, and then click the **Display** button.

   The **List of RAS Information** (List of Core Files) window displays. For window details, see section 4.14.

3. Use a radio button to select the file you want to delete, and then click the **Delete** button.

   A dialog box confirms that you want to delete the file.

4. Click the **OK** button.

   The selected file is deleted.

## 4.15 Managing Programs

NAS Manager provides a GUI from which you can install or uninstall programs that run on NAS Units, or can view the version, license, and other information about the installed programs.

You can use the NAS Manager to manage installation and set up licenses for the programs that run on a NAS Unit, by completing the following tasks:

- Viewing and verifying version and license information about the installed programs
- Performs an upgrade installation of a program version, or additionally installs optional programs.
- Uninstalling programs no longer needed

This section describes the tasks for managing the programs that run on NAS Units.

Before these programs are used, license must be set up from the Storage Navigator Modular. For more information, see the *Storage Navigator Modular User's Guide*.

### 4.15.1 Viewing Program Information

You can use the **List of Programs** window to view information about the programs installed on each NAS Unit.

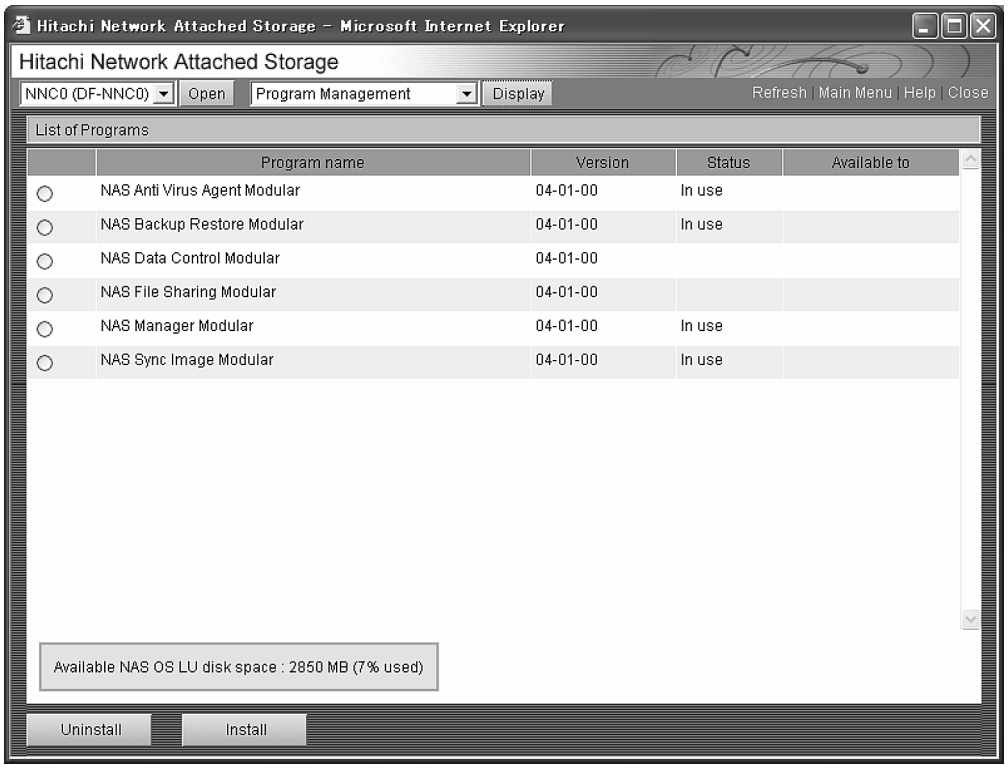



**Figure 4.112 List of Programs Window**

The following table describes the information that is displayed in the window:

**Table 4.73 Contents of List of Programs Window**

| Item | Description |
|---|---|
| **Program name** | Name of an installed program. The individually provided program is listed under the original program. |
| **Version** | Version of the installed program. A hyphen (–) is displayed for patch-version programs. For an individually provided program, a hyphen (–) is displayed. |
| **Status** | Availability of programs (other than NAS Data Control and NAS File Sharing):<br>▪ `In use`<br>The program is available.<br>▪ `Not used`<br>The program is unavailable.<br>To make a program other than NAS Data Control or NAS File Sharing available, a license must be set up. A license can be set up from Storage Navigator Modular. For more information, see the *Storage Navigator Modular User's Guide*. |
| **Available to** | A program for which the validity period of the license is set has the license expiration date displayed. For details on licenses, see the *Storage Navigator Modular User's Guide*. |

To view program information for a NAS Unit, click the **Program Management** button from the **Main Menu** window.

The **List of Programs** window displays.

### 4.15.2 Installing and Uninstalling Programs

You can use the **List of Programs** window to upgrade programs installed on a NAS OS LU for each NAS Unit. You cannot uninstall required programs and patch versions.

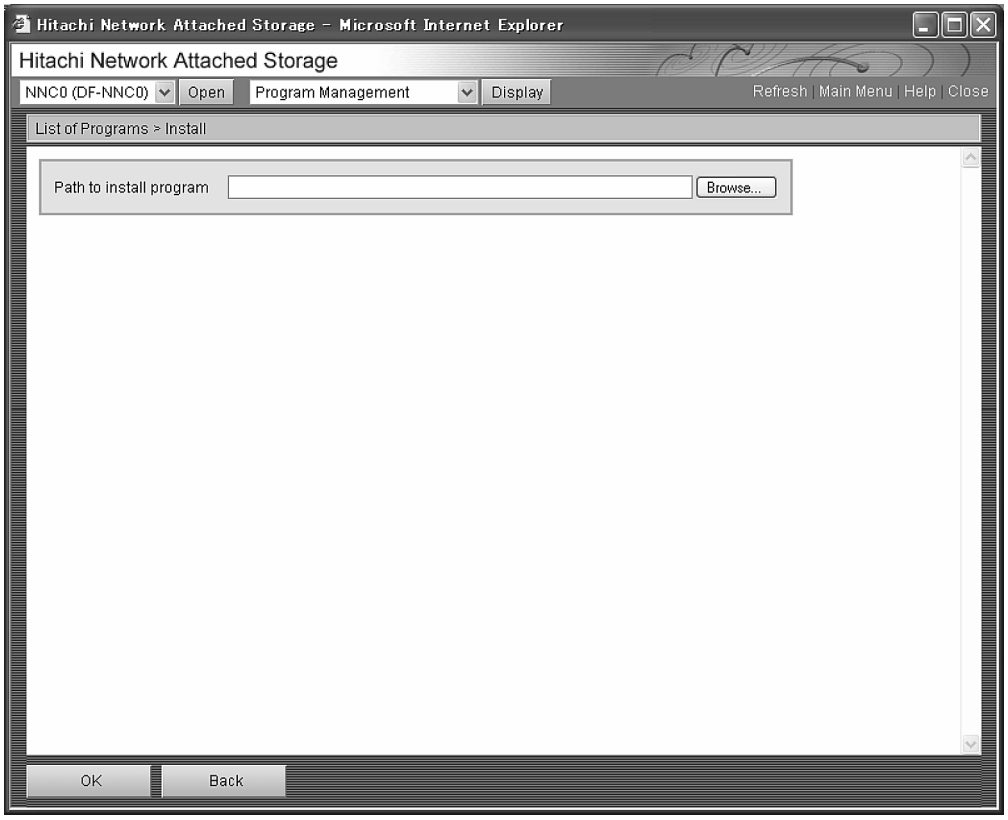



**Figure 4.113 Install Window**

**Before You Install or Uninstall Programs**

In a NAS Modular system, the configurations of programs installed in NAS Units in a cluster must be consistent. You must always control the configurations and versions of programs that have been installed in NAS Units in the same cluster, in order to maintain consistency.

To install a program on a NAS OS LU:

1. Log in to NAS Manager.
2. Load the CD-ROM.
3. In the **Main Menu** window, click the **Program Management** button.

   The **List of Programs** window displays. For window details, see section 4.15.1.
4. Click the **Install** button.

   The Install window displays.
5. In **Path to install program**, specify the path of the program package to be installed.

   To navigate to the file in order to specify the file name, click the **Browse** button.

   Following are the file names of the program packages that are specified for each program to be installed:

   – NAS Manager:

     `NAS_Manager_Modular_`*version-number*`.deb`

- NAS Anti Virus Agent:

  `NAS_Anti_Virus_Agent_Modular_`*version-number*`.deb`

- NAS Backup Restore:

  `NAS_Backup_Restore_Modular` *version-number*`.deb`

- NAS Sync Image:

  `NAS_Sync_Image_Modular_`*version-number*`.deb`

6. Click the **OK** button.

   The installation data is uploaded to the NAS OS LU and a window for confirming the installation displays.

To uninstall a program installed on a NAS OS LU:

1. In the **Main Menu** window, click the **Program Management** button.

   The **List of Programs** window displays. For window details, see section 4.15.1.

2. Select the program to be uninstalled, and then click the **Uninstall** button.

   A dialog box confirms that you want to uninstall the program.

3. Click the **OK** button.

   The selected program is uninstalled.

## 4.16 Modifying a System Administrator's Personal Information

As a system administrator who logs in to NAS Manager and operates and manages a NAS Modular system, you can edit your user name, comment, and password. For increased security, you should regularly change your password.

This section describes how you can view or edit your own user information, and change your password.

### 4.16.1 Viewing a System Administrator's Personal Information

You can use the **Personal Info. Setup** window to view your own information.

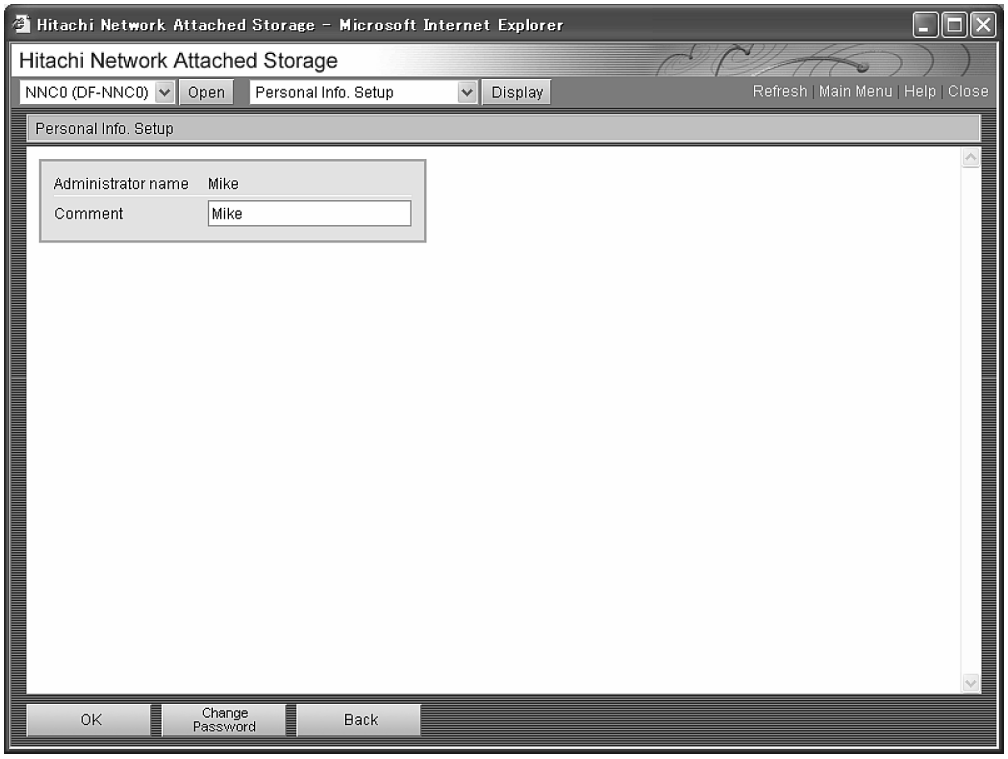



**Figure 4.114 Personal Info. Setup Window**

The following list describes information displayed in the window:

- **Administrator name** User name of the system administrator.
- **Comment** Note for the system administrator. Nothing is displayed unless a comment has been set.

To view user information for the logged-in system administrator, click the **Personal Info. Setup** button from the **Main Menu** window. The **Personal Info. Setup** window displays.

### 4.16.2 Editing a System Administrator's Personal Information

You can use the **Personal Info. Setup** window to change your own user information.

To change user information about a system administrator:

1. In the **Main Menu** window, click the **Personal Info. Setup** button.

   The **Personal Info. Setup** window displays. For window details, see section 4.16.1.

2. Edit your user information.

   As user information, you can edit **Comment**.

Enter a maximum of 32 characters.

You can use any alphanumeric character, number sign (#), percent sign (%), ampersand (&), apostrophe ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), hyphen (-), period (.), forward slash (/), semicolon (;), left angle bracket (<), right angle bracket (>), question mark (?), at mark (@), left bracket ([), right bracket (]), circumflex (^), underscore (_), left brace ({), vertical bar (|), right brace (}), and tilde (~). You can also specify spaces, but spaces cannot be specified at the beginning or at the end of the character string.

This item is optional.

3. Click the **OK** button.

   The user information of the system administrator changes, and the **Main Menu** window re-displays.

### 4.16.3 Changing the System Administrator's Password

You can use the **Change Password** window to change your own password.

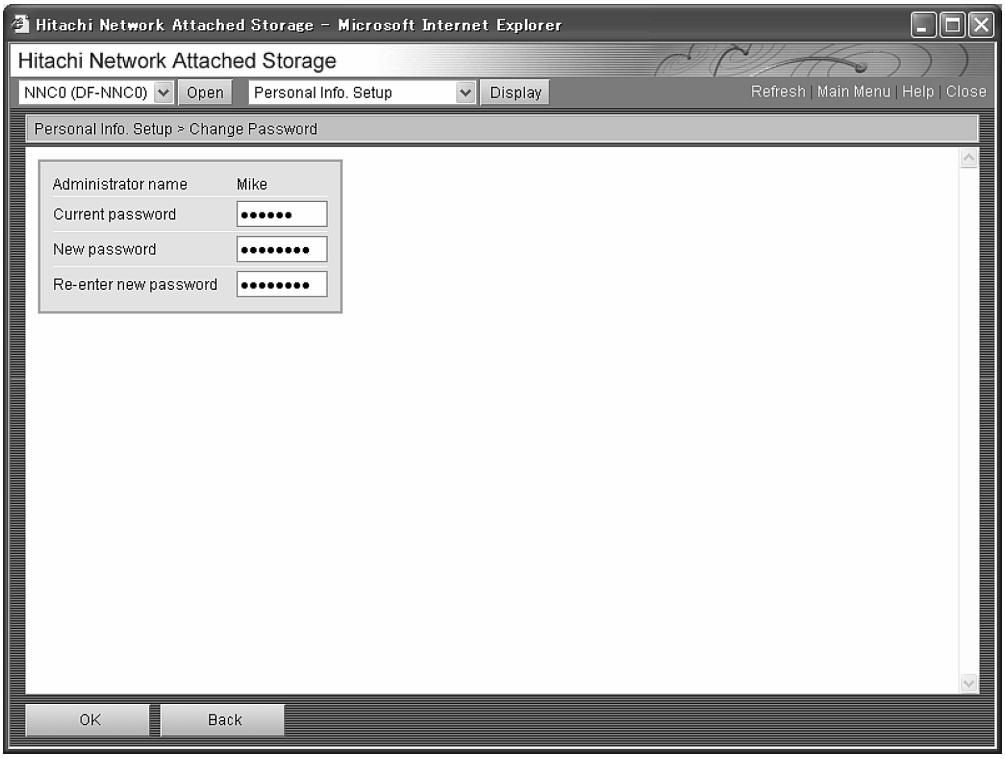



**Figure 4.115 Change Password Window**

To change the password of a system administrator:

1. In the **Main Menu** window, click the **Personal Info. Setup** button.

   The **Personal Info. Setup** window displays. For window details, see section 4.16.1.

2. Click the **Change Password** button.

   The **Change Password** window displays.

3. Enter the required information, and then click the **OK** button.

   The system administrator's password is changed and the **Personal Info. Setup** window re-displays. The following table describes the window's contents:

**Table 4.74 Information Specified in Change Password Window**

| Item | Description |
|---|---|
| **Current password** | Enter the password you are currently using. |
| **New password** | Enter the new password. Specify from 6 to 8 (inclusive) characters.<br>You can use any alphanumeric character, exclamation mark ( ! ), quote ( " ), number sign (#), dollar sign ($), percent sign (%), ampersand (&), apostrophe ( ' ), left parenthesis ( ( ), right parenthesis ( ) ), asterisk (*), plus sign (+), comma ( , ), hyphen (−), period ( . ), forward slash (/), colon ( : ), semicolon ( ; ), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left bracket ( [ ), backslash (\), right bracket ( ] ), circumflex (^), underscore (_), grave accent ( ` ), left brace ( { ), vertical bar ( \| ), right brace ( } ), and tilde (~). |
| **Re-enter new password** | Re-enter the password that you specified in **New password**. |

## 4.17 Saving NAS System LUs

NAS Manager allows you to save NAS system LUs (NAS OS LUs and NAS Cluster Management LU) when either an NFS share service or CIFS share service is available. You must save NAS system LUs after setting the information required for starting a NAS Modular system, such as defining the cluster configuration and creating file systems. When an error occurs in the NAS system LU, contact your HDS representative, then restore a NAS system LU from the backup data.

Two methods for saving NAS system LUs are available:

- **Periodic**

  Use to specify an interval for automatically saving a NAS system LU on a NAS Unit basis.

- **Manual**

  Use whenever setting information for the NAS Modular system changes.

  ***Note:*** If you do not always save the latest data from the NAS system LUs, you may not be able to properly restore a NAS system LU after a failure has occurred.

### 4.17.1 When to Save NAS System LUs

You must save NAS system LUs after setting the information required for starting a NAS Modular system, such as defining the cluster configuration and creating file systems.

NAS system LUs should also be saved manually whenever settings information for the NAS Modular system changes. If you do not always save the latest data from the NAS system LUs, you may not be able to properly restore a NAS system LU after a failure has occurred.

For details on the operations that require NAS system LUs to be saved, see C. Operations that Require NAS System LUs To Be Saved.

### 4.17.2 Saving NAS OS LUs

Use the **Save NAS OS LU** window to enable or disable periodic saving of NAS OS LUs for each NAS Unit and to manually **Save NAS OS LU**s. Also, you can specify an interval for periodic saving of NAS OS LUs on a NAS Unit basis in the **Schedule Settings for NAS OS LU** window.

Only one generation of backup data from a NAS OS LU is available. When you save a NAS OS LU that has already been saved, the previous backup data is discarded.

When a heavy load is being imposed on a NAS Modular system, saving a NAS OS LU might automatically stop due to a timeout to reduce the load. If this happens, wait until the heavy has decreased and run the save operation again for the NAS OS LU.

#### 4.17.2.1 Saving a NAS OS LU Manually

You can use the **Save NAS OS LU** window to manually save a NAS OS LU at any time.

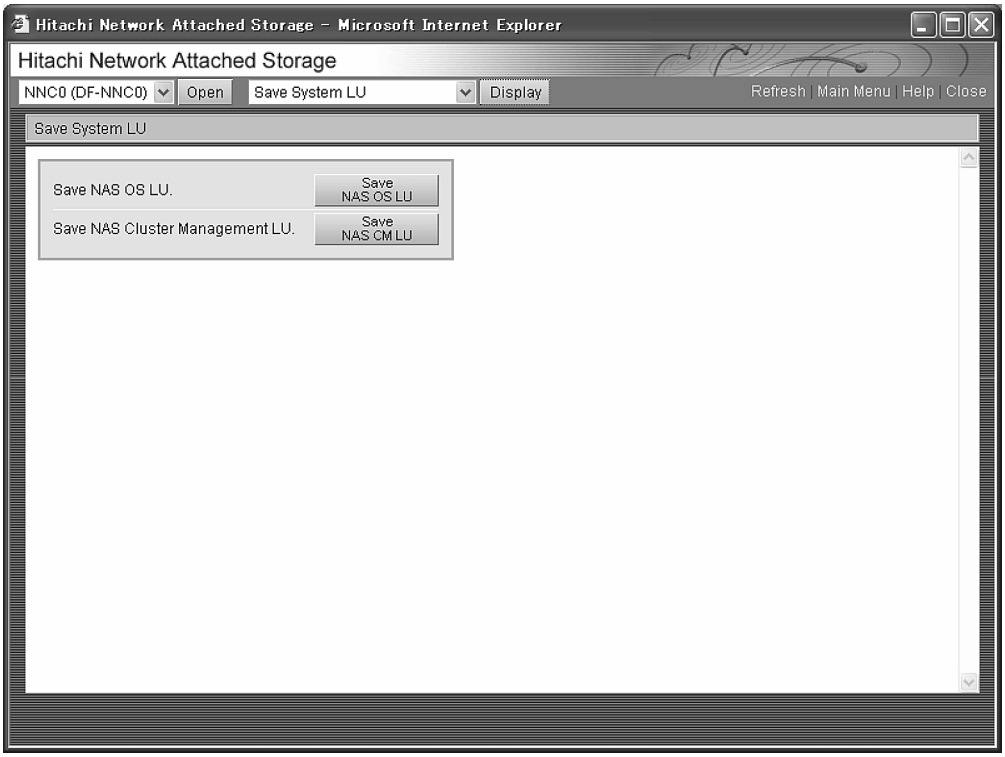



**Figure 4.116 Save System LU Window**

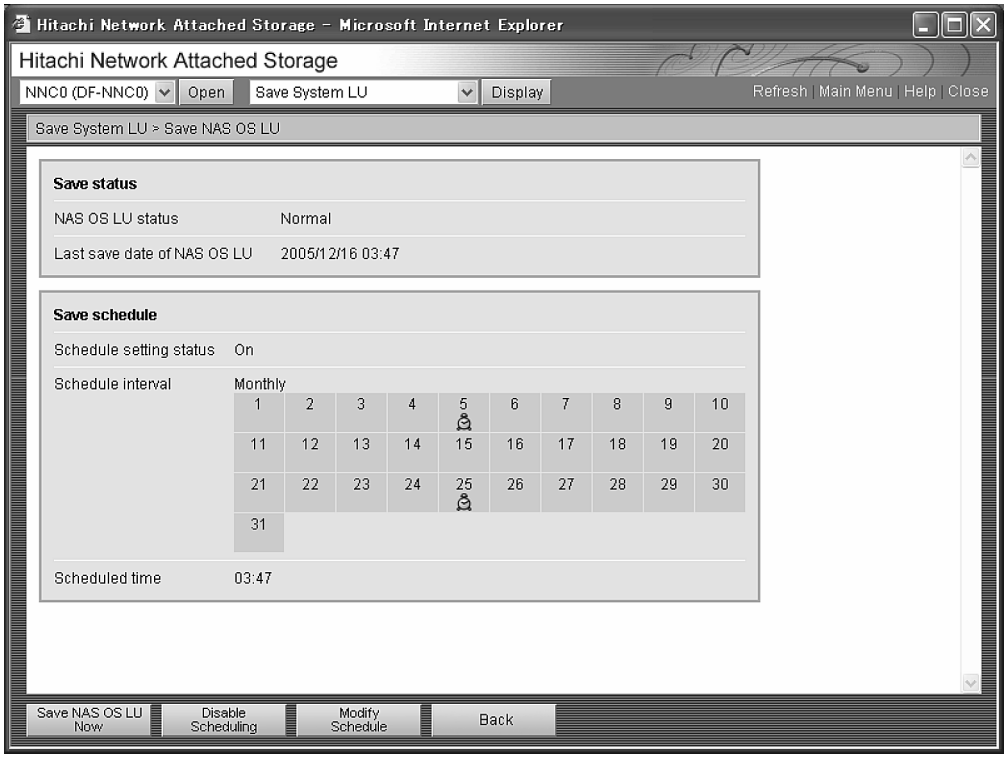



**Figure 4.117 Save NAS OS LU Window**

Before saving a NAS OS LU, make sure that no other system administrators, account administrators, your HDS representative, or end users are logged on to the NAS Unit in the cluster. If another user is logged on, the settings information for the NAS Modular system may change while the NAS OS LU is being saved, and the data may not be saved properly.

In addition, do not save a NAS OS LU manually while it is being saved or restored.

To save a NAS OS LU manually:

1. Log on to the NAS Unit for which you want to save the NAS OS LU.

   If any other system administrator, account administrator, your HDS representative, or end user are logged on, ask them to log off.

2. In the **Main Menu** window, click the **Save System LU** button.

   The **Save System LU** window displays.

3. Click the **Save NAS OS LU** button.

   The **Save NAS OS LU** window displays.

4. Verify the displayed information, as described in Table 4.75, and then click the **Save NAS OS LU Now** button.

   A dialog box confirms that you want to save the NAS OS LU.

5. Click the **OK** button.

   The NAS OS LU is saved.

**Table 4.75 Contents of Save NAS OS LU Window**

| Item | Description |
|---|---|
| **NAS OS LU status** | The save and restore status of the NAS OS LU:<br>▪ `Normal`<br>The NAS OS LU save or restore operation has finished.<br>▪ `Now saving...`<br>The NAS OS LU is being saved.<br>▪ `Now restoring...`<br>The NAS OS LU is being restored. When the status of the NAS OS LU is `Now saving...` or `Now restoring...`, do not save the NAS OS LU. |
| **Last save date of NAS OS LU** | The date and time the NAS OS LU was last saved.<br>A hyphen (-) is displayed if the NAS OS LU backup data has not been saved. |
| **Schedule setting status** | Whether periodic saving of the NAS OS LU is enabled or disabled:<br>▪ `On`<br>Periodic saving of the NAS OS LU is enabled.<br>▪ `Off`<br>Periodic saving of the NAS OS LU is not enabled. |
| **Schedule interval** | The interval in which periodic saving of the NAS OS LU is run.<br>▪ `Daily`<br>Periodic saving of the NAS OS LU is run every day.<br>▪ `Weekly`<br>Periodic saving of the NAS OS LU is run on the specified day of the week. The specified day of the week is also displayed.<br>▪ `Monthly`<br>Periodic saving of the NAS OS LU is run on the specified date every month. The specified date is also displayed.<br>▪ `-`<br>Periodic saving of the NAS OS LU is not enabled. |
| **Scheduled time** | The time when periodic saving of the NAS OS LU starts.<br>A hyphen (-) is displayed if periodic saving of the NAS OS LU is not enabled. |

### 4.17.2.2 Controlling Periodic Saving of a NAS OS LU

In the **Save NAS OS LU** window, you can enable and disable automatic saving of a NAS OS LU on a NAS Unit basis. When the NAS Modular system is first installed, the NAS OS LU periodic save schedule is already set up (automatic saving occurs daily at 3:47 AM). When the program is installed, periodic saving of a NAS OS LU runs at the interval you have set.

To set up a periodic save schedule, make sure that no system administrators, account administrators, your HDS representative, or end users are logged on to any NAS Unit in the cluster at the backup time. If another user is logged on, the settings information for the NAS Modular system may change while the NAS OS LU is being saved, and the data may not be saved properly. It takes about a minute to save a single NAS OS LU.

***Notes:***

- Even if you do set up a periodic save schedule, it is critically important that you also remember to save the NAS OS LUs manually whenever a change is made to the NAS Modular configuration.
- Saving the NAS OS LU imposes heavy loads on the NAS Modular system. When you change the NAS Modular system configuration, you should always save the configuration manually and disable periodic saving of the NAS OS LU before starting the service.
- When an automatic creation schedule is set up in NAS Sync Image for mounting and creating file shares for differential-data snapshots, set periodic saving for the NAS OS LU. Make sure that the times specified for periodic saving of the NAS OS LU and the automatic creation schedule in NAS Sync Image do not overlap and cause simultaneous execution.
- If an error occurs while periodic saving of a NAS OS LU is enabled, and you can still log in to NAS Manager, disable the periodic saving. Periodic saving might overwrite correct data with incorrect data generated after the failure.

To enable or disable periodic saving of a NAS OS LU:

1. Log on to the NAS Unit on which you plan to enable or disable periodic saving.
2. In the **Main Menu** window, click the **Save System LU** button.

   The **Save System LU** window displays.
3. Click the **Save NAS OS LU** button.

   The **Save NAS OS LU** window displays.
4. If you want to enable a periodic save schedule, click the **Enable Scheduling** button. If you want to disable a periodic save schedule, click the **Disable Scheduling** button.

   A dialog box confirms that you want to change the periodic save schedule.
5. Click the **OK** button.

   When you enable a periodic save schedule, **Schedule setting status** changes from `Off` to `On`. When you disable a periodic save schedule, **Schedule setting status** changes from `On` to `Off`.

### 4.17.2.3 Setting Up an Interval for Periodic Saving of a NAS OS LU

You can use the **Schedule Settings for NAS OS LU** window to set up an interval for periodic saving of a NAS OS LU on a NAS Unit basis.

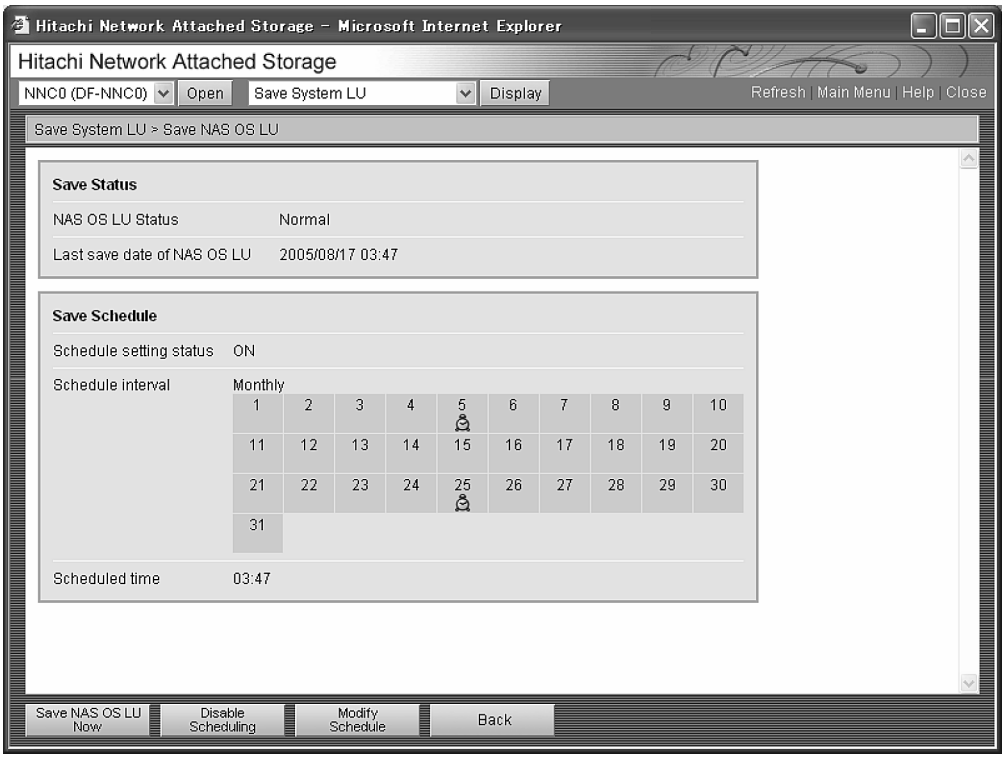



**Figure 4.118 Schedule Settings for NAS OS LU Window**

Saving NAS OS LUs imposes a heavy load on the NAS Modular system. Specify a date and time in which the service is not running for an interval of periodic saving of a NAS OS LU. We recommend that the start time of periodic saving of a NAS OS LU be set to `3:47`.

When the start time of periodic saving is set in the switchover time zone for Daylight Savings Time, save operations might be performed twice or might not be performed on the day of the switch to or from Daylight Savings Time.

To set up an interval for periodic saving of a NAS OS LU:

1. Log on to the NAS Unit on which you plan to set up an interval for periodic saving.
2. In the **Main Menu** window, click the **Save System LU** button.

   The **Save System LU** window displays.
3. Click the **Save NAS OS LU** button.

   The **Save NAS OS LU** window displays.
4. Click the **Modify Schedule** button.

   The **Schedule Settings for NAS OS LU** window displays. Information about the window's contents is described in Table 4.76.

5. Specify necessary information, and then click the **OK** button.

   The **Save NAS OS LU** window re-displays. The specified information is displayed.

**Table 4.76 Contents of Schedule Settings for NAS OS LU Window**

| Item | Description |
|---|---|
| **Interval** | The interval in which periodic saving of the NAS OS LU is run. Select the radio button:<br>▪ `Daily`<br>Periodic saving of the NAS OS LU is run every day.<br>▪ `Weekly`<br>Periodic saving of the NAS OS LU is run on the specified day of the week. Select the check box to specify the day of the week when periodic saving is to be used.<br>▪ `Monthly`<br>Periodic saving of the NAS OS LU is run on the specified date every month. Select the check box to specify the date when periodic saving is to be used.<br>Periodic saving of the NAS OS LU is not run on a date that does not exist for a given month (***Example:*** the 31st day in February). |
| **Time** | The time when periodic saving of the NAS OS LU starts. You can specify the time in one-minute units, in the range from 00:00 to 23:59. |

### 4.17.3 Saving NAS Cluster Management LUs

In the **Save NAS Cluster Management LU** window, you can enable or disable periodic saving of a NAS Cluster Management LU, as well as to save a NAS Cluster Management LU manually.

Only one generation of backup data from a NAS Cluster Management LU is available. When you save a NAS Cluster Management LU that has already been saved, the previous backup data is discarded.

When a heavy load is being imposed on a NAS Modular system, saving a NAS Cluster Management LU might automatically stop due to a timeout to reduce the load. If that happens, wait until the heavy load has decreased and run the save operation again for the NAS Cluster Management LU.

### 4.17.3.1 Saving a NAS Cluster Management LU Manually

You can use the **Save NAS Cluster Management LU** window to manually save a NAS Cluster Management LU.

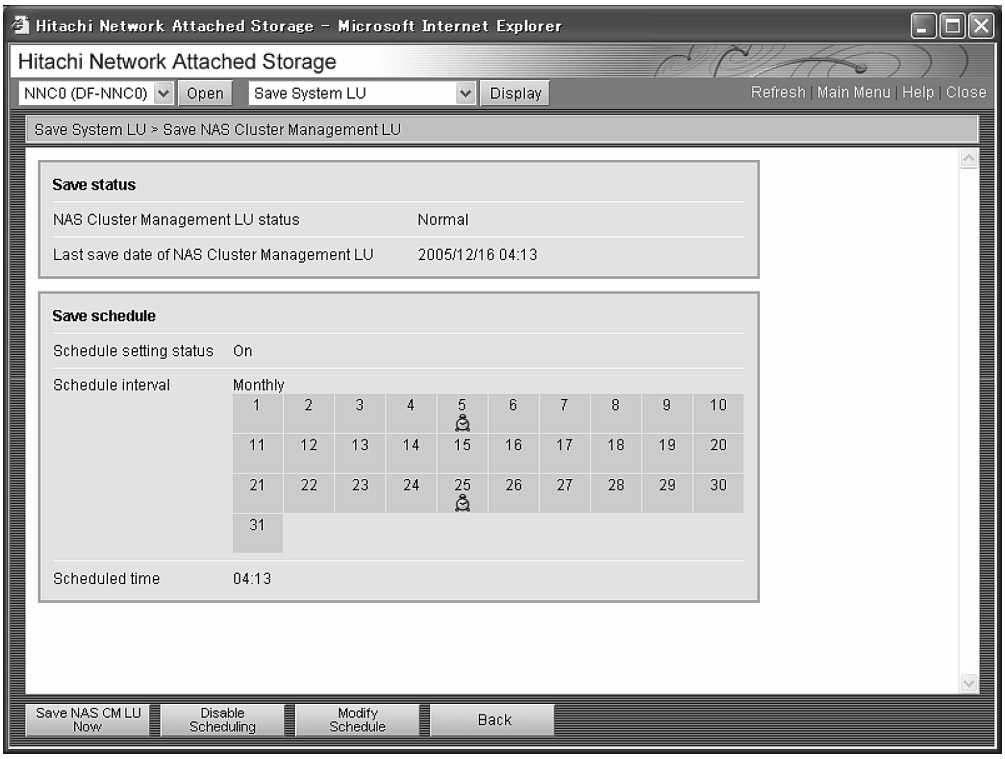



**Figure 4.119 Save NAS Cluster Management LU Window**

Before saving a NAS Cluster Management LU, make sure that no other system administrators, account administrators, your HDS representative, or end users are logged on to any of the NAS Units in the NAS Modular system. If another user is logged on, the settings information for the NAS Modular system may change while the NAS Cluster Management LU is being saved, and the data may not be saved properly.

Additionally, do not save a NAS Cluster Management LU manually while it is being saved or restored.

To save a NAS Cluster Management LU manually:

1. Log on to any NAS Unit.

   If any other system administrator, account administrator, your HDS representative, or end user are logged on, ask them to log off.

2. In the **Main Menu** window, click the **Save System LU** button.

   The **Save System LU** window displays.

3. Click the **Save NAS CM LU** button.

   The **Save NAS Cluster Management LU** window displays.

4. Verify the displayed information, as described in Table 4.77, and then click the **Save NAS CM LU Now** button.

   A dialog box confirms that you want to save the NAS Cluster Management LU.

5. Click the **OK** button.

   The NAS Cluster Management LU is saved.

**Table 4.77 Contents of Save NAS Cluster Management LU Window**

| Item | Description |
|---|---|
| **NAS Cluster Management LU status** | The save and restore status of the NAS Cluster Management LU:<br>▪ `Normal`<br>The NAS Cluster Management LU save or restore operation has finished.<br>▪ `Now saving...`<br>The NAS Cluster Management LU is being saved.<br>▪ `Now restoring...`<br>The NAS Cluster Management LU is being restored.<br>When the status of the NAS Cluster Management LU is `Now saving...` or `Now restoring...`, do not save the NAS Cluster Management LU. |
| **Last save date of NAS Cluster Management LU** | The date and time the NAS Cluster Management LU was last saved.<br>A hyphen (-) is displayed if the NAS Cluster Management LU backup data has not been saved. |
| **Schedule setting status** | Whether periodic saving of the NAS Cluster Management LU is enabled or disabled:<br>▪ `On`<br>Periodic saving of the NAS Cluster Management LU is enabled.<br>▪ `Off`<br>Periodic saving of the NAS Cluster Management LU is not enabled. |
| **Schedule interval** | The interval in which periodic saving of the NAS Cluster Management LU is run:<br>▪ `Daily`<br>Periodic saving of the NAS Cluster Management LU is run every day.<br>▪ `Weekly`<br>Periodic saving of the NAS Cluster Management LU is run on the specified day of the week. The specified day of the week is also displayed.<br>▪ `Monthly`<br>Periodic saving of the NAS Cluster Management LU is run on the specified date every month. The specified date is also displayed.<br>▪ `-`<br>Periodic saving of the NAS Cluster Management LU is not enabled. |
| **Scheduled time** | The time when periodic saving of the NAS Cluster Management LU starts.<br>A hyphen (-) is displayed if periodic saving of the NAS Cluster Management LU is not enabled. |

### 4.17.3.2 Controlling Periodic Saving of a NAS Cluster Management LU

You can use the **Save NAS Cluster Management LU** window to enable and disable automatic saving of a NAS Cluster Management LU. The NAS Cluster Management LU is shared among all NAS Units in a NAS Modular subsystem, so you do not need to enable or disable periodic saving for the NAS Cluster Management LU from each NAS Units but one.

When the NAS Modular system is first installed, automatic saving is set up so that the NAS Cluster Management LU is saved daily.

When T**agmaStore AMS 500**, **TagmaStore AMS 200**, or **TagmaStore WMS 100** is used:

The NAS Cluster Management LU is saved at 4:08 in NNC0 and at 4:12 in NNC2.

When T**agmaStore AMS 1000** is used:

The NAS Cluster Management LU is saved at 4:09 in NNC1 and at 4:13 in NNC3.

***Notes:***

- If you decide to set up a periodic save schedule, make sure that no system administrators, account administrators, your HDS representative, or end users are logged on to any NAS Unit in the NAS Modular system at the backup time. If another user is logged on, the settings information for the NAS Modular system may change while the NAS Cluster Management LU is being saved, and the data may not be saved properly. It takes about 3 minutes to save a NAS Cluster Management LU.
- Even if you do set up a periodic save schedule, it is critically important that you also remember to save the NAS Cluster Management LU manually whenever a change is made to the NAS Modular subsystem.
- Saving NAS Cluster Management LU imposes heavy loads on the NAS Modular system. When you change the NAS Modular system configuration, you should always save the configuration manually and disable periodic saving of the NAS Cluster Management LU before starting the service.

  ***Note:*** When an automatic creation schedule is set up in NAS Sync Image for mounting and creating files shares for differential-data snapshots, set periodic saving for the NAS Cluster Management LU. Make sure that the times specified for periodic saving of the NAS Cluster Management LU and the automatic creation schedule in NAS Sync Image do not overlap and cause simultaneous execution.
- If an error occurs while periodic saving of a NAS Cluster Management LU is enabled, and you can still log in to NAS Manager, disable the periodic saving. Periodic saving might overwrite correct data with incorrect data generated after the failure.

To enable or disable periodic saving of a NAS Cluster Management LU:

1. Log on to any NAS Unit.
2. In the **Main Menu** window, click the **Save System LU** button.

   The **Save System LU** window displays.
3. Click the **Save NAS CM LU** button.

   The **Save NAS Cluster Management LU** window displays.
4. If you want to enable a periodic save schedule, click the **Enable Scheduling** button. If you want to disable a periodic save schedule, click the **Disable Scheduling** button.

   A dialog box is displayed to confirm that you want to change the periodic save schedule.

5. Click the **OK** button.

   When you enable a periodic save schedule, **Schedule setting status** changes from `Off` to `On`. When you disable a periodic save schedule, **Schedule setting status** changes from `On` to `Off`.

### 4.17.3.3 Setting Up an Interval for Periodic Saving of a NAS Cluster Management LU

You can use the **Schedule Settings for NAS Cluster Management LU** window to set up an interval for periodic saving of a NAS Cluster Management LU on a NAS Unit basis.

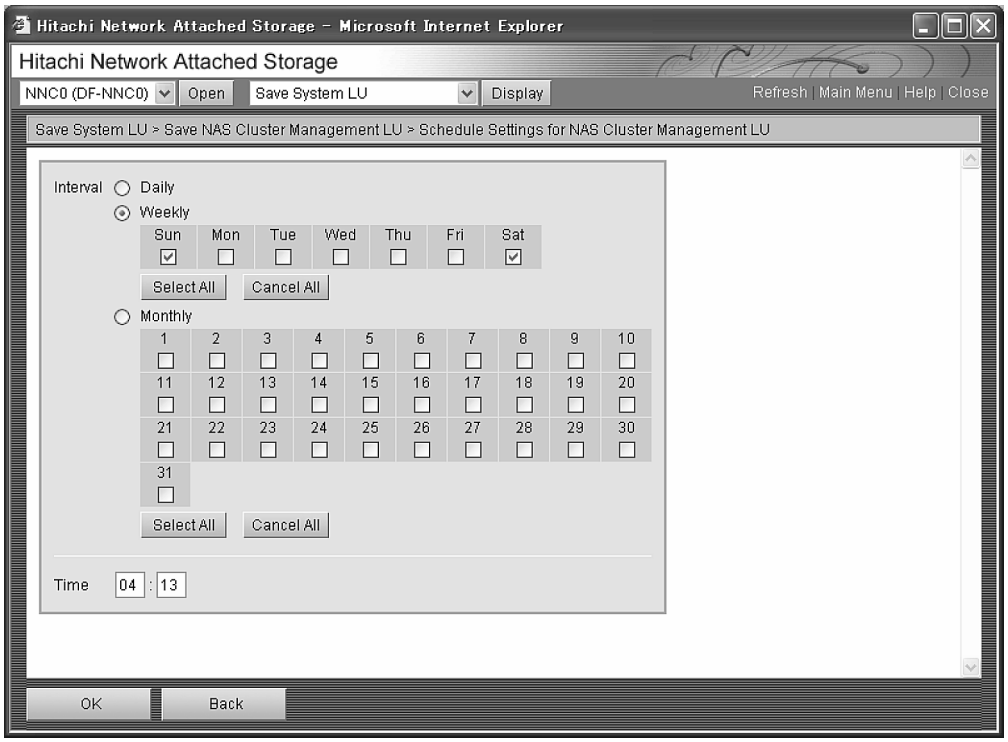



**Figure 4.120 Schedule Settings for NAS Cluster Management LU Window**

***Notes:***

- Saving NAS Cluster Management LU imposes heavy loads on the NAS Modular system. Specify a date and time in which the service is not running for an interval of periodic saving of a NAS Cluster Management LU. We recommend that start time of periodic saving of a NAS Cluster Management LU be set to a time between `4:08` and `4:15`. If periodic saving of a NAS Cluster Management LU conflicts, such as when the same interval for periodic saving of a NAS Cluster Management LU is set for two different NAS Units, the second periodic saving of the NAS Cluster Management LU might fail. However, the first periodic saving of the NAS Cluster Management LU will be performed normally.
- When the start time of periodic saving is set in the switchover time zone for Daylight Savings Time, save operations might be performed twice or might not be performed on the day of the switch to or from Daylight Savings Time.

To set up an interval for periodic saving of a NAS Cluster Management LU:

1. Log on to the desired NAS Unit.
2. In the **Main Menu** window, click the **Save System LU** button.

   The **Save System LU** window displays.
3. Click the **Save NAS CM LU** button.

   The **Save NAS Cluster Management LU** window displays.
4. Click the **Modify Schedule** button.

   The **Schedule Settings for NAS Cluster Management LU** window displays.
5. Specify necessary information, and then click the **OK** button.

   The **Save NAS Cluster Management LU** window re-displays. The specified information is displayed.

   The following table describes the information that is displayed in the window:

**Table 4.78 Info Specified in Schedule Settings for NAS Cluster Management LU Window**

| Item | Description |
|---|---|
| **Interval** | The interval in which periodic saving of the NAS Cluster Management LU is run. Select a radio button:<br>▪ `Daily`<br>Periodic saving of the NAS Cluster Management LU is run every day.<br>▪ `Weekly`<br>Periodic saving of the NAS Cluster Management LU is run on the specified day of the week. Select the check box to specify the day of the week when periodic saving is being run.<br>▪ `Monthly`<br>Periodic saving of the NAS Cluster Management LU is used on the specified date every month. Select the check box to specify the date when periodic saving is being run.<br>Periodic saving of the NAS Cluster Management LU is not run on a date that does not exist for a given month. (***Example:*** the 31st day of February). |
| **Time** | The time when periodic saving of the NAS Cluster Management LU starts. You can specify the time in one-minute units, in the range from 00:00 to 23:59. |

# Chapter 5 Performing System Administrator Operations Using Commands

This chapter describes how the system administrator uses commands to manage items such as NAS Manager file systems, file sharing, checking of network settings and communications, and managing quotas. For details about the syntax of each command, see Chapter 6.

- Using Commands (see section 5.1)
- Executing Commands (see section 5.2)
- Registering a Public Key using Commands (see section 5.3)
- Managing Clusters Using Commands (see section 5.4)
- Managing File Systems Using Commands (see section 5.5)
- Managing File Shares (see section 5.6)
- Managing Quotas Using Commands (see section 5.7 )
- Managing User Mapping Using Commands (see section 5.8)
- Checking the Network Settings and Connectivity (see section 5.9)

## 5.1 Using Commands

The system administrator can use commands whenever necessary to operate the NAS Modular system.

To log in to a NAS Package and execute a command, use `nasroot` for the SSH account. You can also use commands to create a shell script and automate operations. The system administrator can use commands for operations such as registering a public key, managing a cluster, and creating a file system or file share. For more information on how to create a shell script and use commands automatically, see Chapter 6.

### 5.1.1 Operations that can be performed using commands

The following table lists the operations that the system administrator can perform using commands.

**Table 5.1 Operations Performed Using Commands and Document References**

| Operations that can be performed using commands | Details of operations that can be performed using commands | Description of operations using commands | Description of operations using GUI |
|---|---|---|---|
| Managing public keys used by SSH | Viewing public key information | 6.2.54 | 4.6.5.1 |
| | Registering a public key | 5.3.2 | 4.6.5 |
| | Deleting a public key | 5.3.3 | 4.6.5.2 |

| Operations that can be performed using commands | Details of operations that can be performed using commands | Description of operations using commands | Description of operations using GUI |
|---|---|---|---|
| Cluster operations | Viewing the status of a cluster | 5.4.2 | 4.5.3 |
| | Stopping and starting a cluster | 5.4.3 | 4.5.4 |
| | Performing a forced stop for a cluster | 5.4.4 | 4.5.6 |
| | Viewing the status of a node | 5.4.5 | 4.5.3 |
| | Stopping and starting a node | 5.4.6 | 4.5.5 |
| | Viewing the status of a resource group | 5.4.7 | 4.5.7 |
| | Stopping and starting a resource group | 5.4.8 | 4.5.8 |
| | Performing a forced stop for a resource group | 5.4.9 | 4.5.9 |
| | Changing the executing node of a resource group | 5.4.10 | 4.5.11 |
| | Disabling and restarting resource group monitoring | 5.4.11 | 4.5.11 |
| File system operations | Viewing file system information | 5.5.2 | 4.10.4 |
| | Creating a file system | 5.5.3 | 4.10.5 |
| | Mounting a file system | 5.5.4 | 4.10.6 |
| | Unmounting a file system | 5.5.5.2 | 4.10.7 |
| | Deleting a file system | 5.5.6.2 | 4.10.9 |
| | Managing the warning notification related to file system usage | 5.5.7 | - |
| | Managing automatic failover if a file system becomes blocked | 5.5.8 | - |
| | Managing the settings for recording the file creation time | 5.5.9 | - |
| NFS share operations | Viewing information about an NFS share | 5.6.1.2 | 4.11.1 |
| | Creating an NFS share | 5.6.1.3 | 4.11.2 |
| | Editing information about an NFS share | 5.6.1.4 | 4.11.4 |
| | Deleting an NFS share | 5.6.1.5 | 4.11.5 |
| | Setting up an NFS environment for the NAS OS | 5.6.1.6 | - |
| | Deleting mount information for an NFS client | 5.6.1.7 | - |
| | Deleting the file lock information for an NFS client host | 5.6.1.8 | - |
| CIFS share operations | Viewing information about a CIFS | 5.6.2.1 | 4.11.7 |

| Operations that can be performed using commands | Details of operations that can be performed using commands | Description of operations using commands | Description of operations using GUI |
|---|---|---|---|
| | share | | |
| | Creating a CIFS share | 5.6.2.2 | 4.11.2 |
| | Editing information about a CIFS share | 5.6.2.3 | 4.11.11 |
| | Deleting a CIFS share | 5.6.2.4 | 4.11.12 |
| | Viewing ACL settings | 5.6.3.2 | - |
| | Setting an ACL | 5.6.3.3 | - |
| Managing quotas for each file system | Viewing the quota information set for a file system | 5.7.2.1 | 4.12.2 |
| | Setting a user quota for a file system | 5.7.3 | 4.12.4 |
| | Setting a group quota for a file system | | 4.12.3 |
| | Setting the default quota for a file system | | 4.12.5 |
| | Setting a quota grace period for a file system | | 4.12.6 |
| | Setting the quota monitoring method for a file system | | 4.12.7 |

| Operations that can be performed using commands | Details of operations that can be performed using commands | Description of operations using commands | Description of operations using GUI |
|---|---|---|---|
| Managing subtree quotas | Viewing the quota information set for a directory | 5.7.4.1 | - |
| | Viewing quota information for a user or group set for a directory | 5.7.4.2 | - |
| | Setting a quota for a directory | 5.7.4.3 | - |
| | Setting a user quota for a directory | 5.7.4.4 | - |
| | Setting a group quota for a directory | 5.7.4.5 | - |
| | Setting the default quota for a directory | 5.7.4.6 | - |
| | Applying a quota to an existing directory | 5.7.4.7 | - |
| | Setting a quota grace period for a directory | 5.7.4.8 | - |
| | Canceling the quota set for a directory | | - |
| Managing user mapping information | Checking IDs and names mapped by the RID method | - | - |
| Checking network settings and connectivity | Checking the network settings | 5.9.1 | - |
| | Checking the connection to a specified host | 5.9.2 | - |
| | Checking the path that leads to a specified host | 5.9.3 | - |
| Managing FC port | Displaying and changing FC port data transfer rate | 5.10 | - |

### 5.1.2 Flow of operations using commands

The system administrator can use commands to operate the NAS Modular system after specifying the cluster configuration, network information, SSH public key, and other settings from the GUI.

The following figure illustrates the overall flow of operations using commands.

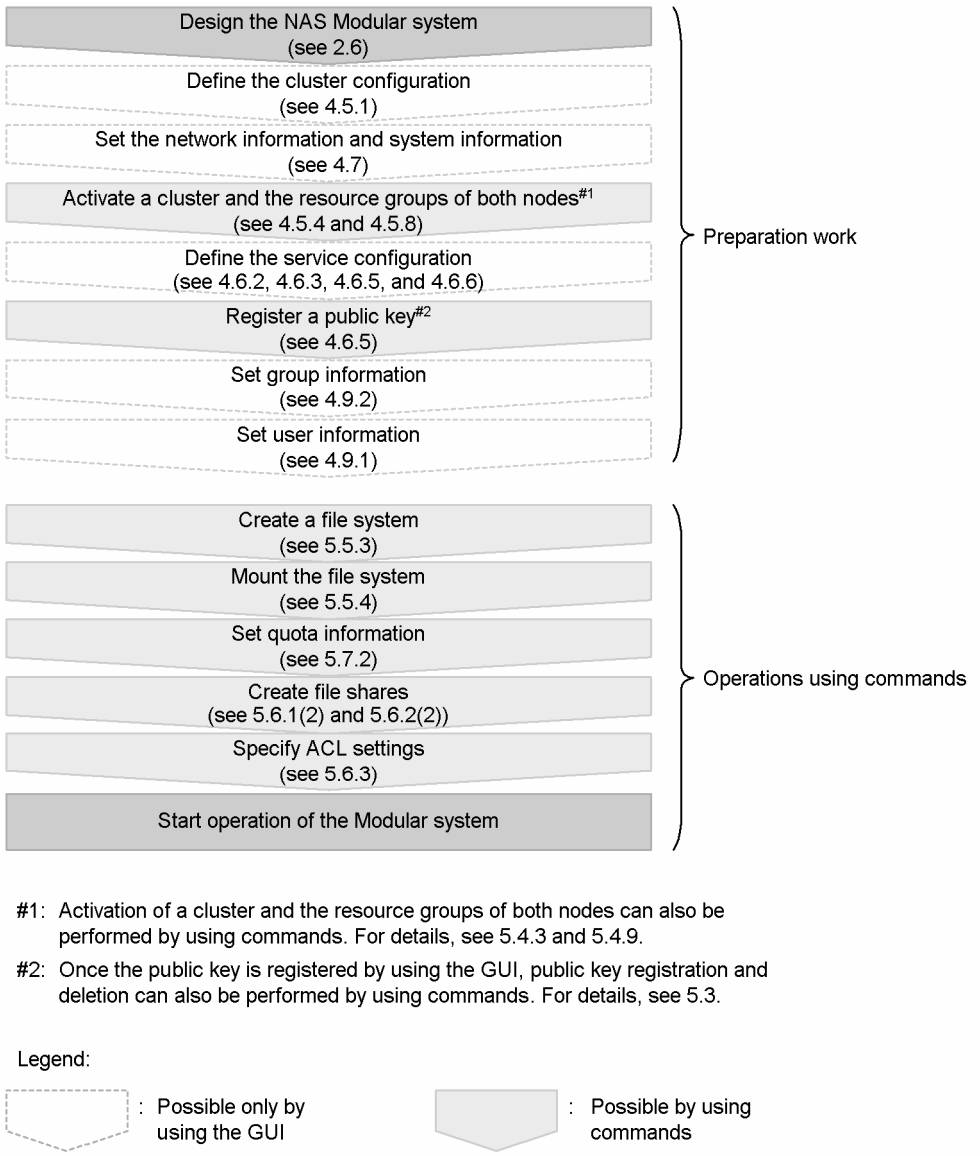



**Figure 5.1 Overall flow of operations using commands**

To use the virus scan functionality (optional) upon starting operation of the NAS Modular system, the virus scan function must be started before a file share is created. For details on starting the virus scan function, see 4.10 .

You need to check whether or not the resource group is partially blocked when the NAS Modular system operation is started. For details on partial blockage of a resource group, see 4.10.

### 5.1.3 Notes on operations (required reading before using commands)

Keep the following points in mind when you execute commands:

- Do not use a command that is not explained in this manual.
- Do not perform GUI operations while commands are being used to perform operations on the NAS Modular system.
- When you register or delete a public key, always perform the operation for both of the nodes that make up a cluster. If you perform different operations for the nodes, you may no longer be able to log in by specifying a service IP address.
- After you execute a command for a cluster, node, or resource group, do not perform another operation until the processing of the command is complete. If you do so, the other operation may fail.
- When one system administrator is setting or updating system configuration information of a node or cluster, another system administrator cannot set or update the information. Do not attempt to set or update system configuration information of a node or cluster while another system administrator is setting or updating the information.
- A cluster must have already been created before a system administrator can use commands to work with a cluster, a file system, a file share, or quota information.
- When a command accepts one of the following signals, the signal will be blocked.

**Table 5.2 List of signals to be blocked with a command**

| Signal value | Signal name | Description |
|---|---|---|
| 1 | SIGHUP | e.g. SSH disconnection |
| 2#1 | SIGINT | e.g. **Ctrl** + **c** |
| 3 | SIGQUIT | e.g. **Ctrl** + \ |
| 15 | SIGTERM | e.g. Shutdown |

#1: The SIGINT signal can be used to cancel the processing of the following commands:

- enas_fsctl command
- enas_quotaget command
- stquota command
- stquotalist command
- stquotaset command

When a resource group is started on a NAS Modular system, resources for which failure is detected are blocked, and the resource group is comprised of the remaining valid resources. When a resource group is partially blocked, services on the node are provided with some services stopped. In this case, when the `enas_clstatus` command or `enas_rgstatus` command is executed, since `Online / No error` is displayed as the resource group status, resource group error information cannot be checked.

A resource group might become partially blocked in the following situations:

- When NAS Modular system operation starts
- When failover or failback occurs
- When a resource group is restarted

If the above operations are performed, or the status of the resource group displayed as `Online` when the `enas_clstatus` command or `enas_rgstatus` command is executed even though the user cannot access the file system, the system messages need to be checked in the **List of RAS Information** (List of Messages) window of NAS Manager to see whether partial resource group blocking has occurred. For details on how to check system messages, see Chapter 9.

The system administrator must check whether the KAQG72006-E message is output within the system messages.

Note that depending on the resource type, other resources using a blocked resource might also be blocked. For example, when a logical volume is blocked, file systems created on the blocked logical volume are also blocked. In this case, the KAQG72006-E message is output for each blocked resource.

- Note that an error will occur if a cluster is stopped, a node is stopped, a resource group is stopped, the executing node of a resource group is changed, or a file system is unmounted while any of the following commands are executing. In this case, perform the above operations again once command processing is finished.
  - `horc_pvol_freeze` command (for NAS Backup Restore)
  - `horc_pvol_unfreeze` command (for NAS Backup Restore)
  - `syncadd` command (for NAS Sync Image)
  - `syncexpand` command (for NAS Sync Image)

## 5.2 Command execution

To use commands to operate the NAS Modular system, at least one public key must be registered for the SSH account (`nasroot`). The fist public key is registered by using the GUI.

NAS Manager commands can be used after a NAS Manager license has been set using Storage Navigator Modular. For details on how to set a NAS Manager license, see the manual *Storage Navigator Modular User's Guide*.

Commands can be executed by logging in to the NAS Unit or from a remote host.

This section describes how a system administrator can execute commands.

### 5.2.1 Executing commands by logging in to the NAS Unit

To execute a command by logging in to the NAS Unit:

2. Log in to the target NAS Unit by using SSH.

   If you want to execute the following commands, we recommend that you specify the service IP address:

   - enas_fsautofo
   - enas_fsfullmsg
   - enas_fsctl
   - stquota
   - stquotalist
   - stquotaset

   f you want to execute other commands, specify the fixed IP address.

   For UNIX:

   Execute the ssh command.

```
ssh {-1|-2} user-name-of-the-ssh-account@host-name-for-the-NAS-Unit
```

   For Windows:

   Use SSH-compliant communications software.

3. Use the sudo command to execute commands.

   The following shows an example of executing a command.

   In this example, you will execute the enas_fscreate command.

```
$ sudo enas_fscreate FS_1 lu1A
```

### 5.2.2 Executing commands from a remote host

To execute a command from a remote host, use the following command line:

```
ssh {-1|-2} user-name-of-the-ssh-account@host-name-for-the-NAS-Unit sudo
command-to-be-executed
```

If you want to execute the following commands, we recommend that you specify the service IP address:

- enas_fsautofo
- enas_fsfullmsg
- enas_fsctl
- stquota
- stquotalist
- stquotaset

If you want to execute other commands, specify the fixed IP address.

You can automatically execute multiple commands by creating a shell script on the remote host. For details on how to create a shell script, see the documentation for the remote host OS.

## 5.3 Register a public key using commands

This section explains how the system administrator can use commands to register and delete public keys.

### 5.3.1 Viewing public key information

A system administrator can use a command to view public key information. To view public key information:

Execute the `enas_sshkeylist` command to view public key information:

```
$ sudo enas_sshkeylist
User  Ver.  Comment
nasroot SSH1  ssh1-050802
nasroot SSH1  ssh1-admin
nasroot SSH1  ssh1-nasroot2
nasroot SSH1  ssh1-admin3
nasroot SSH2  ssh2-nasroot1
...
```

### 5.3.2 Registering a public key

A system administrator can use commands to register a public key that will be used for SSH authentication. Public keys are registered for the SSH account `nasroot`. The maximum number of public keys per node for the SSH1 and SSH2 protocols is 128.

This subsection describes how to register a public key. The procedure assumes that the public key is registered under the following conditions:

- The public key file is created on a UNIX machine.
- The name of the public key file is `naskey.pub`.
- The comment on the public key is `nasroot-key`.
- The host name of the NAS Unit for which the public key is to be registered is `nas01`.
- SSH protocol version 2 is used.

1. Use the key creation tool to create the keys (private and public) used for SSH authentication.

   For details on how to perform installation and create keys, see the relevant documentation.

2. Use the `scp` command to transfer the public key file to the SSH account home directory (`/home/nasroot`).

***Notes:***

A public key file cannot use a name that is already being used by a directory or file name under the home directory of the SSH account.

```
$ scp /home/admin/.ssh/naskey.pub nasroot@nas01:
naskey.pub 100% |************************************| 219   00:00
```

3. Log in to the target NAS Unit by using SSH.

```
$ ssh -2 nasroot@nas01
```

4. Execute the `enas_sshkeyadd` command to register the public key.

   The public key is registered and the specified public key file is deleted from the `/home/nasroot` directory.

```
$ sudo enas_sshkeyadd -2 -c nasroot-key naskey.pub
```

5. Execute the `enas_sshkeylist` command to confirm that the public key has been registered correctly.

```
$ sudo enas_sshkeylist
User  Ver.  Comment
...
nasroot SSH2  nasroot-key
```

6. Perform steps 2 through 5 for the other NAS Unit so that both NAS Units in the cluster have the same settings.

***Notes:***

If you have transferred the wrong file to the `/home/nasroot` directory, you can use the `enas_rmfile` command to delete the file.

```
$ sudo enas_rmfile ssh-key-nasroot.pub
```

### 5.3.3 Deleting a public key

A system administrator can use commands to delete unnecessary public keys.

If you (system administrator) use a command to delete the public key that you are currently using, you will not be able to log in with that key again.

If all public keys are deleted, commands can no longer be used. To enable command usage again, use the GUI to register a public key. For details on how to use the GUI to register a public key, see Chapter 6.

The following procedure shows how to delete a public key. The procedure assumes that you will delete a public key that was registered with a comment of `nasroot-key`.

To delete a public key:

1. Execute the `enas_sshkeylist` command to check the comment on the public key you want to delete.

```
$ sudo enas_sshkeylist
User  Ver.  Comment
nasroot SSH1  ssh1-050802
nasroot SSH1  ssh1-admin
nasroot SSH1  ssh1-nasroot2
nasroot SSH1  ssh1-admin3
nasroot SSH2  nasroot-key
```

2. Execute the `enas_sshkeydel` command to delete the public key.

```
$ sudo enas_sshkeydel -2 -c nasroot-key
```

3. Execute the `enas_sshkeylist` command to confirm that the public key has been deleted.
4. Log in to the other NAS Unit. Perform steps 1 through 3 for the other NAS Unit so that both of the NAS Units that make up the cluster have the same settings.

## 5.4 Managing Clusters using Commands

This section describes how a system administrator can use commands to manage the status of a cluster, node, or resource group.

### 5.4.1 Before using Commands to Manage a Cluster

After the following operations, the system administrator must confirm whether a partial blockage has occurred in the resource group:

- When starting a cluster that was stopped while the resource group was running
- When starting a node that was stopped while the resource group was running
- When starting a resource group
- When changing an executing node of a resource group

For details on partial resource group blockage, see 5.1.3.

### 5.4.2 Viewing the status of a cluster

A system administrator can use a command to view the status of a cluster.

The following procedure shows how to view the status of a cluster. The procedure assumes that you as a system administrator will view the status of the cluster that consists of the two nodes that you are logged in to, the nodes, and the resource groups of each node.

To view the status of a cluster, nodes, and resource groups:

1. Execute the `enas_clstatus` command to view the status of the cluster, nodes, and resource groups.

```
$ sudo enas_clstatus
--Cluster Status--
Cluster name  : nas-cluster01
Cluster status : ACTIVE

--Node Status--
NNC2(DF-H-nnc2)
Node name    : nas-02
Node status   : UP

NNC0(DF-H-nnc0)
Node name    : nas-01
Node status   : UP

--Resource Group Status--
Resource group name   : nas-02
Resource group status  : Online/No error
Running node       : nas-02

Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-01
```

### 5.4.3 Stopping and Starting a Cluster

A system administrator can use commands to stop and start a cluster during maintenance or troubleshooting. If a cluster has failed, the cluster is stopped before troubleshooting is started, and the cluster is started after the troubleshooting is complete. When a cluster is stopped and started, there is no need to stop and start each node in the cluster. If a resource group has been stopped when the cluster is stopped, start the resource group after the cluster is started.

After stopping a cluster while a resource group is running, if you restart the cluster, the resource group will restart automatically. In such a case, the status of the resource group changes in the following order: `Online Ready`, `Initializing`, `Discovery (exclusivity)`, `Online Pending`, and `Online`. If many resources have been registered, it takes several tens of minutes until the status of the resource group changes to `Online/No error`.

#### 5.4.3.1 Stopping a cluster

A system administrator can use commands to stop a cluster.

To stop a cluster:

1. Execute the `enas_clstatus` command to check the status of the cluster and resource groups.

2. Confirm that the status of the cluster and resource groups is as follows:
   - `Cluster status` is `ACTIVE`.
   - `Resource group status` is `Online/No error`, `Offline/No error`, or `Online Maintenance/No error`.

```
$ sudo enas_clstatus

--Cluster Status--
Cluster name  : nas-cluster01
Cluster status : ACTIVE

--Node Status--
NNC2(DF-H-nnc2)
Node name    : nas-02
Node status   : UP

NNC0(DF-H-nnc0)
Node name    : nas-01
Node status   : UP

--Resource Group Status--
Resource group name   : nas-02
Resource group status  : Online/No error
Running node       : nas-02

Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-01
```

3. Execute the `enas_clstop` command to stop the cluster.

   When the `enas_clstop` command is executed, all nodes comprising the cluster and all resource groups running on the nodes are stopped.

```
$ sudo enas_clstop
```

4. Execute the `enas_clstatus` command to confirm that the cluster is stopped.

Confirm that `Cluster status` is `INACTIVE`. Note that if you stop the cluster while a resource group is running, `Resource group status` is `Online Ready`.

```
$ sudo enas_clstatus

--Cluster Status--
Cluster name  : nas-cluster01
Cluster status : INACTIVE
...
--Resource Group Status--
Resource group name   : nas-02
Resource group status  : Online Ready/No error
Running node       :

Resource group name   : nas-01
Resource group status  : Online Ready/No error
Running node       :
```

#### 5.4.3.2 Starting a cluster

A system administrator can use commands to start a cluster.

To start a cluster:

1. Execute the `enas_clstatus` command to confirm that the target cluster is stopped.

   Confirm that `Cluster status` is `INACTIVE`.

```
$ sudo enas_clstatus

--Cluster Status--
Cluster name  : nas-cluster01
Cluster status : INACTIVE

--Node Status--
NNC2(DF-H-nnc2)
Node name    : nas-02
Node status   : INACTIVE

NNC0(DF-H-nnc0)
Node name    : nas-01
Node status   : INACTIVE

--Resource Group Status--
Resource group name   : nas-02
Resource group status  : Online Ready/No error
Running node       :

Resource group name   : nas-01
Resource group status  : Online Ready/No error
Running node       :
```

2. Execute the `enas_clstart` command to start the cluster.

   When the `enas_clstart` command is executed, all nodes comprising the cluster are started. When a node is started, its resource groups can also be started.

```
$ sudo enas_clstart
```

3. Start resource groups, if necessary.

   This step is necessary if resource groups had been stopped when the cluster was stopped. For details on how to start resource groups, see 5.4.8.

4. Execute the `enas_clstatus` to confirm that the cluster, nodes, and resource groups are running correctly.

   Confirm that the status of the cluster, nodes, and resource groups are as follows:

   - `Cluster status` is `ACTIVE`.
   - `Node status` is `UP`.
   - `Resource group status` is `Online/No error`.

```
$ sudo enas_clstatus

--Cluster Status--
```

```
Cluster name  : nas-cluster01
Cluster status : ACTIVE

--Node Status--
NNC2(DF-H-nnc2)
Node name     : nas-02
Node status   : UP

NNC0(DF-H-nnc0)
Node name     : nas-01
Node status   : UP

--Resource Group Status--
Resource group name   : nas-02
Resource group status  : Online/No error
Running node       : nas-02

Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-01
```

### 5.4.4 Performing a Forced Stop for a Cluster

If an error occurs while a cluster or node is being stopped or started and processing cannot be continued, a system administrator can use commands to stop the cluster forcibly.

If a temporary error occurs while a cluster, node, or resource group is being stopped or started, a forced stop followed by a restart may be able to correct the error. If the error cannot be corrected after repeated attempts, the system administrator must determine the cause of the error from the error information and take corrective measures. For details on the corrective measures for an error that occurs while a cluster, node, or resource group is being stopped or started, see Chapter 9.

Some services may remain running after a forced stop. This is because the system ignores any services affected by the error when completing the stop processing. If you start a resource group while some services remain running, two services with the same name may start. To prevent such a problem, do not start a resource group after a forced stop until the cluster or both nodes in the cluster have started. Performing a forced stop for a cluster may take an extended period of time.

To stop a cluster forcibly:

1. Execute the `enas_clstatus` (Display cluster status) command to view the status of the cluster, nodes, and resource groups.

   Confirm that `Cluster status` is not `INACTIVE`. Confirm that Online/srmd executable error or other information is displayed for Resource group status.

```
$ sudo enas_clstatus

--Cluster Status--
Cluster name  : nas-cluster01
Cluster status : ACTIVE
```

```
--Node Status--
NNC2(DF-H-nnc2)
Node name    : nas-02
Node status   : UP

NNC0(DF-H-nnc0)
Node name    : nas-01
Node status   : UP

--Resource Group Status--
Resource group name   : nas-02
Resource group status  : Online/srmd executable error
Running node       : nas-01

Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-01
```

2. Execute the `enas_clstop` command to stop the cluster forcibly.

   All nodes comprising the cluster and all resource groups running on those nodes stop. Any failure that occurs during the stop processing is ignored.

```
$ sudo enas_clstop -f
```

3. Execute the `enas_clstatus` command to confirm that the cluster is stopped.

   Confirm that `Cluster status` is `INACTIVE`. If the processing is not completed within 30 minutes, an error that cannot be corrected by a forced stop may have occurred. Contact maintenance personnel.

```
$ sudo enas_clstatus

--Cluster Status--
Cluster name  : nas-cluster01
Cluster status : INACTIVE

--Node Status--
NNC2(DF-H-nnc2)
Node name    : nas-02
Node status   : INACTIVE

NNC0(DF-H-nnc0)
Node name    : nas-01
Node status   : INACTIVE

--Resource Group Status--
Resource group name   : nas-02
Resource group status  : Online Ready/No error
Running node       :

Resource group name   : nas-01
Resource group status  : Online Ready/No error
Running node       :
```

### 5.4.5 Viewing the Status of Node(s)

A system administrator can use a command to view the status of node(s).

The following procedure shows how to view the status of a node or nodes. The procedure assumes that you as a system administrator will view the status of both nodes that make up the cluster. To view the status of nodes:

Execute the `enas_ndstatus` command to view the status of node(s).

```
$ sudo enas_ndstatus

--Node Status--
NNC2(DF-H-nnc2)
Node name    : nas-02
Node status   : UP

NNC0(DF-H-nnc0)
Node name    : nas-01
Node status   : UP
```

### 5.4.6 Stopping and starting a node

You as a system administrator can use commands to stop and start a node for maintenance or troubleshooting. When recovering a node from failure after failover, stop the node and then start it again once operations have finished.

#### 5.4.6.1 Stopping a Node

A system administrator can use commands to stop a node.

The following procedure shows how to stop a node. The procedure assumes that `nas-01` is the name of the node to be stopped.

To stop a node:

1. Execute the `enas_clstatus` command to check the status of the target node and the resource groups on the node.

   Confirm that the status of the nodes and resource groups are as follows:

   – `Node status` of the target node is `UP`.

   `Resource group status` of each resource group on the target node is `Online/No error`, `Offline/No error`, or `Online Maintenance/No error`.

```
$ sudo enas_clstatus

--Cluster Status--
Cluster name  : nas-cluster01
Cluster status : ACTIVE

--Node Status--
```

```
NNC2(DF-H-nnc2)
Node name    : nas-02
Node status   : UP

NNC0(DF-H-nnc0)
Node name    : nas-01
Node status   : UP

--Resource Group Status--
Resource group name   : nas-02
Resource group status  : Online/No error
Running node       : nas-02

Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-01
```

2. Execute the `enas_ndstop` command to stop the node.

   When the `enas_ndstop` command is executed, the node is stopped, and the resource groups running on the node are failed over to the other node. However, when a node for which two resource groups are running is stopped, the resource groups moved over due to failover are stopped, and the previously running resource groups are failed over to the other node.

```
$ sudo enas_ndstop nas-01
```

3. Execute the `enas_ndstatus` command to confirm that the node is stopped.

   Confirm that `Node status` is `INACTIVE`.

```
$ sudo enas_ndstatus nas-01

...
--Node Status--
...
NNC0(DF-H-nnc0)
Node name    : nas-01
Node status   : INACTIVE

--Resource Group Status--
...
Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-02
```

#### 5.4.6.2 Starting a Node

A system administrator can use commands to start a node.

The following procedure shows how to start a node. The procedure assumes that `nas-01` is the name of the node to be started.

To start a node:

1. Execute the `enas_ndstatus` command to confirm that the target node is stopped.

Confirm that `Node status` is `INACTIVE`.

```
$ sudo enas_ndstatus nas-01

--Node Status--
NNC0(DF-H-nnc0)
Node name    : nas-01
Node status   : INACTIVE
```

2. Execute the `enas_ndstart` command to start the node.

```
$ sudo enas_ndstart nas-01
```

3. Execute the `enas_ndstatus` command to confirm that the node is running correctly.

   Confirm that `Node status` is `UP`.

```
$ sudo enas_ndstatus nas-01

--Node Status--
NNC0(DF-H-nnc0)
Node name    : nas-01
Node status   : UP
```

### 5.4.7 Viewing the status of resource group(s)

A system administrator can use a command to view the status of the specified resource group.

The following procedure shows how to view the status of resource group(s). The procedure assumes that you as a system administrator will view the status of the resource groups on both nodes that make up the cluster. To view the status of resource groups:

Execute the `enas_rgstatus` command to view the status of the resource groups.

```
$ sudo enas_rgstatus

--Resource Group Status--
Resource group name   : nas-02
Resource group status  : Online/No error
Running node       : nas-02

Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-01
```

### 5.4.8 Stopping and Starting a Resource Group

A system administrator can use commands to start or stop an NFS share, a CIFS share, and other services provided by a resource group for each resource group.

Note that if a resource group is to be started when an NFS share has been created, the NFS service must be running.

#### 5.4.8.1 Stopping a Resource Group

A system administrator can use commands to stop a resource group.

The following procedure shows how to stop a resource group. The procedure assumes that `nas-01` is the name of the resource group to be stopped.

To stop a resource group:

1. Execute the `enas_rgstatus` command to view the status of the target resource group.

   Confirm that `Resource group status` is `Online/No error`, `Online Ready/No error`, or `Online Maintenance/No error`.

```
$ sudo enas_rgstatus nas-01

--Resource Group Status--
Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-01
```

2. Execute the `enas_rgstop` command to stop the resource group.

```
$ sudo enas_rgstop nas-01
```

3. Execute the `enas_rgstatus` command to confirm that the resource group is stopped.

   Confirm that `Resource group status` is `Offline/No error`.

```
$ sudo enas_rgstatus nas-01

--Resource Group Status--
Resource group name   : nas-01
Resource group status  : Offline/No error
Running node       :
```

#### 5.4.8.2 Starting a resource group

A system administrator can use commands to start a resource group.

The following procedure shows how to start a resource group. The procedure assumes that `nas-01` is the name of the resource group to be started.

To start a resource group:

1. Execute the `enas_clstatus` command to confirm that the status of the cluster, nodes, and resource groups are as follows:
   - `Cluster status` is `ACTIVE`.
   - `Node status` of the node that contains the resource group to be started is `UP`.
   - `Resource group status` of the resource group to be started is `Offline/No error` or `Online Ready/No error`.

```
$ sudo enas_clstatus

--Cluster Status--
Cluster name  : nas-cluster01
Cluster status : ACTIVE

--Node Status--
NNC2(DF-H-nnc2)
Node name    : nas-02
Node status   : UP

NNC0(DF-H-nnc0)
Node name    : nas-01
Node status   : UP

--Resource Group Status--
Resource group name   : nas-02
Resource group status  : Online/No error
Running node       : nas-02

Resource group name   : nas-01
Resource group status  : Offline/No error
Running node       :
```

2. Execute the `enas_rgstart` command to start the target resource group.

   If many resources have been registered, it may take tens of minutes until the resource group is placed in the `Online/No error` status and becomes available.

```
$ sudo enas_rgstart nas-01
```

3. Execute the `enas_rgstatus` command to confirm that the resource group is running correctly.

   Confirm that `Resource group status` is `Online/No error`.

```
$ sudo enas_rgstatus nas-01

--Resource Group Status--
Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-01
```

### 5.4.9 Performing a Forced Stop for a Resource Group

If an error occurs while a resource group is being stopped or started and processing cannot be continued, a system administrator can use commands to stop the resource group forcibly.

If a temporary error occurs while a cluster, node, or resource group is being stopped or started, a forced stop followed by a restart may be able to correct the error. If the error cannot be corrected after repeated attempts, the system administrator must determine the cause of the error from the error information and take corrective measures. For details on the corrective measures for an error that occurs while a cluster, node, or resource group is being stopped or started, see Chapter 9.

Some services may remain running after a forced stop. This is because the system ignores any services affected by the error when completing the stop processing. If you start a resource group while some services remain running, two services with the same name may start. To prevent such a problem, do not start a resource group after a forced stop until the cluster or both nodes in the cluster have started. Performing a forced stop for a cluster may take an extended period of time.

The following procedure shows how to stop a resource group forcibly. The procedure assumes that `nas-01` is the name of the resource group to be stopped forcibly.

To stop a resource group forcibly:

1. Execute the `enas_rgstatus` command to view the status of the resource group.

   Confirm that `Resource group status` is not `Offline/No error`.

```
$ sudo enas_rgstatus nas-01

--Resource Group Status--
Resource group name   : nas-01
Resource group status  : Online/srmd executable error
Running node       : nas-01
```

2. Execute the `enas_rgstop` command to stop the resource group forcibly.

   All errors occurring during the processing are ignored, and the resource group stops.

```
$ sudo enas_rgstop -f nas-01
```

3. Execute the `enas_rgstatus` command to confirm that the resource group is stopped.

   Confirm that `Resource group status` is `Offline/No error`.

```
$ sudo enas_rgstatus nas-01

--Resource Group Status--
Resource group name   : nas-01
Resource group status  : Offline/No error
Running node       :
```

### 5.4.10 Changing the Execution Node of a Resource Group

A system administrator can use commands to perform a failover or failback that changes the resource group execution node for node maintenance or troubleshooting.

To change the resource group execution node when an NFS share has been created, the NFS service must be running on the other node, which will become the execution node.

The following procedure shows how to change the resource group execution node. The procedure assumes that `nas-01` is the name of the resource group for which the execution node will be changed.

To change the resource group execution node:

1. Execute the `enas_clstatus` command to view the status of the node that will become the resource group execution node and the status of the target resource group.

   Confirm that the node status and the resource group status are as follows:

   - `Node status` of the node that will become the execution node is `UP`.

   `Resource group status` of the target resource group is `Online/No error` or `Online Maintenance/No error`.

```
$ sudo enas_clstatus

--Cluster Status--
Cluster name  : nas-cluster01
Cluster status : ACTIVE

--Node Status--
NNC2(DF-H-nnc2)
Node name    : nas-02
Node status   : UP

NNC0(DF-H-nnc0)
Node name    : nas-01
Node status   : UP

--Resource Group Status--
Resource group name   : nas-02
Resource group status  : Online/No error
Running node       : nas-02

Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-01
```

2. Execute the `enas_rgmove` command to change the resource group execution node.

   If many resources have been registered, it may take tens of minutes until the processing is completed.

```
$ sudo enas_rgmove nas-01
```

3. Execute the `enas_clstatus` command to confirm that the resource group execution node has been changed.

Confirm that the name of the new resource group execution node is displayed as `Running node` of the target resource group.

```
$ sudo enas_clstatus

...
--Resource Group Status--
...
Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-02
```

### 5.4.11 Disabling and restarting resource group monitoring

A system administrator can use commands to temporarily disable monitoring of a resource group so that a failover does not occur automatically during maintenance of the services provided by the resource group.

#### 5.4.11.1 Disabling resource group monitoring

A system administrator can use commands to disable monitoring of a resource group.

The following procedure shows how to disable monitoring of a resource group. The procedure assumes that `nas-01` is the name of the resource group for which monitoring is to be disabled.

To disable resource group monitoring:

1. Execute the `enas_rgstatus` command to view the status of the resource group for which you want to disable monitoring.

   Confirm that `Resource group status` is `Online/No error`.

```
$ sudo enas_rgstatus nas-01

--Resource Group Status--
Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-01
```

2. Execute the `enas_rgmon` command to disable monitoring of the resource group.

```
$ sudo enas_rgmon -off nas-01
```

3. Execute the `enas_rgstatus` command to confirm that monitoring of the resource group is disabled.

   Confirm that `Resource group status` is `Online Maintenance/No error`.

```
$ sudo enas_rgstatus nas-01

--Resource Group Status--
```

```
Resource group name   : nas-01
Resource group status  : Online Maintenance/No error
Running node       : nas-01
```

### 5.4.11.2 Restarting Resource Group Monitoring

A system administrator can use commands to restart monitoring of a resource group.

The following procedure shows how to restart monitoring of a resource group. The procedure assumes that `nas-01` is the name of the resource group for which monitoring is to be restarted.

To restart resource group monitoring:

1. Execute the `enas_rgstatus` command to view the status of the resource group for which you want to restart monitoring.

   Confirm that `Resource group status` is `Online Maintenance/No error`.

```
$ sudo enas_rgstatus nas-01

--Resource Group Status--
Resource group name   : nas-01
Resource group status  : Online Maintenance/No error
Running node       : nas-01
```

2. Execute the `enas_rgmon` command to restart monitoring of the resource group.

```
$ sudo enas_rgmon -on nas-01
```

3. Execute the `enas_rgstatus` command to confirm that monitoring of the resource group has been restarted.

   Confirm that `Resource group status` is `Online/No error`.

```
$ sudo enas_rgstatus nas-01

--Resource Group Status--
Resource group name   : nas-01
Resource group status  : Online/No error
Running node       : nas-01
```

## 5.5 File System Management using Commands

This section describes how a system administrator can use commands to create, mount, and unmount a file system. It also describes how a system administrator can use commands to manage the warning notification for file system usage and to manage automatic failover when a file system becomes blocked.

### 5.5.1 Before managing a file system

In NAS Manager, you can create a file system from multiple device files. When you use multiple device files, use a logical volume manager (LVM). For NAS Manager, use an LVM as a volume manager.

A SATA drive and an FC drive have different I/O performance levels and processing speeds. The system administrator must carefully consider such factors as the purpose of the file system and drive characteristics to determine the device files to be used for the file system.

Also, before starting management of a file system, the system administrator must check the device file allocation method and the concepts relating to file system capacity.

### 5.5.2 Viewing File System Information

A system administrator can use a command to view information about file systems. If a failover occurs, the system administrator can view the information about file systems on the other node until a failback occurs.

You can also view information on differential-data snapshots created or mounted using NAS Sync Image.

The following procedure shows how to view file system information. The procedure assumes that you as a system administrator will view information about all file systems on the node that you are logged in to.

To view file system information:

1. Execute the `enas_fslist` command to view file system information.

```
$ sudo enas_fslist

List of File Systems:
The number of file systems(1)
 File system(used by)   : nasfs01
 Total disk capacity(GB) : 100.000
 Device status      : normal
 Device files      : lu7B lu7C lu7D lu7E lu7F
 Block used(GB)     : 0.318
 Block free(GB)     : 99.682
 I-node used       : 5
 I-node free       : 104529915
 Volume manager     : use
 Mount status      : rw
 Quota          : on

The number of file systems(2)
 File system(used by)   : nasfs02
...
```

### 5.5.3 Creating a File System

A system administrator can use commands to create a file system.

The number of file systems that can be created for one cluster is 256. However, when a volume manager is used, the number of file systems that can be created for one node is 128. The number of logical volumes that can be created for one node is 4096. Thus, you cannot create a file system when the number of logical volumes reaches the maximum (4096).

The following procedure shows how to create a file system. The procedure assumes that the file system is created under the following conditions:

- The name of the file system to be created is `filesystem01`.
- `/dev/enas/lu1A`, `/dev/enas/lu1B`, and `/dev/enas/lu1C` are used as device files.

To create a file system:

1. Execute the `enas_devfreelist` command to confirm that the device files are unused.

```
$ sudo enas_devfreelist

Device files for use:
 /dev/enas/lu1A FC 20.000GB
 /dev/enas/lu1B FC 20.000GB
 /dev/enas/lu1C FC 20.000GB
 /dev/enas/lu22 FC 10.000GB
 /dev/enas/lu23 FC 10.000GB
...
```

2. Execute the `enas_fscreate` command to create a file system.

```
$ sudo enas_fscreate filesystem01 lu1A,lu1B,lu1C
```

3. Execute the `enas_fslist` command to confirm that the file system has been created correctly.

```
$ sudo enas_fslist filesystem01

List of File Systems:
The number of file systems(1)
 File system(used by)   : filesystem01
 Total disk capacity(GB) : 60.000
 Device status      : normal
 Device files      : lu1A lu1B lu1C
 Block used(GB)     :
 Block free(GB)     :
 I-node used       :
 I-node free       :
 Volume manager     : use
 Mount status      : --
 Quota          : --
```

The created file system is not automatically mounted. The system administrator must use the `enas_fsmount` command to mount the created file system. For details on how to mount a file system, see 5.5.4.

### 5.5.4 Mounting a File System

A system administrator can use commands to mount a file system. A maximum of 256 file systems can be mounted for one cluster. File systems are mounted at the following *mount point* directory:

`/mnt/`***file-system-name***

In a NAS Modular system, mount status is maintained even in the event of failover of the resource group providing the mounted file system services or restart of the services, because the mount information is saved on the disk array. The NAS Modular system allows full-time access to the file system by maintaining the mount status.

The differential-data snapshots created by using NAS Sync Image cannot be mounted. If you want to mount the differential-data snapshots created by using NAS Sync Image, see the manual or *NAS Sync Image Modular User's Guide*.

The following procedure shows how to mount a file system. The procedure assumes that the file system `filesystem01` is to be mounted under the following conditions:

- Permit writing.
- Enable the Quota functionality.

To mount a file system:

1. Execute the `enas_fslist` command to view the mount status of the target file system.

   Confirm that `Mount status` is `--`.

```
$ sudo enas_fslist filesystem01

List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem01
 Total disk capacity(GB) : 60.000
 Device status      : normal
 Device files      : lu1A lu1B lu1C
 Block used(GB)     :
 Block free(GB)     :
 I-node used       :
 I-node free       :
 Volume manager     : use
 Mount status      : --
 Quota          : --
```

2. Execute the `enas_fsmount` command to mount the file system.

```
$ sudo enas_fsmount -w -q on filesystem01
```

3. Execute the `enas_fslist` command to confirm that the file system has been mounted correctly.

```
$ sudo enas_fslist filesystem01

List of File Systems:
The number of file systems(1)
 File system(used by)   : filesystem01
...
 Block used(GB)      : 0.193
 Block free(GB)      : 59.807
 I-node used        : 5
 I-node free        : 62717947
...
 Mount status       : rw
 Quota          : on
```

### 5.5.5 Unmounting a File System

A system administrator can use commands to unmount a file system.

The differential-data snapshots created by using NAS Sync Image cannot be unmounted. If you want to unmount the differential-data snapshots created by using NAS Sync Image, see the manual *NAS Sync Image Modular User's Guide*.

#### 5.5.5.1 Before unmounting a file system

Before unmounting a file system, the system administrator must perform the following tasks:

- Delete all NFS shares and CIFS shares.

  An error occurs if the system administrator attempts to unmount a file system without deleting NFS and CIFS shares. For details about how to delete NFS shares, see 5.6.1.5. For details about how to delete CIFS shares, see 5.6.2.4.

- Inform the clients that use services of the file system to be unmounted that the services will be stopped.

  If a file system is unmounted, the services of the file system are stopped.

- If a NAS Backup Restore license has been set, confirm that a backup or restore operation is not being executed. The system administrator can confirm this by checking the connection between the NDMP server and the backup server, and the connection between the NDMP server and the media server.

  If a file system is unmounted while the file system is being backed up or restored, the backup or restore operation fails.

  For details on how to check the connection between the NDMP server and the backup server, or between the NDMP server and the media server, see the manual *NAS Backup Restore Modular User's Guide*.

#### 5.5.5.2 Unmounting a File System

The following procedure shows how to unmount a file system. The procedure assumes that the file system `filesystem01` is to be unmounted.

To unmount a file system:

1. Execute the `enas_fslist` command to view the mount status of the target file system.

   Confirm that `Mount status` is `rw` or `ro`.

```
$ sudo enas_fslist filesystem01

List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem01
 Total disk capacity(GB) : 60.000
 Device status      : normal
 Device files      : lu1A lu1B lu1C
 Block used(GB)     : 0.193
 Block free(GB)     : 59.807
 I-node used       : 5
 I-node free       : 62717947
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the `enas_fsumount` command to unmount the file system.

```
$ sudo enas_fsumount filesystem01
```

3. Execute the `enas_fslist` command to confirm that the file system has been unmounted correctly.

   Confirm that `Mount status` is `--`.

```
$ sudo enas_fslist filesystem01

List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem01
...
 Block used(GB)     :
 Block free(GB)     :
 I-node used       :
 I-node free       :
...
 Mount status      : --
 Quota          : --
```

### 5.5.6 Deleting a file system

A system administrator can use commands to delete a file system.

Deleting a file system frees the configured device files and makes them available for other purposes.

The file systems for which a differential-data storage device has been set by NAS Sync Image and the differential-data snapshots cannot be deleted. When you want to delete the file systems and the differential-data snapshots described above, see the manual *NAS Sync Image Modular User's Guide*

### 5.5.6.1 Before deleting a file system

Before deleting a file system, the system administrator must perform the following tasks:

- Unmount the file system.

  For details on unmounting a file system, see 5.5.5.

- Delete the copy-destination file system (delete the pair by using ShadowImage ).

  For details on deleting copy-destination file systems, see the manuals for ShadowImage.

- Release the differential-data storage device settings.

  For details on releasing differential-data storage device settings, see the manual *NAS Sync Image Modular User's Guide*.

An attempt to delete a file system without completing these tasks will result in an error.

### 5.5.6.2 Deleting a file system

The following procedure shows how to delete a file system. The procedure assumes that the file system `filesystem01` is to be deleted.

To delete a file system:

1. Execute the `enas_fslist` command to view information about the file system to be deleted.

```
$ sudo enas_fslist filesystem01

List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem01
 Total disk capacity(GB) : 60.000
 Device status      : normal
 Device files      : lu1A lu1B lu1C
 Block used(GB)     :
 Block free(GB)     :
 I-node used       :
 I-node free       :
 Volume manager     : use
 Mount status      : --
 Quota          : --
```

2. Execute the `enas_fsdelete` command to delete the file system.

```
$ sudo enas_fsdelete filesystem01
```

3. Execute the `enas_fslist` command to confirm that the file system has been deleted.

### 5.5.7 Managing the Warning Notifications related to File System Usage

A system administrator can use commands to enable and disable functionality that generates a warning notification if the file system usage exceeds a threshold. The system administrator can also view the warning notification settings.

When the warning notification is enabled, and the file system usage exceeds the warning threshold or reaches the maximum value, messages KAQG90002-W to KAQG90005-W are issued to the SNMP server. When the system is first installed, the warning notification is not enabled.

Note that the following explanations assume that operations are performed in normal mode.

#### 5.5.7.1 Viewing the Warning Motification Settings

A system administrator can use commands to view the warning notification settings.

The following procedure shows how to view the warning notification settings. The procedure assumes that the settings for the file system `filesystem02` are to be viewed.

To view the warning notification settings:

1. Execute the `enas_fsfullmsg` or `enas_fsctl` command to view the warning notification settings.

```
$ sudo enas_fsfullmsg filesystem02

filesystem02   Off(0,0)
```

```
$ sudo enas_fsctl -m filesystem02

filesystem02   Off(0,0)
```

#### 5.5.7.2 Enabling the Warning Notification

A system administrator can use commands to enable functionality that generates a warning notification if the file system usage exceeds a threshold.

The following procedure shows how to enable the warning notification. The procedure assumes that a warning notification is to be generated in either of the following cases:

- When the block usage for the file system (`filesystem02`) exceeds 50 GB
- When the number of used i-nodes for the file system (`filesystem02`) exceeds 50,000

To enable the warning notification:

1. Execute the `enas_fslist` command to confirm that the target file system has been mounted with write permissions set.

   Confirm that `Mount status` is `rw`.

```
$ sudo enas_fslist filesystem02

List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem02
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu7B lu7C lu7D lu7E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the `enas_fsfullmsg` or `enas_fsctl` command to view the warning notification settings.

   Confirm that the file system name is followed by the string `Off`.

```
$ sudo enas_fsfullmsg filesystem02
filesystem02   Off(0,0)
```

```
$ sudo enas_fsctl -m filesystem02
filesystem02   Off(0,0)
```

3. Execute the `enas_fsfullmsg` or `enas_fsctl` command to enable warning notification.

```
$ sudo enas_fsfullmsg -s -o blimit=50G,ilimit=50000 filesystem02
```

```
$ sudo enas_fsctl -m -s -o blimit=50G,ilimit=50000 filesystem02
```

4. Execute the `enas_fsfullmsg` or `enas_fsctl` command to confirm that the warning notification has been set correctly.

   Confirm that the file system name is followed by the string `On`.

```
$ sudo enas_fsfullmsg filesystem02
filesystem02   On(50G,50000)
```

```
$ sudo enas_fsctl -m filesystem02
filesystem02   On(50G,50000)
```

### 5.5.7.3 Disabling the Warning Notification

A system administrator can use commands to disable the functionality that generates a warning notification if the file system usage exceeds a threshold.

The following procedure shows how to disable the warning notification. The procedure assumes that the warning notification for the file system `filesystem02` is to be disabled.

To disable the warning notification:

1. Execute the `enas_fsfullmsg` or `enas_fsctl` command to view the warning notification settings.

   Confirm that the file system name is followed by the string `On`.

```
$ sudo enas_fsfullmsg filesystem02
filesystem02   On(50G,50000)
```

```
$ sudo enas_fsctl -m filesystem02
filesystem02   On(50G,50000)
```

2. Execute the `enas_fsfullmsg` or `enas_fsctl` command to disable the warning notification.

```
$ sudo enas_fsfullmsg -u filesystem02
```

```
$ sudo enas_fsctl -m -u filesystem02
```

3. Execute the `enas_fsfullmsg` or `enas_fsctl` command to confirm that the warning notification has been disabled.

   Confirm that the file system name is followed by the string `Off`.

```
$ sudo enas_fsfullmsg filesystem02
filesystem02   Off(50G,50000)
```

```
$ sudo enas_fsctl -m filesystem02
filesystem02   Off(50G,50000)
```

## 5.5.8 Managing Automatic failover if a File System becomes Blocked

A system administrator can use commands to enable or disable the functionality for automatically performing a failover if a file system is blocked. The system administrator can also view the automatic failover settings. When the system is first installed, automatic failover functionality is not enabled.

### 5.5.8.1 Viewing the Automatic Failover Settings

A system administrator can use commands to view the settings for automatic failover when a file system becomes blocked.

The following procedure shows how to view the settings for automatic failover when a file system becomes blocked. The procedure assumes that the automatic failover settings for the file system `filesystem02` are to be viewed. To view the automatic failover settings:

Execute the `enas_fsautofo` or `enas_fsctl` command to view the automatic failover settings.

```
$ sudo enas_fsautofo filesystem02
filesystem02   Off
```

```
$ sudo enas_fsctl -f filesystem02
filesystem02   Off
```

### 5.5.8.2 Enabling Automatic Failover

A system administrator can use commands to enable the functionality that automatically performs a failover if a file system is blocked.

The following procedure shows how to enable automatic failover when a file system becomes blocked. The procedure assumes automatic failover will occur if the file system `filesystem02` is blocked.

To enable automatic failover:

1. Execute the `enas_fslist` command to confirm that the target file system has been mounted with write permissions set.

   Confirm that `Mount status` is `rw`.

```
$ sudo enas_fslist filesystem02

List of File Systems:
The number of file systems(1)
 File system(used by)   : filesystem02
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu7B lu7C lu7D lu7E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the `enas_fsautofo` or `enas_fsctl` command to view the automatic failover settings.

Confirm that the file system name is followed by the string `Off`.

```
$ sudo enas_fsautofo filesystem02
filesystem02   Off
```

```
$ sudo enas_fsctl -f filesystem02
filesystem02   Off
```

3. Execute the `enas_fsautofo` or `enas_fsctl` command to enable automatic failover.

```
$ sudo enas_fsautofo -s filesystem02
```

```
$ sudo enas_fsctl -f -s filesystem02
```

4. Execute the `enas_fsautofo` or `enas_fsctl` command to confirm that automatic failover has been set correctly.

   Confirm that the file system name is followed by the string `On`.

```
$ sudo enas_fsautofo filesystem02
filesystem02   On
```

```
$ sudo enas_fsctl -f filesystem02
filesystem02   On
```

### 5.5.8.3 Disabling Automatic Failover

A system administrator can use commands to disable the functionality that automatically performs a failover if a file system is blocked.

The following procedure shows how to disable automatic failover when a file system becomes blocked. The procedure assumes that the automatic failover functionality for the file system `filesystem02` is to be disabled.

To disable automatic failover:

1. Execute the `enas_fsautofo` or `enas_fsctl` command to view the automatic failover settings.

   Confirm that the file system name is followed by the string `On`.

```
$ sudo enas_fsautofo filesystem02
filesystem02   On
```

```
$ sudo enas_fsctl -f filesystem02
filesystem02   On
```

2. Execute the `enas_fsautofo` or `enas_fsctl` command to disable automatic failover.

```
$ sudo enas_fsautofo -u filesystem02
```

```
$ sudo enas_fsctl -f -u filesystem02
```

3. Execute the `enas_fsautofo` or `enas_fsctl` command to confirm that automatic failover has been disabled.

   Confirm that the file system name is followed by the string `Off`.

```
$ sudo enas_fsautofo filesystem02
filesystem02   Off
```

```
$ sudo enas_fsctl -f filesystem02
filesystem02   Off
```

### 5.5.9 Managing the Settings for Recording the File Creation Time

In the NAS Modular system, the file creation time can be recorded in the file system separately from the last access time (`atime`), the last change time (`ctime`), and the last modification time (`mtime`). Because this function allows a CIFS client to check the file creation time, compatibility between the NAS Modular system and a CIFS client environment is improved.

***Note:***

When the file system is set so as not to record the file creation time, if a CIFS client checks the attributes of a file, the earliest time among the last access time (`atime`), the last change time (`ctime`), and the last modification time (`mtime`) is displayed as the file creation time. Note that, even if the file system is set so as to record the file creation time, the time cannot be viewed from a NFS client.

A system administrator can use commands to change the settings to enable or disable recording of the time that a file is created for existing file systems. The system administrator can also view the settings.

Note that the following explanations assume that operations are performed in normal mode.

#### 5.5.9.1 Viewing the File Creation Time Settings

A system administrator can use commands to view the file creation time settings.

The following procedure shows how to view the file creation time settings. The procedure assumes that the settings for the file system `filesystem02` are to be viewed. To view the file creation time settings:

Execute the `enas_fsctl` command to view the file creation time settings.

```
$ sudo enas_fsctl -c -o create_time filesystem02
$ sudo enas_fsctl -c filesystem02
Filesystem    Create_time
 filesystem02   Off
```

### 5.5.9.2 Changing the Settings to Enable Recording of the File Creation Time

A system administrator can use commands to change the settings to enable or disable recording of the time that a file is created for existing file systems.

The following procedure shows how to change the settings so that the file creation time is recorded. The procedure assumes that the settings for the file system `filesystem02` will be changed.

To enable recording of the file creation time:

1. Execute the `enas_fslist` command to confirm that the target file system has been mounted with write permissions set.

   Confirm that `Mount status` is `rw`.

```
$ sudo enas_fslist filesystem02

List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem02
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu7B lu7C lu7D lu7E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the `enas_fsctl` command to view the file creation time settings.

   Confirm that the file system name is followed by the string `Off`.

```
$ sudo enas_fsctl -c -o create_time filesystem02

$ sudo enas_fsctl -c filesystem02
Filesystem    Create_time
 filesystem02   Off
```

   Execute the `enas_fsctl` command to change the settings so that the file creation time is recorded.

```
$ sudo enas_fsctl -c -s -o create_time filesystem02
```

4. Execute the `enas_fsctl` command to confirm that the settings have been specified correctly.

   Confirm that the file system name is followed by the string `On`.

```
$ sudo enas_fsctl -c -o create_time filesystem02

$ sudo enas_fsctl -c filesystem02
Filesystem    Create_time
```

```
 filesystem02    On
```

If necessary, execute the `enas_fsctl` command to set the file creation time for all existing files.

The oldest of the last access time (`atime`), the last change time (`ctime`), and the last modification time (`mtime`) is set as the file creation time. If this step is performed for a file system or directory that contains 100,000 files, about one minute is required for the processing to finish.

```
$ sudo enas_fsctl -c -x filesystem02
filesystem02: Wait ............. Success
```

#### 5.5.9.3 Disabling Recording of the File Creation Time

A system administrator can use commands to disable recording of the file creation time.

The following procedure shows how to disable recording of the file creation time. The procedure assumes that recording of the file creation time for the file system `filesystem02` will be disabled.

To disable recording of the file creation time:

1. Execute the `enas_fsctl` command to view the file creation time settings.

   Confirm that the file system name is followed by the string `On`.

```
$ sudo enas_fsctl -c -o create_time filesystem02
Filesystem    Create_time
 filesystem02   On
```

2. Execute the `enas_fsctl` command to disable recording of the file creation time.

```
$ sudo enas_fsctl -c -u -o create_time filesystem02
```

3. Execute the `enas_fsctl` command to confirm that recording of the file creation time has been disabled.

   Confirm that the file system name is followed by the string `Off`.

```
$ sudo enas_fsctl -c -o create_time filesystem02
```

### 5.6 File Share Management using Commands

To enable access over a network to the data stored in a disk array, sharing of the file system and files must be set up based on the NFS or CIFS protocol. File shares allow the NAS Modular system to be used as network attached storage (NAS) so that users on heterogeneous operating systems such as UNIX and Windows can access file systems over their networks.

This section explains how a system administrator can use commands to create NFS and CIFS shares, and change file share attributes.

### 5.6.1 Managing NFS shares

This subsection explains how to manage NFS shares by using commands.

#### 5.6.1.1 Before managing NFS shares

The NAS OS provides two types of settings for NFS shares:

- Settings that do not allow other NFS shares to be created in the directory hierarchy at a higher or lower level than the NFS-shared directory

  This NFS share directory specification is for Solaris, HP-UX, and AIX.

- Settings that allow other NFS shares to be created in the directory hierarchy at a higher or lower level than the NFS-shared directory

  This NFS share directory specification is for Linux.

Before you start a NFS share operation, we recommend that you consider how NFS will be used on a NAS Modular system and NFS clients, and set up an NFS environment for the NAS OS. The system administrator must consider the portability from NFS servers and NAS servers of different models, and change the settings as required. For details on how to set up the NFS environment for the NAS OS, see 5.6.1.6.

Note, however, that if the system administrator sets up NFS shares so that they can be created in a hierarchy, some client operations might be restricted. If one of the following events occurs or the following operation is performed, you will not be able to delete or rename the subdirectory of an NFS-shared directory.

- When an NFS client has mounted a subdirectory of a shared directory, the client machine goes down or is stopped without unmounting the subdirectory
- When an NFS client has mounted a subdirectory of a shared directory, a failover or failback occurs, and then an NFS client unmounts the subdirectory from the node on which the subdirectory was not originally mounted.

In such a case, the system administrator must delete the mount information for the NFS client from the NAS OS. After the system administrator has deleted the mount information from the NAS OS, the subdirectories can be deleted or renamed. For details on how to delete mount information for the NFS client from the NAS OS, see 5.6.1.7.

Note that when the NAS OS is installed for the first time, the settings do not allow NFS shares to be created in a hierarchy. When the NAS OS is updated by installation, the settings for the previous version will be inherited. Also, in version 04-01 or earlier, the settings allow NFS shares to be created in a hierarchy.

#### 5.6.1.2 Viewing Information about NFS shares

A system administrator can use commands to view information about NFS shares.

The following procedure shows how to view information about NFS shares. The procedure assumes that information about all NFS shares on the node is to be viewed. To view information about NFS shares:

Execute the `enas_nfslist` command to view information about NFS shares.

```
$ sudo enas_nfslist

List of File Shares:
The number of NFS share(1)
  Shared directory             : /mnt/fs01/dir01
    Public destination host/network    : host01
    Permission mode / Synchronous writing : rw_sync
    Anonymous mapping           : root_only
    Anonymous UID              : --
    Anonymous GID              : --
    Transmission port restriction     : do_not_perform
    Subtree check              : perform
    Access check with lock request    : do_not_perform

The number of NFS share(2)
  Shared directory             : /mnt/fs01/dir02
    Public destination host/network    : host02
...
```

### 5.6.1.3 Creating an NFS share

A system administrator can use commands to create a maximum of 256 NFS shares per cluster.

If an error occurs during NFS share creation, the previous status is restored. The entered settings do not change if a failover or restart occurs once NFS shares have been created.

When an automatic creation schedule created by NAS Sync Image is set for a file system in which NFS shares have been created, the NFS shares can be automatically created in differential-data snapshots. When automatic NFS share creation is enabled, the NFS shares created in the snapshots inherit attributes from the NFS shares created in the file system. If NAS Sync Image is used, take into account how differential-data snapshots will be used when you create NFS shares.

The following procedure shows how to create an NFS share. The procedure assumes that the NFS share is to be created under the following conditions:

- A new directory is created with the name `/mnt/filesystem01/unit01` as a shared directory (owner: `sys01`, owner group: `unit01`).
- The `/mnt/filesystem01/unit01` directory will be made public only to `host01`.

To create an NFS share:

1. Execute the `enas_fslist` command to confirm that the file system in which you want to create a shared directory has been mounted.

If you want to create an NFS share in a newly created shared directory or with write permissions set, confirm that `Mount status` is `rw`.

```
$ sudo enas_fslist filesystem01

List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem01
 Total disk capacity(GB) : 60.000
 Device status      : normal
 Device files      : lu1A lu1B lu1C
 Block used(GB)     : 0.193
 Block free(GB)     : 59.807
 I-node used       : 5
 I-node free       : 62717947
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the `enas_dircreate` command to create a public directory.

   This step is necessary when you create a new shared directory.

```
$ sudo enas_dircreate -u sys01 -g unit01 /mnt/filesystem01/unit01
```

3. Execute the `enas_dirlist` command to confirm that the shared directory has been created correctly.

   This step is necessary when you have created a new shared directory.

```
$ sudo enas_dirlist -d /mnt/filesystem01/unit01
0755 sys01      unit01      /mnt/filesystem01/unit01
```

4. Execute the `enas_nfscreate` command to create an NFS share.

```
$ sudo enas_nfscreate -d /mnt/filesystem01/unit01 -H host01
```

5. Execute the `enas_nfslist` command to confirm that the NFS share has been created correctly.

```
$ sudo enas_nfslist -d /mnt/filesystem01/unit01

List of File Shares:
The number of NFS share(1)
  Shared directory             : /mnt/filesystem01/unit01
    Public destination host/network    : host01
    Permission mode / Synchronous writing : rw_sync
    Anonymous mapping           : root_only
    Anonymous UID             : --
    Anonymous GID             : --
    Transmission port restriction     : do_not_perform
    Subtree check             : perform
    Access check with lock request    : do_not_perform
```

### 5.6.1.4 Editing information about an NFS share

A system administrator can use commands to edit information about an NFS share.

When an automatic creation schedule created by NAS Sync Image is set for a file system in which NFS shares have been created, the NFS shares can be automatically created in differential-data snapshots. When automatic NFS share creation is enabled, the NFS shares created in the snapshots inherit attributes from the NFS shares created in the file system. If NAS Sync Image is used, take into account how differential-data snapshots will be used when you edit the information about an NFS share.

The following procedure shows how to edit information about an NFS share. The procedure assumes that the information is to be edited under the following conditions:

- An NFS share with write permissions set has been created in the `/mnt/filesystem01/unit01` directory and made public on `host01`.
- The write permissions are removed from the NFS share in the `/mnt/filesystem01/unit01` directory.

To edit information about an NFS share:

1. Execute the `enas_nfslist` command to view the current information about the target NFS share.

```
$ sudo enas_nfslist -d /mnt/filesystem01/unit01

List of File Shares:
The number of NFS share(1)
  Shared directory             : /mnt/filesystem01/unit01
    Public destination host/network    : host01
    Permission mode / Synchronous writing : rw_sync
    Anonymous mapping           : root_only
    Anonymous UID              : --
    Anonymous GID              : --
    Transmission port restriction     : do_not_perform
    Subtree check              : perform
    Access check with lock request    : do_not_perform
```

2. Execute the `enas_nfsedit` command to edit information about the NFS share.

```
$ sudo enas_nfsedit -d /mnt/filesystem01/unit01 -H host01 -p ro
```

3. Execute the `enas_nfslist` command to confirm that information about the NFS share has been changed.

```
$ sudo enas_nfslist -d /mnt/filesystem01/unit01

List of File Shares:
The number of NFS share(1)
  Shared directory             : /mnt/filesystem01/unit01
    Public destination host/network    : host01
    Permission mode / Synchronous writing : ro
...
```

### 5.6.1.5 Deleting an NFS Share

A system administrator can use commands to delete an NFS share.

The following procedure shows how to delete an NFS share. The procedure assumes that an NFS share created in the `/mnt/filesystem01/unit01` directory is to be deleted.

To delete an NFS share:

1. Execute the `enas_nfslist` command to view the current NFS share information.

```
$ sudo enas_nfslist -d /mnt/filesystem01/unit01

List of File Shares:
The number of NFS share(1)
  Shared directory             : /mnt/filesystem01/unit01
    Public destination host/network    : host01
    Permission mode / Synchronous writing : ro
    Anonymous mapping           : root_only
    Anonymous UID              : --
    Anonymous GID              : --
    Transmission port restriction     : do_not_perform
    Subtree check              : perform
    Access check with lock request    : do_not_perform
```

2. Execute the `enas_nfsdelete` command to delete the NFS share that you want to delete.

```
$ sudo enas_nfsdelete -d /mnt/filesystem01/unit01 -a
```

3. Execute the `enas_nfslist` command to confirm that the NFS share has been deleted.

```
$ sudo enas_nfslist
```

### 5.6.1.6 Setting up an NFS environment for the NAS OS

A system administrator can use commands to set up an NFS environment for the NAS OS.

The following procedure shows how to set up an NFS environment for the NAS OS. The procedure assumes that the setting that does not allow other NFS shares to be created for directories at a higher or lower level than the NFS-shared directory is enabled.

Note that both of the nodes in the cluster must have the same NFS environment settings.

To set up an NFS environment for the NAS OS:

1. Ask the administrators of client machines that are using the NFS shares on both nodes to perform the following:
   - Inform the end users that the client machine will stop the service for NFS shares
   - Unmount the directory to which the client is mounted for NFS shares
2. Delete any separate NFS shares that have been created for directories at a higher or lower level than the shared directory.

If you change the settings when separate NFS shares have been created for directories at a higher or lower level than the shared directory, failover or failback can no longer be performed.

3. Execute the 6.2.31 enas_nfs_opt_list (List the NFS environment settings of the NAS OS) command to check the NFS environment information set in the NAS OS.

```
$ sudo enas_nfs_opt_list
nfsd_hierarchical_export = 1
```

4. Execute the 6.2.32

enas_nfs_opt_set (Set an NFS environment for the NAS OS) command to set up the NFS environment in the NAS OS.

```
$ sudo enas_nfs_opt_set nfsd_hierarchical_export=0
```

5. Execute the 6.2.31 enas_nfs_opt_list (List the NFS environment settings of the NAS OS)6.2.31 enas_nfs_opt_list (List the NFS environment settings of the NAS OS) command to confirm that the NFS environment settings have been applied to the NAS OS.

```
$ sudo enas_nfs_opt_list
nfsd_hierarchical_export = 0
```

6. Perform steps 2 to 5 on the other node so that both of the nodes in the cluster have the same settings.
7. If the NFS client failed to unmount the shared directory in step 1, restart the NFS client machine.
8. Ask the administrator of the client machine to remount the directory.

#### 5.6.1.7 Deleting mount information for an NFS client

If one of the following events occurs or the following operation is performed, when a hierarchical NFS share creation has been enabled, you will not be able to delete or rename the subdirectory of an NFS-shared directory.

- When an NFS client has mounted a subdirectory of a shared directory, the client machine goes down or is stopped without unmounting the subdirectory
- When an NFS client has mounted a subdirectory of a shared directory, a failover or failback occurs, and then an NFS client unmounts the subdirectory from the node on which the subdirectory was not originally mounted.

For this problem, a system administrator needs to use commands to delete the mount information for an NFS client from the NAS OS.

*Note*

If you delete the mount information for an NFS client on which NFS-shared subdirectories have been mounted correctly, the NFS client can no longer access file shares (`ESTALE` error).

When you want to delete not only mount information from the NAS OS, but also mounted directories themselves, delete their subdirectories first. If you delete the directories first, you can no longer delete the subdirectories.

The following procedure shows how to delete mount information for an NFS client from the NAS OS. The execution example of the procedure assumes that the NFS client host (host name: `ClientHost`) has stopped the system without unmounting the directory (`/mnt/FS_1/share01`).

1. Execute the 6.2.30

enas_nfs_mount_list (List mount information for an NFS client host) command on both nodes in the cluster to check the mount information for the directories on the nodes.

On the node for which mount information is displayed, perform steps 2 and 3. You only have to perform these steps on the node for which mount information is displayed.

```
$ sudo enas_nfs_mount_list -c ClientHost
client:         directory:
ClientHost       /mnt/FS_1/share01
```

2. Execute the 6.2.29

enas_nfs_mount_del (Delete mount information for an NFS client host) command to delete the mount information for the NFS client from the NAS OS.

```
$ sudo enas_nfs_mount_del -c ClientHost /mnt/FS_1/share01
```

3. Execute the 6.2.30

enas_nfs_mount_list (List mount information for an NFS client host)6.2.30

enas_nfs_mount_list (List mount information for an NFS client host) command to confirm that the mount information has been deleted.

#### 5.6.1.8 Deleting the File Lock information for an NFS Client Host

A system administrator can use a command to delete file lock information that remains on the NAS OS for some reason, such as an error on an NFS client host or on the network. Use the procedure described below if an NFS client machine that holds file lock information has terminated abnormally and cannot restart for some reason.

*Notes*

When a file is locked normally by an NFS client, if the NFS file lock information is deleted from the NAS Modular system, the lock on the file is lost, leaving the file vulnerable to damage.

After deleting file lock information that has remained on the NAS OS because of a network error occurring while an NFS client host was normally operating, restart the NFS client host before reconnecting the client to the network.

The following procedure shows how to delete file lock information for an NFS client host from the NAS OS. The procedure assumes that file lock information for the NFS client host `ClientHost` is to be deleted. To delete file lock information:

Execute the `enas_nfs_locks_clear` command to delete the file lock information for the target NFS client host. A confirmation message is output that prompts you to confirm the deletion of the file lock information. Type `y` to delete the information, or `n` to cancel.

```
$ sudo enas_nfs_locks_clear ClientHost
Do you really want to clear locks held for ClientHost (y/n)?y
```

### 5.6.2 Managing CIFS shares

This section explains how to manage CIFS shares by using commands.

#### 5.6.2.1 Viewing information about CIFS shares

A system administrator can use a command to view CIFS share information.

The following procedure shows how to view CIFS share information. The procedure assumes that information about all CIFS shares on the node is to be viewed. To view CIFS share information:

Execute the `enas_cifslist` command to view CIFS share information.

```
$ sudo enas_cifslist

List of File Shares:
The number of CIFS share(1)
 Name of file share      : cifs1
 Shared directory       : /mnt/fs01/dir1
 Use ACL            : not_use
```

```
 Server specification     : --
 Comment for file share    :
 Permission mode        : rw
 Browse permission       : permit
 File access permissions    : rw,ro,ro
 Directory access permissions : rw,ro,ro

The number of CIFS share(2)
 Name of file share      : cifs2
 Shared directory       : /mnt/fs01/dir2
...
```

### 5.6.2.2 Creating a CIFS share

A system administrator can use commands to create a maximum of 256 CIFS shares per cluster.

When an automatic creation schedule created by NAS Sync Image is set for a file system in which CIFS shares have been created, the CIFS shares can be automatically created in differential-data snapshots. When automatic CIFS share creation is enabled, the CIFS shares created in the snapshots inherit attributes from the CIFS shares created in the file system. If NAS Sync Image is used, take into account how differential-data snapshots will be used when you create CIFS shares.

Notes:

The attributes of directories for the mount point of a file system are:

- Owner: The `root` who has read and write permissions
- Group: The `root` who has read-only permission
- Others: Users who have read-only permission

Therefore, if a CIFS shared directory is specified for the mount point, change the permissions to enable users to use the CIFS shared directory.

The following procedure shows how to create a CIFS share. The procedure assumes that the CIFS share is to be created under the following conditions:

- A new directory is created with the name `/mnt/filesystem02/unit10` as a shared directory (owner: `sys02`, owner group: `unit10`).
- `user00` is not allowed to write data to the CIFS share.
- A new CIFS share is created with the name `unit10`.

To create a CIFS share:

1. Execute the `enas_fslist` command to confirm that the file system in which you want to create a shared directory has been mounted.

   If you want to create a CIFS share in a newly created shared directory or with write permissions set, confirm that `Mount status` is `rw`.

```
$ sudo enas_fslist filesystem02
```

```
List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem02
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu7B lu7C lu7D lu7E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the `enas_dircreate` command to create a shared directory.

   This step is necessary when you create a new shared directory. Before all the information of the CIFS share has been applied, it is possible that another user could write data to the CIFS share. For this reason, we recommend that you create a shared directory with permission settings that permit only the owner to write, create a CIFS share, and then set write permissions for the shared directory

```
$ sudo enas_dircreate -u sys02 -g unit10 -m 700
/mnt/filesystem02/unit10
```

3. Execute the enas_dirlist (List directory attributes) command to confirm that the shared directory has been created correctly. This step is necessary when you have created a new shared directory.

```
$ sudo enas_dirlist -d /mnt/filesystem02/unit10
0700 sys02      unit10      /mnt/filesystem02/unit10
```

4. Execute the `enas_cifscreate` to create a CIFS share.

```
$ sudo enas_cifscreate -x unit10 -f rw,rw,rw -F rw,rw,rw -d
/mnt/filesystem02/unit10
```

   Execute the `enas_cifslist` command to confirm that the CIFS share has been created correctly.

```
$ sudo enas_cifslist -x unit10 –v

List of File Shares:
The number of CIFS share(1)
 Name of file share      : unit10
 Shared directory       : /mnt/filesystem02/unit10
 Use ACL            : not_use
 Server specification     : --
 Comment for file share    :
 Permission mode        : rw
 Browse permission       : permit
 File access permissions    : rw,ro,ro
 Directory access permissions : rw,ro,ro
 Write disallowed users    : user00
 Write disallowed groups    : --
```

```
 Write allowed users      : --
 Write allowed groups     : --
```

6. Execute the `enas_diredit` command to change the attributes of the shared directory.

```
$ sudo enas_diredit -m 777 /mnt/filesystem02/unit10
```

Execute the `enas_dirlist` command to confirm that the attributes of the shared directory have been changed.

```
$ sudo enas_dirlist -d /mnt/filesystem02/unit10
```

### 5.6.2.3 Editing information about a CIFS share

A system administrator can use commands to edit information about a CIFS share.

When an automatic creation schedule created by NAS Sync Image is set for a file system in which CIFS shares have been created, the CIFS shares can be automatically created in differential-data snapshots. When automatic NFS share creation is enabled, the CIFS shares created in the snapshots inherit attributes from the CIFS shares created in the file system. If NAS Sync Image is used, take into account how differential-data snapshots will be used when you edit the information about a CIFS share.

The following procedure shows how to edit information about a CIFS share. The procedure assumes that the information is to be edited under the following conditions:

- The name of the CIFS share whose attributes are to be changed is `unit10`.
- The attributes are changed to permit end users to view and specify ACL settings.

To edit information about a CIFS share:

1. Execute the `enas_cifslist` command to view the current information about the target CIFS share.

```
$ sudo enas_cifslist -x unit10

List of File Shares:
The number of CIFS share(1)
 Name of file share      : unit10
 Shared directory       : /mnt/filesystem02/unit10
 Use ACL            : not_use
 Server specification     : --
 Comment for file share    :
 Permission mode        : rw
 Browse permission       : permit
 File access permissions    : rw,ro,ro
 Directory access permissions : rw,ro,ro
```

2. Execute the `enas_cifsedit` command to edit information about the CIFS share.

```
$ sudo enas_cifsedit -x unit10 -a use
```

3. Execute the `enas_cifslist` command to confirm that information about the CIFS share has been changed.

```
$ sudo enas_cifslist -x unit10

List of File Shares:
The number of CIFS share(1)
 Name of file share      : unit10
...
 Use ACL            : use
...
```

4. If you want to apply the changes immediately, restart the CIFS service.

#### 5.6.2.4 Deleting a CIFS share

A system administrator can use commands to delete a CIFS share.

The following procedure shows how to delete a CIFS share. The procedure assumes that the CIFS share `unit10` is to be deleted.

To delete a CIFS share:

1. Execute the `enas_cifslist` command to view the information about the target CIFS share.

```
$ sudo enas_cifslist -x unit10

List of File Shares:
The number of CIFS share(1)
 Name of file share      : unit10
 Shared directory       : /mnt/filesystem02/unit10
 Use ACL            : use
 Server specification     : --
 Comment for file share    :
 Permission mode        : rw
 Browse permission       : permit
 File access permissions    : rw,ro,ro
 Directory access permissions : rw,ro,ro
```

2. Execute the `enas_cifsdelete` command to delete the CIFS share.

```
$ sudo enas_cifsdelete -x unit10
```

3. Execute the `enas_cifslist` command to confirm that the CIFS share has been deleted.

### 5.6.3 Managing ACL

A system administrator can use commands to manage the ACL settings of the shared directory in which a CIFS share has been created. The ACL of a directory can set directory and file access permissions not only for the owner, owner group, and others, but also for a specific user or group.

There are three types of ACLs:

- Access ACL

  An ACL set for only a specified directory

- Default ACL

  An ACL set for only the files and directories created under a specified directory

- Mask

  An ACL for limiting enabled access permissions to owner group, specific users, specific groups, and others. Normally, you do not need to set this item.

  Note that, if an ACL setting is specified from a CIFS client, full control access permissions are always set for a mask.

An ACL can be set to perform more detailed access control than the directory mode allows.

#### 5.6.3.1 Relationship between CIFS clients and ACLs set on a NAS Modular system

Since ACLs set on a NAS Modular system conform to POSIX, some areas differ from access permissions on CIFS clients. The following explains the relationship between ACLs set on a NAS Modular system, and those of CIFS clients.

ACL types and setup targets

When an ACL is set by using the `enas_dirsetacl` command, the access control contents (**Name** and **Apply to**) displayed in a CIFS client differ depending on the type and setup target of the ACL that has been set.

The following table displays the relationship between the type and setup target of the ACL that has been set, and the contents displayed for access control in CIFS clients.

**Table 5.3 Relationship Between Set ACL and Access Control Contents in CIFS Clients**

| **Contents set in the NAS Modular system** | | **Contents displayed in the CIFS client** | |
|---|---|---|---|
| **ACL type** | **Setup target** | **Contents displayed for** Name | **Contents displayed for** Apply to |
| Access ACL | owner | *owner-name* | **This folder only** |
| | owner group | *owner-group-name* | |
| | other | `Everyone` | |
| | specific user | *user-name* or *comment-set-during-user-registration* | |

| | | | |
|---|---|---|---|
| | specific group | *group-name* | |
| | mask | -- | -- |
| Default ACL | owner | `CREATOR OWNER` | **Subfolders and files only** |
| | owner group | `CREATOR GROUP` | |
| | other | `Everyone` | |
| | specific user | *user-name* or *comment-set-during-user-registration* | |
| | specific group | *group-name* | |
| | mask | -- | -- |

Legend: --: Nothing is displayed.

***Note:***

When the same permissions are set for the access ACL and default ACL for a specific user, specific group, or other, **This folder, subfolders and files** is displayed for **Apply to**.

Permission settings

For the ACL set by the `enas_dirsetacl` command, the information displayed as access permissions on a CIFS client differs depending on the specified permission.

The following table shows the relationship between the permissions set and the displayed contents of the access permissions for CIFS clients.

**Table 5.4 Relationship Between Set and Access Permissions Contents for CIFS Clients**

| Details about access permissions displayed for CIFS clients | Permissions set | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 7(rwx) | 6(rw) | 5(rx) | 4(r) | 3(wx) | 2(w) | 1(x) | 0(-) |
| **Traverse Folder/Execute File** | Yes | No | Yes | No | Yes | No | Yes | No |
| **List Folder/Read Data** | Yes | Yes | Yes | Yes | No | No | No | No |
| **Read Attributes** | Yes | Yes | Yes | Yes | No | No | No | No |
| **Read Extended Attributes** | Yes | Yes | Yes | Yes | No | No | No | No |
| **Create Files/Write Data** | Yes | Yes | No | No | Yes | Yes | No | No |
| **Create Folders/Append Data** | Yes | Yes | No | No | Yes | Yes | No | No |
| **Write Attributes** | Yes | Yes | No | No | Yes | Yes | No | No |
| **Write Extended Attributes** | Yes | Yes | No | No | Yes | Yes | No | No |
| **Delete Subfolders and Files** | Yes | No | No | No | No | No | No | No |
| **Delete** | Yes | No | No | No | No | No | No | No |
| **Read Permissions** | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| **Change Permissions** | Yes | No | No | No | No | No | No | No |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Take Ownership** | Yes | No | No | No | No | No | No | No |

Legend: Yes: permitted No: not permitted

### 5.6.3.2 Viewing ACL settings

A system administrator can use commands to view ACL settings for a shared directory in which a CIFS share has been created.

The following procedure shows how to view ACL settings. The procedure assumes that the ACL settings for the `/mnt/filesystem02/unit10` directory are to be viewed. To view ACL settings:

Execute the `enas_dirgetacl` command to view the ACL settings for the directory.

```
$ sudo enas_dirgetacl /mnt/filesystem02/unit10
# file: /mnt/filesystem02/unit10
# owner: sys02
# group: unit10
user::rwx
group::rwx
other::rwx
```

### 5.6.3.3 Setting an ACL

A system administrator can use commands that set an ACL for a shared directory in which a CIFS share has been created. The ACL can be set for a directory before a CIFS share is created in the directory.

Note that the maximum number of ACL entries for a directory is 128 (that is, a maximum of 64 each for access ACLs and default ACLs).

Note that ACL settings are not inherited by subdirectories and files that are under a subdirectory for which an ACL is set. Use a CIFS client to set ACLs for files and subdirectories that are in a shared directory.

When creating a CIFS share for a directory for which an ACL has been set, if the settings are changed so that the ACL is not used, the ACL settings cannot be viewed and the ACL cannot be set from a CIFS client even though the ACL permissions are still enabled.

The following procedure shows how to set an ACL. The procedure assumes that the ACL is set for the `/mnt/filesystem02/unit10` directory under the following conditions:

- Read and write permissions are granted to the user `user01`.
- Read permissions are granted to the group `unit02`.

To set an ACL:

1. Execute the `enas_fslist` command to confirm that the file system that contains the target directory has been mounted with write permissions set.

Confirm that `Mount status` is `rw`.

```
$ sudo enas_fslist filesystem02

List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem02
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu7B lu7C lu7D lu7E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the `enas_dirsetacl` command to set an ACL.

```
$ sudo enas_dirsetacl -m u:user01:rw,g:unit02:r
/mnt/filesystem02/unit10
```

Execute the `enas_dirgetacl` command to confirm that the ACL has been correctly set for the directory.

```
$ sudo enas_dirgetacl /mnt/filesystem02/unit10

# file: /mnt/filesystem02/unit10
# owner: sys02
# group: unit10
user::rwx
user:user01:rw-
group::rwx
group:unit02:r--
mask::rwx
other::rwx
```

## 5.7 Quota management using commands

The *quota management* functionality sets the maximum amount of disk space available, which prevents specific users from using too much disk space. By using the quota management functionality, you can prevent too much disk space from being used.

This section explains how a system administrator can use commands to manage quotas.

### 5.7.1 Note on managing quotas

Quotas cannot be set for differential-data snapshots that have been created using NAS Sync Image.

### 5.7.2 Managing quotas set for file systems

A system administrator can use commands to limit the block usage and i-node usage available to users or groups for each file system.

This subsection describes how to manage quotas for each file system.

#### 5.7.2.1 Viewing the quota information set for a file system

A system administrator can use commands to view the quota information set for a file system.

The following procedure shows how to view the quota information set for a file system. The procedure assumes that the quota information about the users who use the `filesystem02` file system is to be viewed. To view quota information:

Execute the `enas_quotaget` command to view the quota information.

```
$ sudo enas_quotaget filesystem02

List of Quota Information of File System(filesystem02):
The number of quota information(1)
User name : user01
UID    : 110
Block (MB) Used capacity : 0
      Soft limit  : 1536
      Hard limit  : 2048
      Grace period : -
i-node   Used count  : 0
      Soft limit  : 1275000
      Hard limit  : 1700000
      Grace period : -

The number of quota information(2)
User name : user02
UID    : 111
...
```

### 5.7.3 Setting a user quota for a file system

A system administrator can use commands to set a user quota for a file system. The following procedure shows how to set a user quota for a file system. The procedure assumes that a quota is to be set for the `filesystem02` file system under the following conditions:

- A quota is assigned to the user `sys02`.
- The soft limit on block usage is set to 1.5 GB, and the hard limit is set to 2 GB.

To set a user quota for a file system:

1. Execute the enas_fslist command to confirm that the target file system is mounted with the quota functionality enabled.

Confirm that Quota is on.

```
$ sudo enas_fslist filesystem02

List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem02
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu7B lu7C lu7D lu7E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the enas_quotaset command to set the user quota for the file system.

```
$ sudo enas_quotaset -u sys02 -b 1536,2048 filesystem02
```

3. Execute the enas_quotaget command to confirm that the user quota has been correctly set for the file system.

```
$ sudo enas_quotaget -u sys02 filesystem02
List of Quota Information of File System(filesystem02):
The number of quota information(1)
User name : sys02
UID    : 104
Block (MB) Used capacity : 0
      Soft limit  : 1536
      Hard limit  : 2048
      Grace period : -
i-node   Used count  : 0
      Soft limit  : 0
      Hard limit  : 0
      Grace period : -
```

#### 5.7.3.1 Setting a group quota for a file system

A system administrator can use commands to set a group quota for a file system.

The following procedure shows how to set a group quota for a file system. The procedure assumes that a quota is to be set for the `filesystem02` file system under the following conditions:

- A quota is assigned to the group `unit10`.
- The soft limit on block usage is set to 15 GB, and the hard limit is set to 20 GB.

To set a group quota for a file system:

1. Execute the enas_fslist (List file system information) command to confirm that the target file system is mounted with the quota functionality enabled.

   Confirm that Quota is on.

```
$ sudo enas_fslist filesystem02
List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem02
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu7B lu7C lu7D lu7E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

Execute the enas_quotaset (Set quotas for a file system) command to set the group quota for the file system.

```
$ sudo enas_quotaset -g unit10 -b 15360,20480 filesystem02
```

Execute the enas_quotaget (Display the quota information set for a file system) command to confirm that the group quota has been correctly set for the file system.

```
$ sudo enas_quotaget -g unit10 filesystem02
List of Quota Information of File System(filesystem02):
The number of quota information(1)
Group name : unit10
GID    : 104
Block (MB) Used capacity : 0
      Soft limit  : 15360
      Hard limit  : 20480
      Grace period : -
i-node   Used count  : 0
      Soft limit  : 0
      Hard limit  : 0
      Grace period : -
```

### 5.7.3.2 Setting a quota for user(s)

A system administrator can use commands to set a quota for user(s).

The following procedure shows how to set a quota for user(s). The procedure assumes that a quota is to be set for the `filesystem02` file system under the following conditions:

- A quota is assigned to the user `sys02`.
- The soft limit on block usage is set to 3.5 GB, and the hard limit is set to 4 GB.
- The soft limit on i-node usage is set to 700, and the hard limit is set to 800.

To set a quota for a user:

1. Execute the `enas_fslist` command to confirm that the target file system has been mounted with the quota settings enabled.

   Confirm that `Quota` is `on`. For details on the syntax of the `enas_fslist` command, see Chapter *6*.

```
$ sudo enas_fslist filesystem02
```

2. Execute the `enas_quotaset` command to set quota information for the target user.

   For details on the syntax of the `enas_quotaset` command, see Chapter *6*.

```
$ sudo enas_quotaset -u sys02 -b 3584,4096 -i 700,800
filesystem02
```

3. Execute the `enas_quotaget` command to confirm that the quota information has been correctly set for the user.

   For details on the syntax of the `enas_quotaget` command, see Chapter *6*.

```
$ sudo enas_quotaget -u sys02 filesystem02
```

#### 5.7.3.3 Setting a Quota for Group(s)

A system administrator can use commands to set a quota for group(s).

The following procedure shows how to set a quota for group(s). The procedure assumes that a quota is to be set for the `filesystem02` file system under the following conditions:

- A quota is assigned to the group `unit10`.
- The soft limit on block usage is set to 3 GB, and the hard limit is set to 3.5 GB.
- The soft limit on i-node usage is set to 600, and the hard limit is set to 700.

To set a quota for a group:

1. Execute the `enas_fslist` command to confirm that the target file system has been mounted with the quota settings enabled.

   Confirm that `Quota` is `on`. For details on the syntax of the `enas_fslist` command, see Chapter *6*.

```
$ sudo enas_fslist filesystem02
```

2. Execute the `enas_quotaset` command to set quota information for the target group.

   For details on the syntax of the `enas_quotaset` command, see Chapter *6*.

```
$ sudo enas_quotaset -g unit10 -b 3072,3584 -i 600,700
filesystem02
```

3. Execute the `enas_quotaget` command to confirm that the quota information has been correctly set for the group.

   For details on the syntax of the `enas_quotaget` command, see Chapter *6*.

```
$ sudo enas_quotaget -g unit10 filesystem02
```

#### 5.7.3.4 Setting the default quota for a file system

A system administrator can use commands to set the default quota for a file system.

The following procedure shows how to set the default quota for a file system. The procedure assumes that the default quota is to be set for the `filesystem02` file system. As the default quota, the soft limit on block usage will be set to 1 GB, and the hard limit will be set to 1.5 GB.

To set the default quota:

1. Execute the `enas_fslist` command to confirm that the target file system has been mounted with the quota settings enabled.

   Confirm that `Quota` is `on`.

```
$ sudo enas_fslist filesystem02

List of File Systems:
The number of file systems(1)
 File system(used by)   : filesystem02
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu7B lu7C lu7D lu7E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the `enas_quotaset` command to set the default quota for the file system.

```
$ sudo enas_quotaset -d -b 1024,1536 filesystem02
```

3. Execute the `enas_quotaget` command to confirm that the default quota has been correctly set for the file system.

```
$ sudo enas_quotaget -d filesystem02

Default Quota Information of File System(filesystem02):
Block (MB) Soft limit(default) : 1024
      Hard limit(default) : 1536
i-node   Soft limit(default) : 0
      Hard limit(default) : 0
```

### 5.7.3.5 Setting a Quota grace period for a file system

A system administrator can use commands to set a quota grace period for a file system.

Set a grace period for each file system. The grace period you set applies to all users and groups that use that file system.

If you later change the current grace period, the new setting will not apply to the users or groups which are in the grace period because their i-node usage or block usage has already exceeded the soft limit.

- The following procedure shows how to set a quota grace period for a file system. The procedure assumes that the grace period for block usage is to be set to 10 days for the quota set for the `filesystem02` file system.

To set a grace period:

1. Execute the `enas_fslist` command to confirm that the target file system has been mounted with the quota functionality enabled.

   Confirm that `Quota` is `on`.

```
$ sudo enas_fslist filesystem02

List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem02
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu7B lu7C lu7D lu7E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the `enas_quotaset` command to set the quota grace period for the file system.

```
$ sudo enas_quotaset -t -b 10 -i 10 filesystem02
```

   Execute the `enas_quotaget` command to confirm that the quota grace period has been correctly set for the file system.

```
$ sudo enas_quotaget -t filesystem02

Grace Period Information of File System(filesystem02):
Block grace period : 10 days
i-node grace period : 7 days
```

### 5.7.3.6 Setting the Quota Monitoring method for a file system

A system administrator can use commands to set the monitoring method for a quota set for a file system.

The following procedure shows how to set the monitoring method for a quota set for a file system. The procedure assumes that the monitoring method is to be set for the quota that is set for the `filesystem02` file system under the following conditions:

- Quota monitoring begins at 04:30.
- If users or groups that have exceeded the soft limit or grace period are detected, summary information is sent via an SNMP trap.

To set the quota monitoring times:

1. Execute the `enas_fslist` command to confirm that the target file system is mounted with the quota functionality enabled.

   Confirm that `Quota` is `on`.

```
$ sudo enas_fslist filesystem02

List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem02
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu7B lu7C lu7D lu7E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

   Execute the `enas_quotaset` command to set the monitoring method for the quota set for the file system.

```
$ sudo enas_quotaset -m -s 0430 -n summary filesystem02
```

3. Execute the `enas_quotaget` command to confirm that the monitoring method for the quota set for the file system has been correctly set.

```
$ sudo enas_quotaget -m filesystem02

Monitoring Time of File System(filesystem02):
SNMP notification mode : Use a summary notification
04:30
```

### 5.7.4 Managing subtree quotas

The system administrator can use commands to limit the block usage and i-node usage available to each directory immediately under the mount point, or available to each user or group. You can set quotas for a maximum of 255 directories per file system.

This subsection describes how to manage subtree quotas.

#### 5.7.4.1 Viewing the quota information set for directories

A system administrator can use commands to view the subtree quota or default quota information set for directories.

The following procedure shows how to view the quota information set for directories. The procedure assumes that the quota information set for the directories immediately under the `filesystem03` file system is to be viewed. To view the quota information set for the directories:

Execute the stquota (Display the quota information set for a directory) command to view the quota information.

```
$ sudo stquota filesystem03
*** Report for subtree quotas on file system filesystem03
        Block limits            i-node limits
Directory    Used  Soft  Hard Grace    Used  Soft  Hard Grace
----------------------------------------------------------------------------
dirA   --    0   95G  100G         1    0    0
dirB   --    0  9.0G   10G         1    0    0
dirC   --    0   27G   30G         1    0    0
dirD   --    0    0  5.0G         1    0    0
dirE   --    0    0  7.5G         1    0    0
...
```

### 5.7.4.2 Viewing the user or group quota information set for a directory

A system administrator can use commands to view the user or group quota information set for a directory.

The following procedure shows how to view the user or group quota information set for a directory. The procedure assumes that the user quota information set for the `/mnt/filesystem03/dirA` directory is to be viewed. To view the user or group quota information set for a directory:

Execute the stquotalist (List the user or group quota information set for a directory) command to view the quota information.

```
$ sudo stquotalist filesystem03/dirA
*** Report for subtree user quotas on directory filesystem03/dirA
        Block limits            i-node limits
User      Used  Soft  Hard Grace    Used  Soft  Hard Grace
----------------------------------------------------------------------------
user01  --    0    0  2.0G         0    0    0
user02  --    0    0  2.0G         0    0    0
user03  --    0  4.0G  5.0G         0    0    0
user04  --    0  4.0G  5.0G         0    0    0
user05  --    0    0    0         0    0    0
...
```

### 5.7.4.3 Setting a quota for a directory

A system administrator can use commands to set a quota for a directory.

The following procedure shows how to set a quota for a directory. The procedure assumes that a quota is to be set under the following conditions:

- A new directory is created with the name `/mnt/filesystem03/dir01` as a shared directory, and a quota is to be assigned to this directory (owner: `sys05`, owner group: `unit15`)
- The soft limit on block usage is set to 18 GB, and the hard limit is set to 20 GB.

To set a quota for the directory:

1. Execute the enas_fslist (List file system information) command to confirm that the target file system is mounted with the quota functionality enabled.

   Confirm that `Quota` is `on`.

```
$ sudo enas_fslist filesystem03
List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem03
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu8B lu8C lu8D lu8E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the enas_dircreate (Create a directory) command to create a shared directory.

```
$ sudo enas_dircreate -u sys05 -g unit15 /mnt/filesystem03/dir01
```

3. Execute the enas_dirlist (List directory attributes) command to confirm that the shared directory has been correctly created.

```
$ sudo enas_dirlist -d /mnt/filesystem03/dir01
0755 sys05      unit15      /mnt/filesystem03/dir01
```

4. Execute the stquotaset (Set quotas for directories) command to set the quota for the shared directory.

```
$ sudo stquotaset -b 18432 -B 20480 filesystem03/dir01
```

5. Execute the stquota (Display the quota information set for a directory) command to confirm that the quota has been correctly set for the shared directory.

```
$ sudo stquota filesystem03
*** Report for subtree quotas on file system filesystem03
        Block limits            i-node limits
Directory    Used  Soft  Hard Grace    Used  Soft  Hard Grace
----------------------------------------------------------------------------
dir01   --    0   18G   20G         1    0    0
```

### 5.7.4.4 Setting a user quota for a directory

A system administrator can use commands to set a user quota for a directory.

The following procedure shows how to set a user quota for a directory. The procedure assumes that a user quota is to be set under the following conditions:

- The target directory is `/mnt/filesystem03/dir01`.
- A quota is assigned to user `sys03` and `sys04`.
- The soft limit on block usage is set to 900 MB, and the hard limit is set to 1 GB.

To set a user quota for the directory:

1. Execute the enas_fslist (List file system information)command to confirm that the target file system is mounted with the quota functionality enabled.

   Confirm that `Quota` is `on`.

```
$ sudo enas_fslist filesystem03
List of File Systems:
The number of file systems(1)
 File system(used by)   : filesystem03
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu8B lu8C lu8D lu8E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the stquotaset (Set quotas for directories) command to set a user quota for the directory.

```
$ sudo stquotaset -u -b 900 -B 1024 filesystem03/dir01 sys03
sys04
```

3. Execute the stquota (Display the quota information set for a directory) command to confirm that the user quota has been correctly set for the directory.

```
$ sudo stquota -u filesystem03 sys03 sys04
*** Report for subtree user quotas on file system filesystem03
*** User: sys03
        Block limits            i-node limits
Directory    Used  Soft  Hard Grace    Used  Soft  Hard Grace
--------------------------------------------------------------------------------
dir01   --    0  900M  1.0G         0    0    0

*** User: sys04
        Block limits            i-node limits
Directory    Used  Soft  Hard Grace    Used  Soft  Hard Grace
--------------------------------------------------------------------------------
dir01   --    0  900M  1.0G         0    0    0
```

```
$ sudo stquotalist -u filesystem03/dir01
*** Report for subtree user quotas on directory filesystem03/dir01
        Block limits            i-node limits
User      Used  Soft  Hard Grace    Used  Soft  Hard Grace
-------------------------------------------------------------------------------
sys03   --    0  900M  1.0G          0    0    0
sys04   --    0  900M  1.0G          0    0    0
sys05   --    0    0    0          1    0    0
sys06   --    0  1.0G  2.0G          0    0    0
sys07   --    0  512M  1.0G          0    0    0
...
```

### 5.7.4.5 Setting a group quota for a directory

A system administrator can use commands to set a group quota for a directory.

The following procedure shows how to set a group quota for a directory. The procedure assumes that a group quota is to be set under the following conditions:

- The target directory is `/mnt/filesystem03/dir01`.
- A quota is assigned to group `unit20` and `unit21`.
- The soft limit on block usage is set to 9 GB, and the hard limit is set to 10 GB.

To set a group quota for the directory:

1. Execute the enas_fslist (List file system information) command to confirm that the target file system is mounted with the quota functionality enabled.

   Confirm that `Quota` is `on`.

```
$ sudo enas_fslist filesystem03
List of File Systems:
The number of file systems(1)
 File system(used by)   : filesystem03
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu8B lu8C lu8D lu8E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the stquotaset (Set quotas for directories) command to set the group quota for the directory.

```
$ sudo stquotaset -g -b 9216 -B 10240 filesystem03/dir01 unit20
unit21
```

3. Execute the stquota (Display the quota information set for a directory) command to confirm that the group quota has been correctly set for the directory.

```
$ sudo stquota -g filesystem03 unit20 unit21
*** Report for subtree group quotas on file system filesystem03
*** Group: unit20
        Block limits            i-node limits
Directory    Used  Soft  Hard Grace    Used  Soft  Hard Grace
--------------------------------------------------------------------------------
dir01   --    0  9.0G   10G         0    0    0

*** Group: unit21
        Block limits            i-node limits
Directory    Used  Soft  Hard Grace    Used  Soft  Hard Grace
--------------------------------------------------------------------------------
dir01   --    0  9.0G   10G         0    0    0
```

```
$ sudo stquotalist -g filesystem03/dir01
*** Report for subtree group quotas on directory filesystem03/dir01
        Block limits            i-node limits
Group      Used  Soft  Hard Grace    Used  Soft  Hard Grace
--------------------------------------------------------------------------------
unit15  --    0    0    0         1    0    0
unit20  --    0  9.0G   10G         0    0    0
unit21  --    0  9.0G   10G         0    0    0
unit23  --    0  4.5G  5.0G         0    0    0
unit27  --    0  2.3G  2.5G         0    0    0
...
```

### 5.7.4.6 Setting the default quota for a directory

A system administrator can use commands to set the default quota for a directory.

The following procedure shows how to set the default quota for a directory. The procedure assumes that the default quota is to be set under the following conditions:

- The target directory is `/mnt/filesystem03/dir01`.
- The soft limit on block usage is set to 700 MB, and the hard limit is set to 750 MB.

To set the default quota for a directory:

1. Execute the enas_fslist (List file system information)command to confirm that the target file system is mounted with the quota functionality enabled.

   Confirm that `Quota` is `on`.

```
$ sudo enas_fslist filesystem03
List of File Systems:
The number of file systems(1)
 File system(used by)   : filesystem03
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu8B lu8C lu8D lu8E
```

```
 Block used(GB)      : 0.256
 Block free(GB)      : 79.744
 I-node used        : 5
 I-node free        : 83623931
 Volume manager      : use
 Mount status       : rw
 Quota          : on
```

2. Execute the stquotaset (Set quotas for directories) command to set the default quota for the directory.

```
$ sudo stquotaset -d -b 700 -B 750 filesystem03/dir01
```

3. Execute the stquota (Display the quota information set for a directory) command to confirm that the default quota has been correctly set for the directory.

```
$ sudo stquota -d filesystem03
*** Report for subtree user quotas on file system filesystem03
        Default block limits  Default i-node limits
Directory        Soft  Hard  Soft  Hard
--------------------------------------------------------------------------------
dir01          700M  750M    0    0
```

### 5.7.4.7 Applying a quota to an existing directory

If a quota is to be set for a directory that is being used by a user, the system administrator must use commands to apply the quota to the directories and files under the target directory. When the quota is applied, the i-node usage and block usage for the directories and files under the target directory will be recorded as the quota usage.

The following procedure shows how to apply a quota to an existing directory. The procedure assumes that a quota is to be applied under the following conditions:

- A quota is applied to an existing directory with the name `/mnt/filesystem00/dir01`.
- The soft limit on block usage is set to 18 GB, and the hard limit is set to 20 GB.

To apply a quota to an existing directory:

1. Execute the stquotaset (Set quotas for directories) command to set the size of the target directory.

```
$ sudo stquotaset -b 18432 -B 20480 filesystem00/dir01
```

2. Execute the stquotaset (Set quotas for directories) command to apply the quota to the existing directory.

   The i-node usage and block usage for the directories and files under the target directory will be recorded as the quota usage. When this command is executed for a directory that contains 100,000 files, about 30 seconds is required for the processing to finish.

```
$ sudo stquotaset -x filesystem00/dir01
filesystem00/dir01: Wait ............. Success
```

3. Execute the stquota (Display the quota information set for a directory) command to confirm that the quota has been applied to the existing directory.

```
$ sudo stquota filesystem00
*** Report for subtree quotas on file system filesystem00
        Block limits            i-node limits
Directory    Used  Soft  Hard Grace    Used  Soft  Hard Grace
--------------------------------------------------------------------------------
dir01   --  7.0G   18G   20G       100000    0    0
```

### 5.7.4.8 Setting a quota grace period for a directory

A system administrator can use commands to set a quota grace period for a directory.

There are three types of grace periods for a subtree quota: directory grace period, user grace period, and group grace period. A user grace period applies to all users who use the directory. A group grace period applies to all groups that use the directory. You cannot set different grace periods for individual users or groups.

If you later change the current grace period, the new setting will not be applied to the users or groups that are in the grace period because their i-node usage or block usage has already exceeded the soft limit.

The following procedure shows how to set a quota grace period for a directory. The procedure assumes that a grace period is to be set under the following conditions:

- The target directory is `/mnt/filesystem03/dir01`.
- A user grace period is set.
- The grace period for block usage is set to 10 days.

To set a grace period:

1. Execute the enas_fslist (List file system information)command to confirm that the target file system is mounted with the quota functionality enabled.

   Confirm that `Quota` is `on`.

```
$ sudo enas_fslist filesystem03
List of File Systems:
The number of file systems(1)
 File system(used by)  : filesystem03
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu8B lu8C lu8D lu8E
 Block used(GB)     : 0.256
 Block free(GB)     : 79.744
 I-node used       : 5
 I-node free       : 83623931
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the stquotaset (Set quotas for directories) command to set the quota grace period for the directory.

```
$ sudo stquotaset -t -u -b 10 filesystem03/dir01
```

3. Execute the stquota (Display the quota information set for a directory) command to confirm that the grace period for the quota has been correctly set for the directory.

```
$ sudo stquota -t -u filesystem03
*** Report for subtree user quotas on file system filesystem03
Directory        Block grace time  i-node grace time
--------------------------------------------------------------------------------
dir01               10days        7days
```

### 5.7.4.9 Canceling the quota set for a directory

The system administrator can use commands to cancel a quota set for a directory.

Canceling a quota cancels the following settings:

- Quota set for the directory
- User quota set for the directory
- Group quota set for the directory
- Default quota set for the directory

The following procedure shows how to cancel a quota set for a directory. The procedure assumes that the quota set for the `/mnt/filesystem03/dir01` directory is to be canceled.

To cancel a quota set for a directory:

1. Execute the enas_fslist (List file system information) command to confirm that the target file system is mounted with the quota functionality enabled.

   Confirm that `Quota` is `on`.

```
$ sudo enas_fslist filesystem03
List of File Systems:
The number of file systems(1)
 File system(used by)   : filesystem03
 Total disk capacity(GB) : 80.000
 Device status      : normal
 Device files      : lu8B lu8C lu8D lu8E
 Block used(GB)     : 21.149
 Block free(GB)     : 58.851
 I-node used       : 3247615
 I-node free       : 80376321
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

2. Execute the stquota (Display the quota information set for a directory) command to check the quota information set for the directory.

```
$ sudo stquota filesystem03
*** Report for subtree quotas on file system filesystem03
        Block limits            i-node limits
Directory    Used  Soft  Hard Grace    Used  Soft  Hard Grace
----------------------------------------------------------------------------
dir01   --  7.0G   18G   20G       100000    0    0
```

3. Execute the stquotaset (Set quotas for directories) command to cancel the quota set for the directory.

   When this command is executed for a directory that contains 100,000 files, about 30 seconds is required for the processing to finish.

```
$ sudo stquotaset -r filesystem03/dir01
filesystem03/dir01: Wait ............. Success
```

4. Execute the stquota (Display the quota information set for a directory) command to confirm that the quota set for the directory has been canceled.

## 5.8 Managing user mapping information using commands

A system administrator can use commands to check the ID or name of a user or group mapped using the RID method.

***Note:***

To check LDAP mapping information, download the entire user-mapping information log group from the **List of RAS Information** (Batch-download) window.

The following procedure shows how to check the ID or name of a user or group mapped using the RID method. The procedure assumes that the user ID mapped with the user `User1`, who belongs to the domain `DOMAIN001`, is to be checked. To check user mapping information:

Execute the `enas_umidget` command to check the name or ID assigned by user mapping.

```
$ sudo enas_umidget -u "Domain001\User1"
```

## 5.9 Checking the network settings and connectivity using commands

This section explains how a system administrator can use commands to check the network settings and connectivity.

### 5.9.1 Checking the network settings

A system administrator can use commands to check the network settings.

The following procedure shows how to check the network settings. The procedure assumes that the settings for all network interfaces are to be checked.

To check the network settings:

1. Execute the `enas_netstat` command to view the network settings.

   The displayed information is added to the beginning of the log file. If the addition of information causes the log file to exceed 1 MB, some entries at the end of the log file are deleted so that the log file size does not exceed 1 MB.

```
$ sudo enas_netstat –i
Kernel Interface table
Iface     MTU Met  RX-OK RX-ERR RX-DRP RX-OVR  TX-OK TX-ERR TX-DRP
TX-OVR Flg
agr0     1500  02078250496   0   0 01616205327  0   0   0 BMsmRU
agr1     1500  0 1085569   0   0  0  26421  0   0   0 BMOsmRU
mtp1     1500  0  18816   0   0   0  4270  0   0   0 BMRU
mng1     1500  0 344026   0   0   0 197488  0   0   0 BMRU
gbe1     1500  01137649328   0   0   0894093613  0  0   0 BMsRU
gbe2     1500  0 543161   0   0   0  13211   0  0   0 BMOsRU
gbe3     1500  0940601168   0   0  0722111714   0  0   0 BMsRU
gbe4     1500  0 542408   0   0   0  13210  0   0   0 BMsRU
lo     16436  0499247407   0   0   0499247407   0   0   0 LRU
rdn0     1500  02079336065   0  0 01616231748   0   0   0 BMmRU
rdn0.0002  1500  02077674250   0  0 01616178767   0   0   0 BMmRU
rdn0.0002:0 1500  0   - no statistics available -            BMmRU
stnet0    2016  0 404739   0   0   0 421185   0   0   0 ORU
stnet1    2016  0 619195   0   0   0 621104   0   0   0 ORU
```

2. From the **List of RAS Information** (Batch-download) window, acquire the log file.

   This step is necessary if you want to save the log file output when the `enas_netstat` command is executed. Download all log data to acquire the log files.

*Notes:*

The `enas_eraselog` command can be used to delete log files.

```
$ sudo enas_eraselog
```

### 5.9.2 Checking the connection to a specified host

A system administrator can use commands to check the connection between the NAS Unit that the system administrator is logged in to and a specified host.

The following procedure shows how to check the connection to a specified host. The procedure assumes that the connection to the host `host01` is to be checked.

To check the connection to a specified host:

1. Execute the `enas_ping` command to check the connection to the host specified in the command.

The displayed information is added to the beginning of the log file. If the addition of information causes the log file to exceed 1 MB, some entries at the end of the log file are deleted so that the log file size does not exceed 1 MB.

```
$ sudo enas_ping host01

PING host01 (10.208.151.100): 56 data bytes
64 bytes from 10.208.151.100: icmp_seq=0 ttl=255 time=1.4 ms
64 bytes from 10.208.151.100: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from 10.208.151.100: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=4 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=5 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=6 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=7 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=8 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=9 ttl=255 time=0.3 ms

--- host01 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.3/1.4 ms
```

2. From the **List of RAS Information** (Batch-download) window, acquire the log file and packet dump file.

   This step is necessary if you want to save the log file output when the `enas_ping` command is executed. Download all log files of the network information log group.

***Notes:***

The `enas_eraselog` command can be used to delete log files. For details on the syntax of the `enas_eraselog` command, see Chapter *6*.

```
$ sudo enas_eraselog
```

### 5.9.3 Checking the path that leads to a specified host

A system administrator can use commands to check the path to a specified host from the NAS Unit that the system administrator is logged in to.

The following procedure shows how to check the path to a specified host. The procedure assumes that the path to the host `host01` is to be displayed with IP addresses only.

To check the path to a specified host:

1. Execute the `enas_traceroute` command to view information about the path to the host specified in the command.

   The displayed information is added to the beginning of the log file. If the addition of information causes the log file to exceed 1 MB, some entries at the end of the log file are deleted so that the log file size does not exceed 1 MB.

```
$ sudo enas_traceroute -n host01

traceroute to host01 (10.208.151.100), 30 hops max, 38 byte packets
```

```
 1 10.208.151.100 0.683 ms 0.202 ms 0.123 ms
```

2. From the **List of RAS Information** (Batch-download) window, acquire the log file and packet dump file.

   This step is necessary if you want to save the log file output when the `enas_traceroute` command is executed. Download all log data to acquire the log files.

***Notes:***

The `enas_eraselog` command can be used to delete log files.

```
$ sudo enas_eraselog
```

## 5.10 Managing the FC port using commands

To use a device connected to the FC port on a NAS Unit, make sure that the settings of the FC port and the device are the same. If the settings differ, the NAS Unit may fail to recognize the device.

This section describes how a system administrator can use commands to change the settings of the FC port on an NAS Unit.

### 5.10.1 Before changing the settings of the FC port

When a tape device has been connected, temporarily unregister it. For details on how to do this, see the manual *NAS Backup Restore Modular User's Guide*.

### 5.10.2 Changing the data transfer rate of the FC port

A system administrator can use commands to change the data transfer rate of the FC port on a NAS Unit.

After installation, the data transfer rate of the FC port on a NAS Unit is initially set to 2 Gbps Even when you use a device that supports the automatic negotiation function by connecting it to the FC port, we recommend that you change the setting of the data transfer rate of the device so that it matches the one set for the FC port on the NAS Unit.

***Note:***

For the data transfer rates supported by the device connected to the FC port, see the documentation for the device.

The following procedure shows how to change the data transfer rate of the FC port. The procedure changes the data transfer rate of the FC port from 2 Gbps to 1 Gbps.

To change the data transfer rate of the FC port:

3. Execute the enas_fcparm (Display and change the settings of the FC port) command to check the current data transfer rate of the FC port.

```
$ sudo enas_fcparm –d
  Speed      = 2Gbps
```

Execute the enas_fcparm (Display and change the settings of the FC port) command to change the data transfer rate of the FC port.

```
$ sudo enas_fcparm -s 1
```

Execute the enas_fcparm (Display and change the settings of the FC port) command to confirm that the data transfer rate of the FC port has been changed.

```
$ sudo enas_fcparm -d
  Speed      = 1Gbps
```

Confirm that the NAS Unit and the device connected to the FC port can communicate with each other.

Confirm that:

- Message KAQG35060-I has been output to the system message log.
- The green LED for the FC port is lit.

For the location of the LED, see the documentation for the disk array.

# Chapter 6 Performing NAS Management Tasks Using Commands

This chapter describes commands used in NAS OS and NAS Manager, command formats, and command descriptions.

- Reviewing Command Functions (see section 6.1)
- enas_cifscreate (Create a CIFS Share) (see section 6.2)
- Executing Commands

## 6.1 Reviewing Command Functions

The following table lists the NAS OS and NAS Manager commands by their use:

**Table 6.1 List of Commands**

| Purpose | Command | Description |
|---|---|---|
| Management of public keys used for SSH | enas_rmfile (Delete a specified file) | Deletes a specified file |
| | enas_sshkeyadd (Register a public key) | Registers a public key |
| | enas_sshkeydel (Delete a public key) | Deletes a public key |
| | enas_sshkeylist (List public key information) | Lists public key information |
| Cluster manipulation | enas_clstart (Start a cluster) | Starts a cluster |
| | enas_clstatus (Display cluster status) | Displays cluster status |
| | enas_clstop (Stop a cluster) | Stops a cluster |
| | enas_ndstart (Start a node) | Starts a node |
| | enas_ndstatus (Display node status) | Displays node status |
| | enas_ndstop (Stop a node) | Stops a node |
| | enas_rgmon (Disable and restart resource group monitoring) | Disables and restarts resource group monitoring |
| | enas_rgmove (Change the execution node of a resource group) | Changes the execution node of a resource group |
| | enas_rgstart (Start a resource group) | Starts a resource group |
| | enas_rgstatus (Display resource group status) | Displays resource group status |
| | enas_rgstop (Stop a resource group) | Stops a resource group |

| | | |
|---|---|---|
| Manipulate a file system | enas_devfreelist (List available device files information) | Lists available device files information |
| | enas_fsautofo (Manage the automatic failover functionality used when a file system is blocked) | Manages the automatic failover functionality used when a file system is blocked |
| | enas_fscreate (Create a file system) | Creates a file system |
| | enas_fsctl (Manage an active file system) | Manages an active file system |
| | enas_fsdelete (Delete a file system) | Deletes a file system |
| | enas_fsfullmsg (Manage the warning notification functionality for file system usage) | Manages the warning notification functionality for file system usage |
| | enas_fslist (List file system information) | Lists file system information |
| | enas_fsmount (Mount a file system) | Mounts a file system |
| | enas_fsumount (Unmount a file system) | Unmounts a file system |
| Manipulate a directory | enas_dircreate (Create a directory) | Creates a directory |
| | enas_diredit (Change directory attributes) | Changes directory attributes |
| | enas_dirgetacl (Display ACL information) | Displays ACL information |
| | enas_dirlist (List directory attributes) | Lists directory attributes |
| | enas_dirsetacl (Set ACLs) | Sets ACLs |
| Manipulate an NFS share | enas_nfs_locks_clear (Delete file lock information for an NFS client host) | Deletes file lock information for the NFS client host |
| | enas_nfs_mount_del (Delete mount information for an NFS client host) | Deletes mount information for an NFS client host |
| | enas_nfs_mount_list (List mount information for an NFS client host) | Lists mount information for an NFS client host |
| | enas_nfs_opt_list (List the NFS environment settings of the NAS OS) | Lists the NFS environment settings in the NAS OS |
| | enas_nfs_opt_set (Set an NFS environment for the NAS OS) | Sets the NFS environment for the NAS OS |
| | enas_nfscreate (Create an NFS share) | Creates an NFS share |
| | enas_nfsdelete (Delete NFS shares) | Deletes NFS shares |
| | enas_nfsedit (Edit NFS share information) | Edits NFS share information |
| | enas_nfslist (List NFS share information) | Lists NFS share information |
| Manipulate a CIFS share | enas_cifscreate (Create a CIFS share) | Creates a CIFS share |

| | | |
|---|---|---|
| | enas_cifsdelete (Delete a CIFS share) | Deletes a CIFS share |
| | enas_cifsedit (Edit CIFS share information) | Edits CIFS share information |
| | enas_cifslist (List CIFS share information) | Lists CIFS share information |
| Manage quotas for each file system | enas_quotaget (Display the quota information set for a file system) | Displays the quota information set for a file system |
| | enas_quotaset (Set quotas for a file system) | Sets the quota for a file system |
| Manage subtree quotas | stquota (Display the quota information set for a directory) | Displays the quota information set for a directory |
| | stquotalist (List the user or group quota information set for a directory) | Lists the user or group quota information set for a directory |
| | stquotaset (Set quotas for directories) | Sets the quota for a directory |
| Manage user mapping information | enas_umidget (Check IDs and names mapped using RIDs) | Checks IDs and names mapped using RIDs |
| Check the network settings and communications | enas_eraselog (Delete the logs generated at command execution) | Delete the logs generated at command execution |
| | enas_netstat (Display the network setting information) | Displays the network setting information |
| | enas_ping (Display the connection to a specified host) | Displays the connection to a specified host |
| | enas_traceroute (Display the path that leads to the specified host) | Displays the path that leads to the specified host |
| Manage the FC port | enas_fcparm (Display and change the settings of the FC port) | Displays and changes the settings of the FC port |

## 6.2 enas_cifscreate (Create a CIFS Share)

- **Synopsis**

```
enas_cifscreate -x share-name -d shared-directory [-a
{use|not_use}]
  [-s {make_public|do_not_make_public|allow|deny}
  :hostname[,hostname...]]
  [-c comment] [-b {permit|do_not_permit}] [-p {ro|rw}]
  [-f {ro|rw|none},{ro|rw|none},{ro|rw|none}]
  [-F {ro|rw|none},{ro|rw|none},{ro|rw|none}]
  [-g {allow|disallow|default}]
  [-S {perform|do_not_perform|default}]
  [-C {use|do_not_use|default}]
  [-t {write_permitted_users|owner_only|default}]
```

```
  [-D add:user[,user...]] [-A add:user[,user...]]
enas_cifscreate -h
```

- **Description**

  Creates a CIFS share using the specified attributes.

- **Arguments and Options**

**Table 6.2 enas_cifscreate Arguments and Options**

| Item | Use |
|---|---|
| `-h` | Specify this option if you want to view the command syntax. |
| `-x` *share-name* | Specify a name of the CIFS share that can be referred to by the users.<br>A name of the CIFS share must be a string no longer than 80 characters, and must be unique within the node. If the automatic creation schedule (automatic creation of shares) of NAS Sync Image is used, the CIFS share name can be a maximum of 69 characters. You can use alphanumeric characters, left parentheses ( ( ), right parentheses ( ) ), hyphens ( - ), periods ( . ), at marks (@), and underscores ( _ ). However, you cannot specify periods ( . ) by themselves as in ( . ) or ( . . ), nor can you specify a period ( . ) at the end of a character string, as in (Abc.).<br>In Windows, the entered value is not case sensitive. Specify a name that is unique regardless of whether upper-case or lower-case alphabetic characters are used.<br>`global`, `homes`, and `printers` cannot be specified as a CIFS share name. |
| `-d` *shared-directory* | Specify a shared directory in the `/mnt/`*file-system-name* or `/mnt/`*file-system-name/subdirectory* format. The directory to be specified must already exist. Specify the shared directory so that it is unique within the cluster. Specify 6 to 256 characters for the absolute path of the directory in which you want to create a CIFS share. When the automatic creation schedule (automatic creations of shares) of NAS Sync Image is used, the CIFS shared directory can be a maximum of 241 characters.<br>▪ When specifying a subdirectory under a file system:<br>`/mnt/`*mounted-file-system-name/subdirectory*<br>▪ When specifying the whole of each file system:<br>`/mnt/`*mounted-file-system-name* |
| `-a {use\|not_use}` | Specify whether to allow CIFS clients to view or set ACLs. If you omit this option, it defaults to `not_use`.<br>▪ `use`<br>Specify whether to allow CIFS clients to view or set ACLs. Once you have created a CIFS share, you cannot change this option to not_use, which does not allow CIFS clients to view or set ACLs.<br>▪ `not_use`<br>Specify this option to prohibit CIFS clients from viewing or setting ACLs. |
| `-s {make_public\|do_not_make_public\|allow\|deny}:hostname[, hostname...]` | Specify whether to make the CIFS share public to the host or network specified in hostname. hostname specifies a host name or network name. Specify the host and network names using 1,023 characters or less in total. When you specify multiple hosts or networks, specify the host names or network addresses, separated by commas (,).<br>If you omit this option, it defaults to `make_public` for all hosts and networks.<br>▪ `make_public or allow`<br>Make the CIFS share public to the host or network specified in *hostname*.<br>▪ `do_not_make_public or deny`<br>Do not make the CIFS share public to the host or network specified in *hostname*. You can specify `not` instead of `do_not_make_public` or `deny`.<br>See ***Notes***. |

| Item | Use |
|---|---|
| -c *comment* | Specify a comment no longer than 256 characters for the CIFS share.<br>If you omit this option, no comment is specified.<br>You can use alphanumeric characters, exclamation marks (!), number signs (#), dollar signs ($), ampersands (&), apostrophes ('), left parentheses ( (), right parentheses ()), asterisks (*), plus signs (+), commas (,), hyphens (-), periods (.), forward slashes (/), colons (:), left angle brackets (<), right angle brackets (>), question marks (?), at marks (@), left brackets ( [), back slashes (\), right brackets (]), circumflex (^), underscores (_), grave accents (`), left braces ({), vertical bars (\|), right braces (}), and tildes (~). You cannot specify a space at the beginning or the end of a character string. You cannot specify a backslash (\) at the end of a character string. |
| -b {permit\|do_not_permit} | Specify whether to permit reference to the share name when no writing is permitted. If you omit this option, it defaults to permit.<br>▪ permit<br>Permit reference to the name of the CIFS share.<br>▪ do_not_permit<br>Do not permit reference to the name of the CIFS share. You can specify not instead of do_not_permit. |
| -p {ro\|rw} | Specify access permissions for the CIFS share. If you omit this option, it defaults to rw. If you do not have write permission for the shared file system, select ro. In this case, even if you select rw, ro will be set.<br>▪ ro<br>Do not permit writing to the CIFS share.<br>▪ rw<br>Permit writing to the CIFS share. |
| -f {ro\|rw\|none},{ro\|rw\|none},{ro\|rw\|none} | Specify access permissions, when creating a file in a writable CIFS share, in the following order: the owner, the owner group, then the other users.<br>If the -p option is specified to ro, you can omit this option.<br>If the -p option is omitted or if the -p option is specified to rw and this option is omitted, it defaults to rw,ro,ro.<br>▪ ro<br>Do not permit writing to files.<br>▪ rw<br>Permit writing to files.<br>▪ none<br>Do not grant read or write permission to files. |
| -F {ro\|rw\|none},{ro\|rw\|none},{ro\|rw\|none} | Specify access permissions, when creating a directory in a writable CIFS share, in the following order: the owner, the owner group, then the other users.<br>If the -p option is specified to ro, you can omit this option.<br>If the -p option is omitted or if the -p option is specified to rw and this option is omitted, it defaults to rw,ro,ro.<br>▪ ro<br>Do not permit writing to directories.<br>▪ rw<br>Permit writing to directories |

| Item | Use |
|---|---|
| -g {allow\|disallow\|default} | Specify access permissions for a guest account. If you omit this option, it defaults to default. If the -g option is omitted or the -g option is specified as default, the CIFS default specified in the CIFS service configuration definitions is used. The guest account is regarded as nobody (user ID: 65534) regardless of the CIFS service authentication mode. Therefore, allow access permissions in the CIFS share that guest account users can access as nobody. The guest account cannot be set for the ACL.<br>▪ allow<br>Allows guest account users access to CIFS share.<br>▪ disallow<br>Disallows guest account users access to CIFS share.<br>▪ default<br>Uses the CIFS default specified in the CIFS service configuration definitions. |
| -S {perform\|do_not_perform\|default} | Specify whether to perform synchronous control for writing when a write request is issued from the CIFS client to the CIFS share. If the -S option is omitted or the -S option is specified as default, the CIFS default specified in the CIFS service configuration definitions is used. If the -S option is specified as perform, data reliability improves when an error occurs in the network or the CIFS client, because a flush to disk is performed each time the CIFS client issues a write request. However, performance might deteriorate because a flush to disk occurs each time a write request is issued.<br>Regardless of the setting for this item, data can be saved to the disk when there is a flush to the file to be updated, or when the file is closed.<br>▪ perform<br>Performs synchronous control when a write request is issued from the client to the CIFS share.<br>▪ do_not_perform<br>Does not perform synchronous control when a write request is issued from the client to the CIFS share. You can specify not instead of do_not_perform.<br>▪ default<br>Uses the CIFS default specified in the CIFS service configuration definitions. |
| -C {use\|do_not_use\|default} | Specify whether to allow clients to view or set ACLs. If the -C option is omitted or the -C option is specified as default, the CIFS default specified in the CIFS service configuration definitions is used. If the -C option is specified as use, performance enhances when the updated data in the CIFS share file is cached on the client. If you omit this option, it defaults to default. However, data reliability might deteriorate when an error occurs in the network or the CIFS client.<br>▪ use<br>Updated data in the CIFS share file will be cached on the client.<br>▪ do_not_use<br>Updated data in the CIFS share file will not be cached on the client. You can specify not instead of do_not_use.<br>▪ default<br>Uses the CIFS default specified in the CIFS service configuration definitions. |

| Item | Use |
|---|---|
| -t {write_permitted_users\|owner_only\|default} | Select the users for which you want to permit time-stamp updating for files in the CIFS share. If you omit this option, it defaults to default. If the -t option is omitted or the -t option is specified as default, the CIFS default specified in the CIFS service configuration definitions is used. Specify write_permitted_users if the file is shared by the CIFS service only.<br>▪ write_permitted_users<br>Select this if you want to permit time-stamp updating for all users who are permitted to write to the file. You can specify write instead of write_permitted_users.<br>▪ owner_only<br>Select this if you want to limit time-stamp updating to the file owner only. You can specify owner instead of owner_only.<br>▪ default<br>Specify this to use the CIFS default specified in the CIFS service configuration definitions. |
| -D add:*user*[,*user*...] | Add users or groups for which you do not want to permit writing during access to the CIFS share. When you specify a group, prefix (@) to the group name. Specify users or groups to be added after add:. The users and groups registered by user mapping cannot be specified.<br>This option is enabled when both read and write permissions to the CIFS share are granted (when -p rw is specified). |
| -A add:*user*[,*user*...] | Add users or groups for which you want to permit writing during access to the CIFS share. When you specify a group, prefix (@) to the group name. To specify multiple user names or group names, separate each name with a comma (,). Specify users or groups to be added after add: and separate each name with a comma (,). The users and groups registered by user mapping cannot be specified. If you do not have write permission for the shared file system and specify a user or group, the setting will not take effect.<br>This option is enabled when read-only permission to the CIFS share is granted (when -p ro is specified).<br>If the file system is mounted as read-only, the user and group settings specified in this option will be invalid. Also, if the same user or group is specified in the -A option and the -D option, the content specified for the -A option will take effect. |

***Notes:***

- If **Host access restrictions** is specified in the **CIFS Service Management** window, the settings in the **CIFS Service Management** window are applied to all CIFS shares regardless of the setting specified by the -s option. When you want to set **Host access restrictions** for each CIFS share separately, use the -s option for the enas_cifscreate command or the enas_cifsedit command rather than specifying **Host access restrictions** in the **CIFS Service Management** window.
- When the -s option is used to permit access to a CIFS share, user authentication for CIFS clients is still performed.
- If you specify a host name in *hostname*, edit the /etc/hosts file by using the **Edit System File** window to add the names and IP addresses of all hosts that are to access the CIFS share. If the host names are not added to the /etc/hosts file, access will be denied even if the -s option specifies that access to the CIFS share is permitted. For details about the **Edit System File** window, see section 4.7.11.

  If you specify make_public (or allow) in the /etc/hosts file, add the names and IP addresses of all hosts for which you want to permit access.

If you specify `do_not_make_public` (or `deny, not`) in the `/etc/hosts` file, add the names of all hosts for which you want (and do not want) to permit access. This distinguishes hosts with access permissions from hosts without access permissions.

- The format for specifying a network name in *hostname* is as follows:

  For a network address, specify an IP address (***example:*** `10.203.15.0`).

  For a network range using a netmask, use the following format:

  *network-address*`/`*netmask* (***example:*** `10.203.15.0/255.255.255.0`).

- **Example**

  Use the following command to create the CIFS share `CIFS1` with the following conditions:

  - Specify the shared directory to `/mnt/FS1/dir_case1` (`-d`).
  - Do not permit writing to directories in the CIFS share (`-p`).

  **$ sudo enas_cifscreate -x CIFS1 -d /mnt/FS1/dir_case1 -p ro**

### 6.2.1 enas_cifsdelete (Delete a CIFS Share)

- **Synopsis**

  `enas_cifsdelete -h|-x` *share-name*

- **Description**

  Deletes a CIFS share.

- **Arguments and Options**

  **`-h`**

  Specify this option if you want to view the command syntax.

  **`-x`** ***share-name***

  Specify the name of the CIFS share to be deleted.

- **Example**

  Use the following command to delete the CIFS share `CIFS1`:

  ```
  $ sudo enas_cifsdelete -x CIFS1
  ```

### 6.2.2 enas_cifsedit (Edit CIFS Share Information)

- **Synopsis**

```
enas_cifsedit -x share-name [-X new-share-name] [-a use]
  [-s {default|{make_public|do_not_make_public|allow|deny}
  :[{add|del}:]hostname[,hostname...]
  [:[{add|del}:]hostname[,hostname...]]}]
  [-c comment] [-b {permit|do_not_permit}] [-p {ro|rw}]
  [-f {ro|rw|none},{ro|rw|none},{ro|rw|none}]
  [-F {ro|rw|none},{ro|rw|none},{ro|rw|none}]
  [-g {allow|disallow|default}]
  [-S {perform|do_not_perform|default}]
  [-C {use|do_not_use|default}]
  [-t {write_permitted_users|owner_only|default}]
  [-D {add|del}:user[,user...][:{add|del}:user[,user...]]]
  [-A {add|del}:user[,user...][:{add|del}:user[,user...]]]
enas_cifsedit -h
```

- **Description**

  Updates CIFS share information using the specified attributes.

- **Arguments and options**

**Table 6.3 enas_cifsedit Arguments and Options**

| Item | Use |
|---|---|
| `-h` | Specify this option if you want to view the command syntax. |
| `-x` *share-name* | Specify the name of the CIFS share whose attributes are to be changed. |

| Item | Use |
|---|---|
| -X *new-share-name* | Specify to change the name of the CIFS share.<br>A name of the CIFS share must be a string of no more than 80 characters that is unique within a node. If the automatic creation schedule (automatic creation of shares) of NAS Sync Image is used, the CIFS share name can be a maximum of 69 characters. You can use alphanumeric characters, left parentheses ( ( ), right parentheses ( ) ), hyphens ( - ), periods ( . ), at marks ( @ ), and underscores ( _ ). However, you cannot specify periods ( . ) by themselves as in ( . ) or ( . . ), nor can you specify a period ( . ) at the end of a character string, as in ( Abc. ).<br>In Windows, the entered value is not case sensitive. Specify a name that is unique regardless of whether upper-case or lower-case alphabetic characters are used.<br>global, homes, and printers cannot be specified as a CIFS share name. |
| -a use | Specify to view or set ACLs from CIFS client (you cannot specify the value not_use) . |
| -s {default\|{make_public\|do_not_make_public\|allow\|deny}:[{add\|del}:]*hostname*[,*hostname*...][:[{add\|del}:]*hostname*[,*hostname*...]]} | Specify the hosts or networks permitted to access the CIFS share. You can use a netmask to specify a network address. To specify multiple host names or network addresses, separate each with a comma ( , ). Specify the host and network names using 1,023 characters or less in total. However, if you specify add, specify *hostname* so that the sum of characters for the currently set host and network names and the specified *hostname* will be 1,023 or less. If you omit this option, the current setting information applies.<br>default<br>Make the CIFS share public to all hosts and networks (the default setting).<br>make_public or allow<br>Make the CIFS share public to the host or network.<br>do_not_make_public or deny<br>Do not make the CIFS share public to the host or network. You can specify not instead of do_not_make_public or deny.<br>If you specify make_public (or allow) or do_not_make_public (or deny) without specifying add or del, the setting for whether the CIFS share is made public to the host or network specified in hostname is set. If this occurs, the current setting information is deleted and the new information specified by the executing command is set.<br>If add is specified with make_public (or allow) or do_not_make_public (or deny), the host or network specified in hostname is added to the current setting information. If del is specified with make_public (or allow) or do_not_make_public (or deny), the host or network specified in hostname is deleted from the current setting information. |

| Item | Use |
|---|---|
| | The processing to be used differs depending on the combination specified for make_public (or allow), do_not_make_public (or deny), add, and del.<br>An error occurs if you duplicate a host name with `make_public` (or `allow`), and `do_not_make_public` (or `deny`). The processing to be executed differs depending on the combination specified for `make_public` (or `allow`), `do_not_make_public` (or `deny`), `add`, and `del`.<br>For example, if `host1` and `host2` are allowed to access the CIFS share (`-s make_public:host1,host2`), you must enter the permissions as follows:<br>To allow `host3` and `host4` to access the CIFS share:<br>`-s make_public:add:host3,host4`<br>Specifying the `-s` option as above, the command adds `host3` and `host4` to the hosts permitted to access the CIFS share.<br>To replace `host2` with `host5` among the hosts permitted to access the CIFS share:<br>`-s make_public:add:host5:del:host2`<br>Specifying the `-s` option as above, `host5` is allowed to access the CIFS share and `host2` is prohibited from accessing the CIFS share.<br>To change the settings so that only `host6` is allowed to access the CIFS share:<br>Specify the `-s` option in either of the following ways:<br>`-s make_public:host6`<br>If you specify `make_public` (or `allow`) or `do_not_make_public` (or `deny`) and you do not specify `add` or `del`, all current information about which hosts and networks are granted or denied access to the CIFS share is deleted and the new information is set.<br>Specifying the `-s` option as above, the information about the hosts or networks permitted access (`host1` and `host2`) is deleted and only `host6` is allowed to access the CIFS share.<br>`-s make_public:add:host6:del:host1,host2`<br>Specifying the `-s` option as above, `host6` is allowed to access the CIFS share, and `host1` and `host2` are no longer permitted access.<br>To change the settings so that only `host1` is prohibited from accessing the CIFS share:<br>`-s do_not_make_public:host1`<br>Specifying the `-s` option as above, all information about the hosts and networks granted or denied access to the CIFS share is deleted, and only `host1` is allowed to access the CIFS share.<br>See ***Notes.*** |

| Item | Use |
|---|---|
| -c *comment* | Specify a comment of no more than 256 characters for the CIFS share that can be referred to by the users.<br>If you omit this option, the current setting information applies.<br>You can use alphanumeric characters, exclamation marks (!), number signs (#), dollar signs ($), ampersands (&), apostrophes ('), left parentheses ( (), right parentheses ()), asterisks (*), plus signs (+), commas (,), hyphens (-), periods (.), forward slashes (/), colons (:), left angle brackets (<), right angle brackets (>), question marks (?), at marks (@), left brackets ( [), back slashes (\), right brackets (]), circumflex (^), underscores (_), grave accents (`), left braces ({), vertical bars (\|), right braces (}), and tildes (~). You cannot specify a space at the beginning or the end of a character string. You cannot specify a backslash (\) at the end of a character string. |
| -b {permit\|do_not_permit} | In the CIFS client environment, specify whether to display a CIFS share name in the CIFS share name list. If you omit this option, the current setting information applies.<br>permit<br>Permit reference to the name of the CIFS share.<br>do_not_permit<br>Do not permit reference to the name of the CIFS share. You can specify not instead of do_not_permit. |
| -p {ro\|rw} | Specify access permissions for the CIFS share. If you omit this option, the current setting information applies. If you do not have write permission for the shared file system, select ro. In this case, even if you select rw, ro will be set.<br>ro<br>Do not permit writing to the CIFS share.<br>rw<br>Permit writing to the CIFS share. |
| -f {ro\|rw\|none},{ro\|rw\|none},{ro\|rw\|none} | Specify access permissions when you create a file in the writable CIFS share, in the following order: for the owner, the owner group, then the other users.<br>If the -p option is specified to ro, you can omit this option.<br>If the -p option is specified to rw, or if this option is omitted, the current setting information applies.<br>ro<br>Do not permit writing.<br>rw<br>Permit writing.<br>none |

| Item | Use |
|---|---|
| -F {ro\|rw\|none },{ro\|rw\|none },{ro\|rw\|none } | Specify access permissions when you create a directory in the writable CIFS share, in the following order: for the owner, the owner group, then the other users.<br>If the -p option is specified to ro, you can omit this option.<br>If the -p option is specified to rw, or if this option is omitted, the current setting information applies.<br>▪ ro<br>Do not permit writing to directories.<br>▪ rw<br>Permit writing to directories.<br>▪ none<br>Do not permit writing or reading to directories. |
| -g {allow\|disallow\|default} | Specify access permissions for guest accounts. If the -g option is omitted, the current settings are inherited. If the -g option is specified as default, the CIFS default specified in the CIFS service configuration definitions is used. The guest account is regarded as nobody (user ID: 65534) regardless of the CIFS service authentication mode. Therefore, allow access permissions in the CIFS share that guest account users can access as nobody. The guest account cannot be set for the ACL.<br>▪ allow<br>Allows guest account users access to CIFS share.<br>▪ disallow<br>Disallows guest account users access to CIFS share.<br>▪ default<br>Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** window. |
| -S {perform\|do_not_perform\|default} | Specify whether to perform synchronous control for writing when a write request is issued from a CIFS client to the CIFS share. If the -S option is omitted, the current settings are inherited. If the -S option is specified as default, the CIFS default specified in the CIFS service configuration definitions is used. If the -S option is specified as perform, data reliability improves when an error occurs in the network or the CIFS client, because a flush to disk is performed each time the CIFS client issues a write request. However, performance might deteriorate because a flush to disk occurs each time a write request is issued.<br>Regardless of the setting for this item, data can be saved to the disk when there is a flush to the file to be updated, or when the file is closed.<br>▪ perform<br>Performs synchronous control when a write request is issued from a client to the CIFS share.<br>▪ do_not_perform<br>Does not perform synchronous control when a write request is issued from a client to the CIFS share. You can specify not instead of do_not_perform.<br>▪ default<br>Uses the CIFS default specified in the CIFS service configuration definitions. |

| Item | Use |
|---|---|
| -C {use\|do_not_use\|default} | Specify whether the updated data in the CIFS share file is to be cached on the client. If the -C option is omitted, the current settings are inherited.<br>▪ use<br>Updated data in the CIFS share file will be cached on the client. If the -C option is specified as use, performance enhances if the updated data in the CIFS share file is cached on the client. However, data reliability might deteriorate when an error occurs in the network or the CIFS client.<br>▪ do_not_use<br>Updated data in the CIFS share file will not be cached on the client. You can specify not instead of do_not_use.<br>default<br>Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** window.<br>This option is enabled when both read and write permissions to the CIFS share are granted (when -p rw is specified).<br>To add users or groups to those not permitted to write to the CIFS share, specify add: followed by the user or group names. To delete users or groups from those without write permission, specify del: followed by the user or group names.<br>Also, if the same user or group is specified in the -A option and the -D option, the content specified for the -A option will take effect. |
| -t {write_permitted_users\|owner_only\|default} | Specify the user for whom you want to permit time-stamp updating for files in the CIFS share. If the -t option is omitted, the current settings are inherited. Specify write_permitted_users if the file is shared by the CIFS service only.<br>▪ write_permitted_users<br>Specify this if you want to permit time-stamp updating for all users who are permitted to write to the file. You can specify write instead of write_permitted_users.<br>▪ owner_only<br>Select this if you want to limit time-stamp file updating to the file owner only. You can specify owner instead of owner_only.<br>▪ default<br>Specify this to use the CIFS default specified in the CIFS service configuration definitions. |
| -D {add\|del}:*user*[,*user*...] [:{add\|del}:*user*[,*user*...]] | Add or delete users or groups for which you do not want to permit writing during access to the CIFS share. When you specify a group, prefix (@) to the group name. Specify users or groups to be added after add:. To specify multiple groups or multiple users, separate each name with a comma (,) Specify users or groups to be deleted after del:. The users and groups registered by user mapping cannot be specified. |

| Item | Use |
|---|---|
| -A {add\|del}:*user*[,*user*...][:{add\|del}:*user*[,*user*...]] | Add or delete users or groups for which you want to permit writing during access to the CIFS share. When you specify a group, prefix (@) to the group name. Specify users or groups to be added after add:. To specify multiple groups or multiple users, separate each name with a comma (,). Specify users or groups to be deleted after del:. The users and groups registered by user mapping cannot be specified. If you do not have write permission for the shared file system and specify a user or group, the setting will not take effect.<br>This option is enabled when read-only permission to the CIFS share is granted (when -p ro is specified).<br>To add users or groups to those with write permission, specify add: followed by the user or group names. To delete users or groups from those with write permission, specify del: followed by the user or group names.<br>If the file system is mounted as read-only, the user and group settings specified in this option will be invalid. Also, if the same user or group is specified in the -A option and the -D option, the content specified for the -A option will take effect. |

***Notes:***

- If **Host access restrictions** is specified in the **CIFS Service Management** window, the settings in the **CIFS Service Management** window are applied to all CIFS share regardless of the setting specified by the -s option. When you want to set up **Host access restrictions** for each CIFS share separately, use the -s option for the enas_cifscreate command or the enas_cifsedit command rather than specifying **Host access restrictions** in the **CIFS Service Management** window.
- Even if you specify the -s option to permit access to a CIFS share, user authentication for CIFS clients is performed:
  - If you specify a host name in *hostname*, edit the /etc/hosts file by using the **Edit System File** window to add the names and IP addresses of all hosts that access the CIFS share. If a host name is not added in the /etc/hosts file, access is rejected even if the -s option specifies that access to the CIFS share is permitted. For details about the **Edit System File** window, see section 4.7.11.
  - If you specify make_public (or allow), in the /etc/hosts file add the names and IP addresses of all hosts for which you want to permit access.
  - If you specify do_not_make_public (or deny, not), in the /etc/hosts file add the names and IP addresses of all hosts for which you want to permit access as well as all hosts for which you do not want to permit access. This allows the hosts for which access is permitted to be distinguished from those for which access is not permitted.

  The format for specifying a network name in *hostname* is as follows:
  - When specifying a network address, specify an IP address:

    (***example:*** 10.203.15.0).
  - When specifying a network range by using a netmask, use:

    *network-address*/*netmask* (***example:*** 10.203.15.0/255.255.255.0).

Following is an example of editing the information on the CIFS share `CIFS1` with the following conditions:

a) Permit writing to the CIFS share (`-p`).

b) Add or delete users for which writing to the CIFS share is not permitted (`-D`).

**$ sudo enas_cifsedit -x CIFS1 -p rw -f rw,rw,ro -F rw,rw,ro -D add:USER1,USER2,USER3,USER4,USER5:del:USER6**

### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter.<br>▪ A name that cannot be specified for a CIFS share name was specified. You cannot specify "`global`", "`homes`", or "`printers`" as a CIFS share name, regardless of whether the name is in upper-case or lower-case characters. Specify a correct CIFS share name. |
| 10 | ▪ A name not registered in the system was specified for the argument of an option. Retry specifying a parameter name registered in the system.<br>▪ A name already registered in the system was specified for the argument of an option. Check the name and retry.<br>▪ The specified name of file share is already used by another file share. Specify a unique name of file share.<br>▪ The specified file share does not exist. Display the **List of File Shares** again and specify a name of file share that exists in the list. Acquire all the Management log files if the error occurs again, and inform maintenance personnel.<br>▪ The maximum number of users/groups that can be specified for the Write allowed users/groups or Write disallowed users/groups has been exceeded. Enter a suitable value.<br>▪ Allowing access as a guest account cannot be specified because the CIFS service authentication mode is set to the NT server authentication mode. Do not attempt to allow access as a guest account.<br>▪ This operation cannot be performed because the capacity of the differential-data storage device is insufficient. Resolve the problem by using a NAS Sync Image operation.<br>▪ A value exceeding the maximum size that can be set for the host/network of the `-s` option was specified. Enter a valid value. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | The CIFS file share editing failed. A conflict with another system administrator's operation or an internal error may have occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel. |
| 70 | ▪ An operation cannot be performed because the file system corresponding to the specified directory is defined by the other node in the cluster. Specify a file share corresponding to a file system created on the operating node.<br>▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first.<br>▪ The specified file share does not exist on the operating node. The file share was created on the other node, the resource group is in the OFFLINE state, or the resource group is undergoing failover. Make sure that the following items corresponding to the specified file share are correct: the file system name, and the resource group state. |

| | |
|---|---|
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 98 | Some other error occurred. |
| 99 | ▪ An internal error occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and inform maintenance personnel.<br>▪ The specified operation failed. The file system or device file may be blocked. In the **List of File Systems**, check the state of the file system. If the file system has an error status, inform maintenance personnel. If the file system does not have an error status, acquire all the Management log files and inform maintenance personnel. |

## Example

### To edit the CIFS share information according to the following conditions:

- The name of the CIFS share is `cifs1`.
- Change the settings to allow writing to the CIFS share.
- Deny write operations to the user registered in the user mapping (`DOMAIN01\user100`).

```
$ sudo enas_cifsedit -x cifs1 -p rw -D add:"DOMAIN01\user100"
```

### 6.2.3 enas_cifslist (List CIFS Share Information)

- **Synopsis**

  `enas_cifslist -h|[-x` *share-name*`] [-c] [-v] [-O {1|2|all}]`

- **Description**

  Displays a list of information for the CIFS shares that have been made public on the node you are operating. If the `-x` option is specified, the command only displays information on the specified CIFS share. The information is displayed by CIFS share in ascending order of share names.

**Table 6.4 Information Displayed when enas_cifslist**

| Item | Information Displayed |
|---|---|
| `Name of file share` | Name of the CIFS share that a user can view. |
| Shared directory | Displays the absolute path for the directory where the CIFS share was created. |
| Use ACL | Displays whether end users are allowed to view and set ACLs.<br>`use`<br>End users are allowed to view and set ACLs.<br>`not_use`<br>End users are not allowed to view and set ACLs. |
| Server specification | When specific hosts or networks are allowed to access the CIFS share, `make_public` appears in this item, followed by the specific host names or network addresses.<br>When specific hosts or networks are not allowed to access the CIFS share, `do_not_make_public` appears in this item, followed by the specific host names or network addresses. |
| `Comment for file share` | CIFS share comment that a user can view. The colon ( **:** ) in the comment is displayed even when you specify the `-c` option. |
| `Permission mode` | Access permission for the CIFS share.<br>`ro`<br>Only read permission is granted.<br>`rw`<br>Read and write permissions are granted. |
| `Browse permission` | Displays whether viewing the CIFS share name is permitted.<br>`permit`<br>Viewing the CIFS share name is permitted.<br>`do_not_permit`<br>Viewing the CIFS share name is not permitted. |

| Item | Information Displayed |
|---|---|
| `File access permissions` | Displays the access permissions when a file has been created in the writable CIFS share. The permissions are listed in order for the owner, owner group, and other users. The permissions are separated with commas (`,`).<br>`ro`<br>The file is read-only.<br>`rw`<br>Both read and write permissions are granted for the file.<br>`none`<br>No access permissions are granted for the file. |
| `Directory access permissions` | Displays the access permissions when a directory has been created in a writable CIFS share. The permissions are listed in order for the owner, owner group, and other users. The permissions are separated with commas (`,`).<br>`ro`<br>The directory is read-only.<br>`rw`<br>Both read and write permissions are granted for the directory.<br>`none`<br>No access permissions are granted for the directory. |
| Write disallowed users | Displays users who do not have write permission for the CIFS share. This information appears only when the `-v` option is specified.<br>If no users are prohibited from writing to the CIFS share, `--` appears for this item. |
| Write disallowed groups | Displays groups that do not have write permission for the CIFS share. This information appears only when the `-v` option is specified.<br>Each group name is prefixed with an at mark (@). If no groups are prohibited from writing to the CIFS share, `--` appears for this item. |
| Write allowed users | Displays users who have write permission for the CIFS share. This information appears only when the `-v` option is specified. If no users are allowed to write to the CIFS share, `--` appears for this item. |
| Write allowed groups | Displays groups that have write permission for the CIFS share. This information appears only when the `-v` option is specified.<br>Each group name is prefixed with an at mark (@).<br>If no groups are allowed to write to the CIFS share, `--` appears for this item. |
| Guest account access | Displays whether access to the CIFS share is permitted for guest accounts. This item appears only when `1` or `all` is specified in the `-O` option.<br>`allow`<br>Access is permitted for guest accounts.<br>`disallow`<br>Access is not permitted for guest accounts.<br>`default`<br>The default set in the CIFS service configuration definitions in the **CIFS Service Management** window applies. |

| Item | Information Displayed |
|---|---|
| Synchronous writing | Displays whether synchronous control for writing is performed when a CIFS client issues a write request to the CIFS share. This item appears only when `1` or `all` is specified in the `-O` option.<br>`perform`<br>Synchronous control is performed.<br>`do_not_perform`<br>Synchronous control is not performed.<br>`default`<br>The default set in the CIFS service configuration definitions in the **CIFS Service Management** window applies. |
| CIFS client cache | Displays whether the updated data in the CIFS share file is cached on the client. This item appears only when `1` or `all` is specified in the `-O` option.<br>`use`<br>Updated data is cached on the client.<br>`do_not_use`<br>Updated data is not cached on the client.<br>`default`<br>The default set in the CIFS service configuration definitions in the **CIFS Service Management** window applies. |
| File timestamp changeable | Displays users who can update the time-stamp of files in the CIFS share. This item appears only when `2` or `all` is specified in the `-O` option.<br>`default` appears for this item if the time-stamp parameter is not set individually for each CIFS share (if the default set in the CIFS service configuration definitions in the **CIFS Service Management** window is being used).<br>`write_permitted_users`<br>All users with file write permission are allowed to update a file time-stamp.<br>`owner_only`<br>Only the file owner is allowed to update a file time-stamp.<br>`default`<br>The default set in the CIFS service configuration definitions in the **CIFS Service Management** window applies. |

## Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| `65` | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| `70` | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first.<br>▪ The specified file share does not exist on the operating node. The file share was created on the other node, the resource group is in the OFFLINE state, or the resource group is undergoing failover. Make sure that the following items corresponding to the specified file |

| | |
|---|---|
| | share are correct: the file system name, and the resource group state. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 98 | Some other error occurred. |
| 99 | ▪ An internal error occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and inform maintenance personnel. |

- **Arguments and Options**

  **-h**

  Specify this option if you want to view the command syntax.

  **-x *share-name***

  Specify the name of the CIFS share for which you want to display the information. If you omit this option, the command displays all the information on the CIFS shares that have been made public on the node you are operating.

  **-c**

  Use to display CIFS share information separated with colons (:).

```
Name-of-file-share:Shared-directory: ...
   :
   : (Repeatedly displayed for each CIFS share.)
   :
```

  If you omit this option, information is displayed in a detailed format.

```
List of File Shares:
The number of CIFS share (counter) (1)
 item-name: value
   :
   : (All items are output.)
   :
(One blank line) (2)
   :
   : ((1) through (2) is output for each CIFS share.)
   :
```

  *counter*: This value starts counting from 1, and a number is assigned to each name of the CIFS share.

  *item-name*: An item in Table 6.4 is displayed.

  *value*: The value of an item in Table 6.4 is displayed.

  **-v**

  Specify to display the information for `Write disallowed users, Write disallowed groups, Write allowed users, and Write allowed groups`.

  **-o {1|2|all}**

  Specify which optional information to be displayed. If this option is omitted, optional information is not displayed.

**1**

Specify to display the information for `Guest account access`, `Synchronous writing`, and `CIFS client cache`.

**2**

Specify to display the information for `File timestamp changeable`.

**all**

Specify to display all optional information.

***Note:*** The optional information to be displayed is identical whether you specify `1` or `all`.

- **Examples**
  - To display the information on the CIFS share `CIFS1` by specifying the `-c` option:

```
$ sudo enas_cifslist -x CIFS1 -c -v -O all
CIFS1:/mnt/CIFS1_dir:use:make_public,192.1.2.3:comment:rw:
permit:rw,rw,rw:rw,rw,rw:USER1,USER2:@GROUP1,@GROUP2:--:--:
default:perform:use:owner_only
```

  - To display the information on the CIFS share `CIFS1` without specifying the `-c` option:

```
$ sudo enas_cifslist -x CIFS1 -v -O all
List of File Shares:
The number of CIFS share(1)
 Name of file share      : CIFS1
 Shared directory       : /mnt/CIFS1_dir
 Use ACL            : use
 Server specification     : make_public,192.1.2.3
 Comment for file share    : comment
 Permission mode        : rw
 Browse permission       : permit
 File access permissions    : rw,rw,rw
 Directory access permissions : rw,rw,rw
 Write disallowed users    : USER1,USER2
 Write disallowed groups    : @GROUP1,@GROUP2
 Write allowed users      : --
 Write allowed groups     : --
 Guest account access     : default
 Synchronous writing      : perform
 CIFS client cache       : use
 File timestamp changeable   : owner_only
```

### 6.2.4 enas_clstart (Start a cluster)

#### Synopsis

```
enas_clstart [-h]
```

#### Description

Starts the cluster that contains the node to which you are logged in.

This command can be executed when the cluster is in the `INACTIVE` state.

If you start the cluster with the resource group status in the `Online Ready/No error` state, the resource group also starts automatically. After `enas_clstart` command processing completes, it might take a while until resource group-related operations can be performed (`Online/No error` state).

#### Options and arguments

**`-h`**

Specify this option if you want to view the command syntax.

#### Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| `25` | The cluster status is not `INACTIVE`. Check the cluster status, stop the cluster, and then try again. |
| `34` | The service IP address is not specified in the cluster. Specify one or more service IP addresses in the cluster. |
| `65` | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| `66` | The processing of the failover function has failed. If this message is displayed when performing a manual failover, make sure that the failover-destination node has started. In other cases, check (in all nodes in the cluster) whether a KAQG7*nnnn* message was output to the system messages. If a system message was output, take appropriate action. If you cannot identify the cause, acquire all the Management log files and Cluster log files, and then inform maintenance personnel. |
| `70` | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| `97` | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| `99` | An internal error occurred. Acquire all the Management log files and inform maintenance personnel. |

### Example

**To start the cluster:**

```
$ sudo enas_clstart
```

### 6.2.5 enas_clstatus (Display cluster status)

#### Synopsis

```
enas_clstatus [-c] [--] [cluster-name]
enas_clstatus -h
```

#### Description

Displays the status of the cluster that contains the node you are logged in to.

#### Options and arguments

**-c**

Specify this option if you want to display cluster status information separated by colons (:). When the -c option is specified, any colon (:) contained in the cluster, node, and resource group names is replaced with a number sign (#).

**-h**

Specify this option if you want to view the command syntax.

**--**

Specify this to prevent all of the character string following this option from being treated as an option. For example, if you want to specify -h as the cluster name, specify -- -h.

***cluster-name***

Specify this option to view the status of only the cluster containing the node you are logged in to.

#### Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.5 Information displayed when executing the enas_clstatus command**

| Item | Description |
|---|---|
| --Cluster Status-- | Information about the cluster is displayed. |
| Cluster name | The name of the cluster is displayed. |
| Cluster status | The status of the cluster is displayed.#1<br>ACTIVE<br>The cluster is running normally. |

| | | |
|---|---|---|
| | INACTIVE<br>The cluster is stopped.<br>UNKNOWN#2<br>The status cannot be determined. | |
| --Node Status-- | If you do not specify a cluster name, the command displays the status of the node to which you are logged in and the status of the other node in the cluster, in that order. | |
| *NAS-Unit-name*, *NNC-name* | The NAS Unit name and NNC name are displayed in the following format:<br>*NAS-Unit-name* (*NNC-name*) | |
| Node name | The name of the node is displayed. | |
| Node status | The status of the node is displayed.#1<br>UP<br>The node is running normally.<br>INACTIVE<br>The node is stopped.<br>DOWN<br>The node ended abnormally and has shut down.<br>UNKNOWN#2<br>The status cannot be determined. | |
| --Resource Group Status-- | If you do not specify a cluster name, the command displays the status of the resource group that belongs to the node to which you are logged in and the status of the resource group that belongs to the other node in the cluster, in that order. | |
| Resource group | The name of a resource group is displayed. | |
| Resource group status | The s and error information about a resource group, displayed in the following format:<br>*resource-group-status*/*error-information* | |
| | *resource-group-status* | Online Ready<br>The resource group cannot start because the cluster is inactive, or an error was detected when the cluster was stopping.<br>Initializing<br>The resource group is initializing.<br>Discovery (exclusivity)<br>Online processing is being performed for the resource group, before operations begin.<br>Online Pending<br>The resource group is starting.<br>Online<br>The resource group is active.<br>Online Maintenance<br>Automatic failover is impossible because monitoring is disabled.<br>Offline Pending<br>The resource group is stopping.<br>Offline<br>The resource group is stopped.<br>Internal Error<br>An internal error was detected. Contact the |

| | | |
|---|---|---|
| | | maintenance personnel. |
| | *error-information* | `No error`<br>No errors occurred.<br>`Internal error - not recoverable`<br>An unrecoverable internal error occurred. Contact the maintenance personnel.<br>`Monitor activity unknown`<br>An error occurred during monitoring or while monitoring was being disabled. If you retry operation and the error persists, perform a forced stop and fix the problem.<br>`No available nodes` or `No available nodes in failure domain after monitor failure`<br>An error occurred, but a failover could not be performed because it is already in a failover status. Perform a forced stop and remove the error that caused failover.<br>`Node not available (exclusivity)`<br>Failover is impossible because the `Node status` of the alternate node is not `ACTIVE`. Perform a forced stop and start the alternate node. If you cannot start the alternate node, perform a forced stop for the alternate node and fix the problem.<br>`Node unknown`<br>The resource group cannot be started because the `Node status` of the node is `UNKNOWN`. Perform a forced stop and start the node whose resource group you want to start. If you cannot start the node, perform a forced stop for the node and fix the problem.<br>`Split resource group (exclusivity)`<br>A duplicate resource group is active in the cluster. Perform a forced stop for the cluster, and then ask maintenance personnel to shut down and restart the NAS OS of the NAS Unit in the cluster.<br>`srmd executable error`<br>An error occurred during start or stop processing. Perform a forced stop and fix the problem. |
| `Running node` | The name of the node on which the resource group is running is displayed. | |

#1:

If an error occurs in the NAS Modular system, the status of clusters and nodes might not be displayed. In this case, collect the error information and contact the maintenance personnel.

#2:

If you execute the `enas_clstatus` command while you are logged in to a stopped node, the cluster and the other node are shown as having `UNKNOWN` status, regardless of their actual status. To check the cluster status, the status of the other node, and the resource group status, log on to the active node (the other node), and then re-execute the `enas_clstatus` command.

### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| 26 | The specified cluster does not exist. Specify an existing cluster, and then try again. |
| 65 | Another user is exclusively using a resource of the status display processing, or an exclusively used node has stopped. Wait a while, and then retry. If a processing node stops, wait about 15 minutes or boot the stopped node. |
| 66 | The processing of the failover function has failed. If this message is displayed when performing a manual failover, make sure that the failover-destination node has started. In other cases, check (in all nodes in the cluster) whether a KAQG7*nnnn* message was output to the system messages. If a system message was output, take appropriate action. If you cannot identify the cause, acquire all the Management log files and Cluster log files, and then inform maintenance personnel. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | An internal error occurred. Acquire all the Management log files and inform maintenance personnel. |

### Examples

#### To display cluster, node, and resource group statuses by specifying the `-c` option:

```
$ sudo enas_clstatus -c
ClusterDF8:ACTIVE:NNC2:D730100045:nodennc2:UP:NNC0:D730100041:nodennc
0:UP:nodennc2:Online/No error:nodennc2:nodennc0:Online/No
error:nodennc0
```

#### To display cluster, node, and resource group statuses without specifying the `-c` option:

```
$ sudo enas_clstatus

--Cluster Status--
Cluster name  : ClusterDF8
Cluster status : ACTIVE

--Node Status--
```

```
NNC2(D730100045)
Node name    : nodennc2
Node status   : UP

NNC0(D730100041)
Node name    : nodennc0
Node status   : UP

--Resource Group Status--
Resource group name   : nodennc2
Resource group status  : Online/No error
Running node       : nodennc2

Resource group name   : nodennc0
Resource group status  : Online/No error
Running node       : nodennc0
```

**To display only the status of the `ClusterDF8` cluster by specifying the `-c` option:**

```
$ sudo enas_clstatus -c ClusterDF8
ClusterDF8:ACTIVE
```

**To display only the status of the `ClusterDF8` cluster without specifying the `-c` option:**

```
$ sudo enas_clstatus ClusterDF8


--Cluster Status--
Cluster name  : ClusterDF8
Cluster status : ACTIVE
```

### 6.2.6 enas_clstop (stop a cluster)

- **Synopsis**

  `enas_clstop -h|[-x share-name] [-f] [-h]`

- **Description**

  Stops the cluster that contains the node to which you are logged in.

You can execute this command when the cluster and resource group have the following statuses:

- The cluster status is `ACTIVE`.
- The resource group status is `Online/No error`, `Offline/No error`, or `Online Maintenance/No error`.

#### Options and arguments

**`-f`**

Specify this option if you want to forcibly stop the cluster. If an error occurs during a cluster startup or stop operation and prevents processing from continuing, you can forcibly stop the cluster by executing this command with the `-f` option specified.

**`-h`**

Specify this option if you want to view the command syntax.

#### Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| `24` | The cluster status is not `ACTIVE`. Check the cluster status, start the cluster, and then try again. |
| `65` | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| `66` | The processing of the failover function has failed. If this message is displayed when performing a manual failover, make sure that the failover-destination node has started. In other cases, check (in all nodes in the cluster) whether a KAQG7*nnnn* message was output to the system messages. If a system message was output, take appropriate action. If you cannot identify the cause, acquire all the Management log files and Cluster log files, and then inform maintenance personnel. |
| `70` | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| `97` | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |

| | |
|---|---|
| 99 | An internal error occurred. Acquire all the Management log files and inform maintenance personnel. |

## Examples

### To stop the cluster:

```
$ sudo enas_clstop
```

### To forcibly stop the cluster:

```
$ sudo enas_clstop -f
```

### 6.2.7 enas_devfreelist (List available device files information)

- **Synopsis**

  ```
  enas_devfreelist [-h]
  ```

- **Description**

  Displays information about device files that are not in use. The information appears in ascending order of the device file paths. No information appears for failed device files.

**Table 6.6 Information Displayed when enas_devfreelist Command is Used**

| Item | Displayed Information |
|---|---|
| *Device- file -path* | Displays the path of the device file.<br>`/dev/enas/lu`*XX*<br>(where *XX* is a hexadecimal number) |
| *Drive- type* | Displays the drive types.<br>SATA<br>Displayed if the drive type is SATA<br>FC<br>for an FC device). |
| *Device- file -capacity* | *Device file capacity in GB.*<br>*device-file-capacityGB* |

- **Arguments and Options**

  **-h**

  Use to output the command format to the standard error.

  Specify this option if you want to view the command syntax.

- **Example**

  To display the information on available device files:

```
$ sudo enas_devfreelist -d
Device files for use:
 /dev/enas/lu02 FC 20.000GB
 /dev/enas/lu03 FC 20.000GB
 /dev/enas/lu04 FC 20.000GB
 /dev/enas/lu12 SATA 10.000GB
 /dev/enas/lu13 SATA 10.000GB
 /dev/enas/lu14 SATA 10.000GB
```

## Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node has stopped during processing, wait about 15 minutes or boot the stopped node. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 98 | Some other error occurred. |
| 99 | ▪ Information acquisition of a device file failed because of an unexpected error in internal processing. A problem may exist in the information acquisition processing of a device file. Acquire all the Management log files and inform maintenance personnel.<br>▪ Access to the NAS Cluster Management LU failed. Acquire all the Management log files and inform maintenance personnel.<br>▪ Acquisition of the device file information from the NAS Cluster Management LU failed. Acquire all the Management log files and inform maintenance personnel.<br>▪ Updating of the device file information of the NAS Cluster Management LU failed. Acquire all the Management log files and inform maintenance personnel.<br>▪ An internal error occurred. A conflict with another system administrator's operation or system error may have occurred. Retry. If the error occurs again, acquire all the Management log files and then inform maintenance personnel.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and inform maintenance personnel. |

## Example

### To view information about available device files:

```
$ sudo enas_devfreelist
Device files for use:
 /dev/enas/lu02 FC 20.000GB
 /dev/enas/lu03 FC 20.000GB
```

```
/dev/enas/lu04 FC 20.000GB
/dev/enas/lu12 SATA 10.000GB
/dev/enas/lu13 SATA 10.000GB
/dev/enas/lu14 SATA 10.000GB
```

### 6.2.8 enas_dircreate (Create a Subdirectory)

- **Synopsis**

  *enas_dircreate -u {user-name|user-ID} -g {group-name|group-ID}*
  *[-m mode] path*

- **Description**

  Creates a directory to be made public as an NFS share or CIFS share in a file system.

  If you want to create a hierarchy of directories under the mount point, create the top directory first, and then create the lower directories.

  To prevent data from being lost, no command is provided in NAS Manager for deleting subdirectories. When you use the `enas_dircreate` command to create a subdirectory, check the path of the subdirectory.

- **Arguments and Options**

**Table 6.7 enas_dircreate Arguments and Options**

| Item | Use |
|---|---|
| `-h` | Specify this option if you want to view the command syntax. |
| `-u` *user* | When you specify the owner by using its user ID, specify it in the range from 0 to 2,147,483,147. Non-zero IDs cannot start with 0. |
| `-g` { *group-name* \| *group-ID* } | Specify the group name or group ID of the owner group for the directory you are creating.<br>When you specify the owner group by using its group ID, specify it in the range from 0 to 2,147,483,147. Non-zero IDs cannot start with 0. |
| `-m` *mode* | Specify the mode of the directory to be created as the logical OR of the mode bits shown below. Mode bits are specified as octal numbers. The valid value range is from 0000 to 3777. The value must be specified with 3 or 4 digits. If you omit this option, a directory with a mode of `0755` is created.<br>Mode bits<br>`2000`<br>Group ID. The group ID of files or directories created under a directory is set as the directory group ID.<br>`1000`<br>Sticky bit. Set this bit so that only the creator is allowed to delete files or directories created under the directory.<br>Permission mode bit<br>Specify access permissions for the directory for the owner, the owner group, and the other users.<br>`0400` Reading by the owner.<br>`0200` Writing by the owner.<br>`0100` Directory search by the owner.<br>`0040` Reading by the group.<br>`0020` Writing by the group.<br>`0010` Directory search by the group.<br>`0004` Reading by the other users.<br>`0002` Writing by the other users.<br>`0001` Directory search by the other users. |

| Item | Use |
|---|---|
| *path* | Specify the absolute path of the directory to be created. In the directory name, you can use alphanumeric characters, hyphens (-), periods (.), and underscores (_). You cannot include any symbolic links in the path. |

- **Example**

  Use the following command to create the subdirectory `dir_case1` with the following conditions:

  - Create the subdirectory under the file system `FS1`.
  - Specify `USER1` as the owner of `dir_case1` (`-u`).
  - Specify `test_grp` as the group of `dir_case1` (`-g`).
  - Set the mode to `750` (`-m`).

  **$ sudo enas_dircreate -u USER1 -g test_grp -m 750 /mnt/FS1/dir_case1**

### 6.2.9 enas_dircreate (Create a directory)

#### Synopsis

```
enas_dircreate -u {user-name|user-ID} -g {group-name|group-ID}
  [-m mode] path
enas_dircreate -h
```

#### Description

Creates a directory to be used as an NFS or CIFS shared directory in a file system.

If you want to create a hierarchy of directories under the mount point, create the top directory first, and then create the lower directories.

To prevent data from being lost, no command is provided in NAS Manager for deleting directories. When you use the `enas_dircreate` command to create a directory, check the path of the directory.

#### Options and arguments

**`-g {`*group-name*`|`*group-ID*`}`**

Specify the group name or group ID of the owner group for the directory you are creating.

When you specify the owner group by using its group ID, specify it in the range from 0 to 2,147,483,147. Non-zero IDs cannot start with 0.

**`-h`**

Specify this option if you want to view the command syntax.

**`-m`** ***mode***

Specify the mode for the owner, owner group, and other users. Specify the mode as a 3-digit or 4-digit number representing the logical OR of the following octal numbers. If you omit this option, a directory with a mode of `0755` is created.

**Table 6.8 Directory Modes Specifiable in the -m option of the enas_dircreate Command**

| Octal numbers | Description |
|---|---|
| 2000 | Uses the SetGID. The subdirectories and files created under the directory inherit the GID of the directory. When further subdirectories are created under the directory to which the SetGID is applied, those subdirectories inherit the GID of the upper directory. |
| 1000 | Sets the sticky bit so that subdirectories and files created under the directory can only be deleted or renamed by the owner. |
| 0400 | Sets read permission for the owner. |
| 0200 | Sets write permission for the owner. |
| 0100 | Sets search permission for the owner. |

| | |
|---|---|
| 0040 | Sets read permission for the owner group. |
| 0020 | Sets write permission for the owner group. |
| 0010 | Sets search permission for the owner group. |
| 0004 | Sets read permission for other users. |
| 0002 | Sets write permission for other users. |
| 0001 | Sets search permission for other users. |

**-u** {***user-name***|***user-ID***}

Specify the user name or user ID of the owner of the directory to be created.

When you specify the owner by using its user ID, specify it in the range from 0 to 2,147,483,147. Non-zero IDs cannot start with 0.

***path***

Specify the absolute path of the directory to be created. In the directory name, you can use alphanumeric characters, hyphens (-), periods (.), and underscores (_). You cannot include any symbolic links in the path.

## Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter.<br>▪ The specified UID or GID is invalid. Enter a numerical value from 0 to 2,147,483,147 for the ID. Do not enter a zero at the beginning of the value. |
| 10 | ▪ A name not registered in the system was specified for the argument of an option. Retry specifying a parameter name registered in the system.<br>▪ A directory cannot be created because a parent directory does not exist. Make sure that the parent directory exists, and then re-execute the operation.<br>▪ The name of a directory that already exists was specified. Specify the name of the new directory to be created.<br>▪ The specified directory contains a relative path or symbolic link. Specify an absolute pathname. Moreover, for a directory, specify a path that does not include a symbolic link. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 70 | ▪ Directory operations cannot be performed because the file system corresponding to the specified directory is being failed over. Specify a file system that is not being failed over. If you want to perform a directory operation using the specified file system, carry out failback, and then perform the operation.<br>▪ The file system corresponding to the specified directory is not mounted, or automatic failover is being carried out. If failover was carried out, remove the problem and then retry. If the file system is not mounted, mount the file system, and then retry.<br>▪ The directory operation cannot be performed because the file system corresponding to the specified directory does not exist. Specify the right file system name.<br>▪ The directory operation cannot be performed because the file system corresponding to the |

| | |
|---|---|
| | specified directory is defined by the other node in the cluster. On the other node of the cluster, perform the directory operation for the file system corresponding to the specified directory.<br>▪ The directory operation cannot be performed because the file system corresponding to the specified directory is mounted but writing is not permitted. Mount the file system with writing permitted, and then retry the operation.<br>▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first.<br>▪ A directory operation failed because the resource group corresponding to the specified directory is in the OFFLINE state. Check the state of the resource group. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 98 | Some other error occurred. |
| 99 | ▪ An internal error occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel.<br>▪ The specified directory operation failed. The file system may be blocked. In the **List of File Systems**, check the state of the file system. If the file system has an error status, inform maintenance personnel.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and inform maintenance personnel. |

## Example

### To create a directory according to the following conditions:

- Create the directory `dir_case1` directly under the `/mnt/FS1`.
- Specify `USER1` as the owner.
- Specify `GROUP1` as the owner group.
- Set the mode to `750`.

```
$ sudo enas_dircreate -u USER1 -g GROUP1 -m 750 /mnt/FS1/dir_case1
```

### 6.2.10 enas_diredit (Change Directory Attributes)

- **Synopsis**

```
enas_diredit [-u {user-name|user-ID}] [-g {group-name|group-ID}]
  [-m mode] path
enas_diredit -h
```

- **Description**

  Changes the permission, owner, and group of the directory to be made public by file sharing. If you omit all the options, only the path validation check is performed.

- **Arguments and Options**

**Table 6.9 enas_diredit Arguments and Options**

| Item | Use |
|---|---|
| `-h` | Specify this option if you want to view the command syntax. |
| `-u` {*user-name*\|*user-ID*} | Specify the user name or user ID if you want to change the owner of the specified directory. If you omit this option, the current setting still applies.<br>When you specify the owner by using its user ID, specify it in the range from 0 to 2,147,483,147. Non-zero IDs cannot start with 0. |
| `-g` *group* | Specify the group name if you want to change the group name of the specified directory. If you omit this option, the group name is not changed.<br>When you specify the owner group by using its group ID, specify it in the range from 0 to 2,147,483,147. Non-zero IDs cannot start with 0. |
| `-m` *mode* | Specify the mode of the directory to be changed. Specify the mode as the logical OR of the mode bits shown below. Mode bits are specified as octal numbers. The valid value range is from 0000 to 3777. The value must be specified with 3 or 4 digits. If you omit this option, the current mode setting is not changed.<br>Mode bits<br>`2000`<br>Group ID. The group ID of files or directories created under a directory is set as the directory group ID.<br>`1000`<br>Sticky bit. Set this bit so that only the creator is allowed to delete files or directories created under the directory.<br>Permission mode bit<br>Specify access permissions for the directory for the owner, the owner group, and the other users.<br>`0400` Reading by the owner.<br>`0200` Writing by the owner.<br>`0100` Directory search by the owner.<br>`0040` Reading by the group.<br>`0020` Writing by the group.<br>`0010` Directory search by the group.<br>`0004` Reading by the other users.<br>`0002` Writing by the other users.<br>`0001` Directory search by the other users. |
| *Path* | Specify the absolute path of the directory whose attributes you are changing. You cannot include any symbolic links in the path. |

## Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command and use the command again, specifying a suitable parameter.<br>▪ The specified UID or GID is invalid. Enter a numerical value from 0 to 2,147,483,147 for the ID. Do not enter a zero at the beginning of the value. |
| 10 | ▪ A name not registered in the system was specified for the argument of an option. Use the command again, specifying a parameter name registered in the system.<br>▪ The specified directory does not exist. Specify an existing directory.<br>▪ The specified directory contains a relative path or symbolic link. Specify an absolute pathname. For a directory, specify a path that does not include a symbolic link. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then use again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 70 | ▪ Directory operations cannot be performed because the file system corresponding to the specified directory is being failed over. Specify a file system that is not being failed over. If you want to perform a directory operation using the specified file system, carry out failback, and then perform the operation.<br>▪ The file system corresponding to the specified directory is not mounted, or automatic failover is being carried out. If failover was carried out, remove the problem and use the command again. If the file system is not mounted, mount the file system, and use the command again.<br>▪ The directory operation cannot be performed because the file system corresponding to the specified directory does not exist. Specify the right file system name.<br>▪ The directory operation cannot be performed because the file system corresponding to the specified directory is defined by the other node in the cluster. On the other node of the cluster, perform the directory operation for the file system corresponding to the specified directory.<br>▪ The directory operation cannot be performed because the file system corresponding to the specified directory is mounted but writing is not permitted. Mount the file system with writing permitted, and use the command again.<br>▪ The license of NAS Manager is not set. For details on license setup, see the manual for *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first.<br>▪ A directory operation failed because the resource group corresponding to the specified directory is in the OFFLINE state. Check the state of the resource group. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform your HDS representative. |
| 98 | Some other error occurred. |
| 99 | ▪ An internal error occurred. Use the command again. Acquire all the Management log files if this error occurs again, and inform your HDS representative.<br>▪ The specified directory operation failed. The file system may be blocked. In the **List of File Systems**, check the state of the file system. If the file system has an error status, inform your HDS representative.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and inform your HDS representative. |

- **Example**

  Use the following command to change the mode bit of the subdirectory `/mnt/FS1/dir_case1` to `777`:

  ```
  $ sudo enas_diredit -m 777 /mnt/FS1/dir_case1
  ```

### 6.2.11 enas_dirgetacl (Display ACL information)

#### Synopsis

```
enas_dirgetacl path
enas_dirgetacl -h
```

#### Description

Displays the ACL information set for a shared directory in a CIFS share.

#### Options and arguments

**-h**

Specify this option if you want to view the command syntax.

***path***

Specify the absolute path of the directory for which to display ACL information. You cannot include any symbolic links in the path.

#### Displayed information

For an ACL set by a CIFS client, the information displayed by the `enas_dirgetacl` command depends on the information selected in **Apply onto**. An ACL set by a CIFS client with **This folder only** selected in **Apply onto** will be displayed as an access ACL. An ACL set with **Subfolders and files only** selected in **Apply onto** will be displayed as the default ACL.

***Notes:***

You can check the **Apply onto** setting from a CIFS client (Windows 2000 environment) as follows:

On the CIFS client, display the directory properties.

Select the **Security** page, and then click the **Advanced** button.

Select the **Permissions** page, and then click the **View/Edit** button.

The following table lists the information displayed when you execute the command.

**Table 6.10 ACL settings displayed when executing the enas_dirgetacl command**

| Item | Description |
|---|---|
| `# file` | Displays the specified directory name. |
| `# owner` | Displays the directory owner name. |
| `# group` | Displays the directory owner group name. |
| `user` | Displays the ACL entry for the owner or the specific user.<br>If the entry is for the owner, information is displayed in the following format:<br>`user::`*`access-permissions`*<br>If the entry is for a specific user, information is displayed in either of the |

| | |
|---|---|
| | following formats:<br>`user:`*`user-name`*`:`*`access-permissions`*<br>`user:`*`user-ID`*`:`*`access-permissions`* |
| `group` | Displays the default ACL entry for the group.<br>If the entry is for the owner group, information is displayed in the following format:<br>`group::`*`access-permissions`*<br>If the entry is for a specific group, information is displayed in either of the following formats:<br>`group:`*`group-name`*`:`*`access-permissions`*<br>`group:`*`group-ID`*`:`*`access-permissions`* |
| `mask` | Displays the permissions (mask) applied to the specific user or group.<br>The mask is the ACL entry that limits the access permissions that are valid for the specific user, specific group, or the other. |
| `other` | Displays the ACL entry for others. |
| `default:user` | Displays the default ACL entry for the owner or the specific user.<br>If the entry is for the owner, information is displayed in the following format:<br>`default:user::`*`access-permissions`*<br>If the entry is for a specific user, information is displayed in the following format:<br>`default:user:` *`user-name`*`:`*`access-permissions`*<br>`default:user:` *`user-ID`*`:`*`access-permissions`* |
| `default:group` | Displays the default ACL entry for the group.<br>If the entry is for the owner group, information is displayed in the following format:<br>`default:group::`*`access-permissions`*<br>If the entry is for a specific group, information is displayed in either of the following formats:<br>`default:group:`*`group-name`*`:`*`access-permissions`*<br>`default:group:`*`group-ID`*`:`*`access-permissions`* |
| `default:mask` | Displays the default access permissions (mask) applied to the specific user or group. |
| `default:other` | Displays the default ACL entry for others. |

***Note:***

When the mask is set by using the `enas_dirsetacl` command, or when the ACL specifies that the mask is not to be recalculated (specifying the `-n` option), the ACLs for the owner group and specific user or group might not be controlled as specified by the specified access permissions. When the setting for the mask is in effect, the ACL for the specific user is followed by the access permissions that are actually in effect.

*ACL-for-specific-user* `#effective:`***access-permissions-in-effect***

## Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry |

| | |
|---|---|
| | specifying a suitable parameter. |
| 10 | ▪ The specified directory does not exist. Specify an existing directory.<br>▪ The specified directory contains a relative path or symbolic Link. Specify an absolute pathname. Moreover, for a shared directory, specify a path that does not include a symbolic link. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | An attempt to acquire the ACL has failed. A conflict with another system administrator's operation or an internal error may have occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first.<br>▪ The directory operation cannot be performed because the file system corresponding to the specified directory does not exist. In the **List of File Systems** check the file system name, and then specify the right file system name.<br>▪ The directory operation cannot be performed because the file system corresponding to the specified directory is defined by the other node in the cluster. On the other node of the cluster, perform the operation for the specified directory.<br>▪ The file system corresponding to the specified directory is not mounted. The resource group is in the Offline state, or a failover might be occurring. If the resource group is in the Offline state or a failover is occurring, remove the problem and then try again. If the file system is not mounted, mount the file system, and then retry. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | ▪ An error occurred in the shared processing of commands. Acquire all the Management log files and inform maintenance personnel.<br>▪ The specified directory operation failed. The file system may be blocked. In the **List of File Systems**, check the state of the file system. If the file system has an error status, inform maintenance personnel.<br>▪ An internal error may have occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel. |

## Example

### To display the default ACL settings for the `/mnt/ACLCIFS/acldir` directory:

```
$ sudo enas_dirgetacl /mnt/ACLCIFS/acldir
# file: /mnt/ACLCIFS/acldir
# owner: user1
# group: gruop1
user::rwx
user:user2:rwx      #effective:r-x
group::rwx        #effective:r-x
group:group2:r-x
mask:r-x
other:r-x
default:user::rwx
default:user:user2:rwx  #effective:r-x
default:group::r-x
```

```
default:mask:r-x
default:other:---
```

### 6.2.12 enas_dirlist (List Directory Attributes)

- **Synopsis**

  ```
  enas_dirlist [-d] [-n] [-c] path
  enas_dirlist -h
  ```

- **Description**

  Displays attributes of subdirectories under the specified directory. The information is displayed by directory in ascending order of directory names.

**Table 6.11 Information Displayed when enas_dirlist Command is Used**

| Item | Description |
|---|---|
| *Directory mode* | Displays the directory mode as the logical OR of mode bits (a 4-digit octal number).<br>`2000`<br>Uses the SetGID.<br>`1000`<br>Sets the sticky bit.<br>`0400`<br>Sets read permission for the owner.<br>`0200`<br>Sets write permission for the owner.<br>`0100`<br>Sets search permission for the owner.<br>`0040`<br>Sets read permission for the owner group.<br>`0020`<br>Sets write permission for the owner group.<br>`0010`<br>Sets search permission for the owner group.<br>`0004`<br>Sets read permission for other users.<br>`0002`<br>Sets write permission for other users.<br>`0001`<br>Sets search permission for other users. |
| *owner* | Displays the user name or user ID of the owner.<br>Specify the `-n` option to display the user ID.<br>Specify the `-c` option to display the entire user name and user ID. If you omit the `-c` option, the user name is left-justified (and padded with spaces) to a maximum of 16 characters. The 17th and subsequent characters are truncated.<br>If the user ID cannot be converted into the user name, the user ID is displayed. |
| *owner-group* | Displays the group name or group ID of the owner group.<br>Specify the `-n` option to display the group ID.<br>Specify the `-c` option to display the entire group name and group ID. If you omit the `-c` option, the group name is left-justified (and padded with spaces) to a maximum of 16 characters. The 17th and subsequent characters are truncated. |

| | |
|---|---|
| | If the group ID cannot be converted into the group name, the group ID is displayed. |
| *directory-path* | Displays the full path of the specified directory. |

- **Arguments and Options**

**Table 6.12 enas_dirlist Arguments and Options**

| Item | Use |
|---|---|
| `-h` | Specify this option if you want to view the command syntax. |
| `-d` | Specify this if you want to display the attributes of the specified directory. If you omit this option, this command displays a list of attributes for the directories under the directory specified in *directory-path*. If there are no directories under *directory-path*, nothing is displayed. |
| `-n` | Specify this if you want to display the user ID and the group ID instead of the user name and the group name. If you omit this option, the user name and the group name are displayed. |
| `-c` | Specify the following to display directory information separated with colons (`:`).<br>*directory-mode*`:`*user-name*`:`*group-name*`:`*directory-name*<br>`:`<br>`: (Information is output for each directory.)`<br>`:`<br>If you omit this option, directory information is displayed, separated with spaces.<br>*directory-mode user-name group-name directory-name*<br>`:`<br>`: (Information is output for each directory.)`<br>`:` |
| *path* | Specify the path of the directory whose directory attributes are to be viewed.<br>Specify the directory path in the `/mnt/`*file-system-name*`/`*subdirectory* format. The specified path must already exist. The specified file system must be mounted on `/mnt/`*file-system-name*. In addition, if the specified file system was defined in another node and then failed over, the subdirectory under `/mnt/`*file-system-name* cannot be displayed.<br>You can also specify a subdirectory with more than one depth level, such as `aaa/bbb/ccc`. |

## Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command and use it again, specifying a suitable parameter. |
| `10` | ▪ The specified directory does not exist. Specify an existing directory.<br>▪ The specified directory contains a relative path or symbolic link. Specify an absolute pathname. Moreover, for a directory, specify a path that does not include a symbolic link. |
| `65` | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then use again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| `70` | ▪ Directory operations cannot be performed because the file system corresponding to the specified directory is being failed over. Specify a file system that is not being failed over. If you want to perform a directory operation using the specified file system, carry out failback, and then perform the operation.<br>▪ The file system corresponding to the specified directory is not mounted, or automatic failover is being carried out. If failover was carried out, remove the problem and use the command again. If the file system is not mounted, mount the file system and use the command again. |

| | |
|---|---|
| | ▪ The directory operation cannot be performed because the file system corresponding to the specified directory does not exist. Specify the right file system name.<br>▪ The directory operation cannot be performed because the file system corresponding to the specified directory is defined by the other node in the cluster. On the other node of the cluster, perform the directory operation for the file system corresponding to the specified directory.<br>▪ The license of NAS Manager is not set. For details on license setup, see the manual for *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first.<br>▪ A directory operation failed because the resource group corresponding to the specified directory is in the OFFLINE state. Check the state of the resource group. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform your HDS representative. |
| 98 | Some other error occurred. |
| 99 | ▪ An internal error occurred. Use the command again. Acquire all the Management log files if this error occurs again, and inform your HDS representative.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and inform your HDS representative.<br>▪ The specified directory operation failed. The file system may be blocked. In the **List of File Systems**, check the state of the file system. If the file system has an error status, inform your HDS representative. |

- **Examples**
  - To view attributes of the subdirectory `dir1` specifying the `-c` option:

```
$ sudo enas_dirlist -d -c /mnt/FS1/dir1
0755:USER1:GROUP1:/mnt/FS1/dir1
```

  - To view attributes of the subdirectory `dir1` without specifying the `-c` option:

```
$ sudo enas_dirlist -d /mnt/FS1/dir1
0755 USER1      GROUP1      /mnt/FS1/dir1
```

### 6.2.13 enas_dirsetacl (Set ACLs)

#### Synopsis

```
enas_dirsetacl [-n] [-d] {-s|-m|-x}
  acl-spec[,acl-spec...] path
enas_dirsetacl -b path
enas_dirsetacl -k path
enas_dirsetacl -h
```

#### Description

Sets an ACL for the shared directory in a CIFS share. For one directory, you can set up to 128 ACL entries (up to 64 each for access ACLs and masks, and for the default ACLs and masks).

In the default ACL of the owner group, if you specify `0` or `-` for access permission, you must also specify `0` or `-` for access permissions in the default ACL of other users. However, in the default ACL of specific users or specific groups, do not specify `0` or `-` for access permissions.

#### Options and arguments

**`-b`**

Specify this option when you want to delete all access ACLs or default ACLs for the specific user or group.

**`-d`**

Specify this option if you want to set a default ACL. If you omit this option, an access ACL is set. If you omit any of the default ACL entries for the owner, owner group, or other users, the permissions set for the owner, owner group, or other users of the parent directory apply.

**`-h`**

Specify this option if you want to view the command syntax.

**`-k`**

Specify this option if you want to delete all default ACLs.

**`-n`**

Specify this option if you do not want to recalculate the mask. You do not need to specify this option for normal operation. If you set an ACL without specifying this option, the mask will be recalculated to an appropriate value.

**`{-s|-m|-x}`** ***acl-spec*`[,`*`acl-spec`*`...]`**

Specify this option if you want to add, modify, or delete the specified ACL entry.

`-s`

Specify this option to delete all the existing ACL entries and reset the ACL.

When you set an access ACL, all the ACL entries for the access ACL are deleted, and then the new ACL entries for the access ACL are added. You must specify ACL entries for the owner, owner group, and other users.

When you set a default ACL, all the ACL entries for the default ACL are deleted, and then the new ACL entries for the default ACL are added.

`-m`

Specify this option in the following cases:

- When you want to add a new ACL entry to the existing ACL entries.
- When you want to change the ACL entries.

`-x`

Specify this option if you want to delete the specified ACL entry.

Only the following ACL entries can be deleted:

- An access ACL for a specific user or group.
- A default ACL for a specific user or group.

When deleting a default ACL or a mask of the default ACL for the owner, owner group and others, specify the `-k` option.

*acl-spec*`[,`*acl-spec*`...]`

Specify the ACL entry to be added, modified, or deleted. Specify the ACL entry in the following format:

```
processing-target:user-or-group:access-permissions
```

However, when the `-x` option is specified to delete the ACL for a specific user or a specific group, the *acl-spec* argument must be specified in the following format:

```
processing-target:user-or-group
```

The table below explains the information specified as ACL entries.

**Table 6.13 Information specified as ACL entries in the enas_dirsetacl command**

| Item | Specification |
|---|---|
| *processing-target* | Specify the target of ACL addition, modification, or deletion.<br>`u` or `user`<br>Specify this option to set an ACL for the owner or for a specific user.<br>`g` or `group`<br>Specify this option to set an ACL for the owner group or for a specific group.<br>`m` or `mask` |

| | |
|---|---|
| | Specify this option if you want to set a mask. You do not need to operate the mask for normal operation.<br>`o` or `other`<br>Specify this option if you want to set an ACL for others. |
| *user-or-group* | Specify this argument if you want to add, modify, or delete the ACL for a specific user or group.<br>To specify a user, specify the user name or user ID here. To specify a group, specify the group name or group ID here.<br>You do not need to specify this argument in the following cases:<br>▪ When you are to add, modify, or delete the ACL for the owner, owner group, or others.<br>▪ When you are to set a mask. |
| *access-permissions* | Specify the access permissions to be added, changed, or deleted. Use a combination of characters or set an octal number representing the logical OR of the permissions.<br>In octal notation, `r` (read permission), `w` (write permission), `x` (directory search permission), and `-` (not permitted) correspond to `4`, `2`, `1`, and `0`, respectively.<br>For example, if you want to allow read and write access, specify `rw` or `6`. |

### *path*

Specify the absolute path of the directory for which the ACL is to be set. You cannot include any symbolic links in the path.

## Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter.<br>▪ A syntax error exists in the specified ACL Specify a valid ACL.<br>▪ When the -s option is specified to set an access ACL, the access ACL for Owner, Owner Group, and Other must also be specified. When the `-s` option is specified to set an access ACL, include the access ACL for Owner, Owner Group, and Other.<br>▪ The specified ACL cannot be deleted because it is an access ACL for Owner, Owner Group, and Other, or it is a mask. Specify an ACL other than a mask or an access ACL for Owner, Owner Group, and Other. |
| `10` | ▪ The specified directory does not exist. Specify an existing directory.<br>▪ The specified directory contains a relative path or symbolic Link. Specify an absolute pathname. Moreover, for a shared directory, specify a path that does not include a symbolic link.<br>▪ A name not registered in the system was specified for the argument of an option. Retry specifying a parameter name registered in the system.<br>▪ The mask for the default ACL cannot be deleted because a default ACL is set. When deleting a mask for default ACLs, delete all of the default ACLs. |
| `65` | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| `66` | An attempt to set the ACL has failed. A conflict with another system administrator's operation or an internal error may have occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel. |

| | |
|---|---|
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first.<br>▪ The directory operation cannot be performed because the file system corresponding to the specified directory does not exist. In the **List of File Systems** check the file system name, and then specify the right file system name.<br>▪ The directory operation cannot be performed because the file system corresponding to the specified directory is defined by the other node in the cluster. On the other node of the cluster, perform the operation for the specified directory.<br>▪ The file system corresponding to the specified directory is not mounted. The resource group is in the Offline state, or a failover might be occurring. If the resource group is in the Offline state or a failover is occurring, remove the problem and then try again. If the file system is not mounted, mount the file system, and then retry.<br>▪ The directory operation cannot be performed because the file system corresponding to the specified directory is mounted but writing is not permitted. Mount the file system with write permissions, and then retry the operation. If the file system is mounted without write permissions, this operation cannot be performed.<br>▪ The operation cannot be performed on the specified file share. Another system administrator might have performed an operation on the specified file share. Check the latest status in the **List of File Shares** window.<br>▪ The ACL cannot be set because there is not enough space on the file system corresponding to the specified directory. Delete any unnecessary data or expand the file system capacity, and then retry execution. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | ▪ An error occurred in the shared processing of commands. Acquire all the Management log files and inform maintenance personnel.<br>▪ The specified directory operation failed. The file system may be blocked. In the **List of File Systems**, check the state of the file system. If the file system has an error status, inform maintenance personnel.<br>▪ An internal error may have occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel. |

## Examples

### To modify the access ACL for a directory according to the following conditions:

- The directory whose ACL is to be changed is `/mnt/ACLCIFS/acldir`.
- Read and write permissions are granted to `user01` user.
- Read permission is granted to `ACL-users` group.

```
$ sudo enas_dirsetacl -m u:user01:rw,g:ACL-users:r
/mnt/ACLCIFS/acldir
```

### To delete the default ACL entries for a directory according to the following conditions:

- The directory whose ACL is to be deleted is `/mnt/ACLCIFS/acldir`.
- Delete the ACL entry for user `user01` user.
- Delete the ACL entry for group `ACL-users` group.

```
$ sudo enas_dirsetacl -d -x u:user01,g:ACL-users /mnt/ACLCIFS/acldir
```

### 6.2.14 enas_eraselog (Delete Logs)

- **Synopsis**

  enas_eraselog

- **Description**

  Deletes the packet dump files and the log files that are created when the enas_netstat, enas_ping, or enas_traceroute command is used.

- **Arguments and Options**

  None.

- **Return Value**

  Always 0.

- **Example**

  $ sudo enas_eraselog

### 6.2.15 enas_fcparm (Display and change the settings of the FC port)

#### Synopsis

```
enas_fcparm -d
enas_fcparm -s {1|2}
```

#### Description

Displays or changes the settings of the FC port on the NAS Unit.

The initial data transfer speed on the FC port is 2 Gbps.

#### Options and arguments

**-d**

Specify this option if you want to view the settings of the FC port.

**-s {1|2}**

Specify this option if you want to change the data transfer speed on the FC port.

1

Specify this if you want to change the data transfer speed to 1 Gbps.

2

Specify this if you want to change the data transfer speed to 2 Gbps.

#### Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.14 Information displayed when executing the enas_fcparm command**

| Item | Description |
|---|---|
| Speed | Displays the data transfer speed specified for the FC port.<br>1Gbps<br>Displayed when the data transfer speed on the FC port is specified as 1 Gbps.<br>2Gbps<br>Displayed when the data transfer speed on the FC port is specified as 2 Gbps. |

#### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | The specified option and argument are incorrect. Check the command syntax, specify the correct option and argument, and then execute the command again. |
| 2 | The file that contains the settings of the FC port does not exist. Acquire all of the kernel logs, and then contact maintenance personnel. |

| | |
|---|---|
| 3 | An attempt to read the set value from the file that contains the settings of the FC port or an attempt to save the set value to the file has failed. Execute the command again. If the error occurs again, acquire all of the kernel logs, and then contact maintenance personnel. |
| 4 | An attempt to restart the FC adapter driver has failed. Execute the command again. If the error occurs again, acquire all of the kernel logs, and then contact maintenance personnel. |
| 5 | Processing of the `enas_fcparm` command is being executed. Make sure that maintenance personnel or other administrators are not operating the FC port in the cluster. If no one is operating the FC port, execute the command again. If the error occurs again, acquire all of the kernel logs, and then contact maintenance personnel. |
| 6 | The `enas_fcparm` command cannot be executed because the device connected to the FC port is attached to the NAS Unit. Detach the device, and then execute the command again. If the error occurs again, acquire all of the kernel logs, and then contact maintenance personnel. |

## Examples

### To view the data transfer speed specified on the FC port:

```
$ sudo enas_fcparm –d
  Speed     = 2Gbps
```

### To change the data transfer speed on the FC port to 1 Gbps:

```
$ sudo enas_fcparm –s 1
```

### 6.2.16 enas_fsautofo (Manage auto failover functionality when a file system is blocked)

#### Synopsis

```
enas_fsautofo [-s|-u] -a
enas_fsautofo [-s|-u] file-system-name[ file-system-name...]
enas_fsautofo -h
```

#### Description

Enables or disables automatic failover that occurs when a file system is blocked. Also displays the automatic failover settings.

We recommend that you specify the service IP address when you log in if you want to use this command.

When the NAS Modular system is first deployed, automatic failover is disabled so that failover does not occur when a file system is blocked. Change this setting as required, depending on how the NAS Modular system is to be used.

If you omit the `-s` and `-u` option, the automatic failover settings are displayed separately for each file system.

If you execute this command while processing for a cluster, node, or resource group is in progress, the automatic failover setting might not complete normally. Execute the command so as to avoid contention with cluster, node, or resource group operations.

#### Options and arguments

**-a**

Specify this option if you want to enable or disable automatic failover for all file systems mounted on the node you are logged in to. If the command processing fails for any file system, processing continues for the other file systems.

**-h**

Specify this option if you want to view the command syntax.

**-s**

Specify this option to enable automatic failover when a file system is blocked.

**-u**

Specify this option to disable automatic failover so that failover does not occur when a file system is blocked.

***file-system-name*[ *file-system-name*...]**

Specify the file system names if you want to enable or disable automatic failover for specific file systems. You can specify an asterisk (*) or question mark (?) as a wildcard. Separate multiple file system names with spaces.

## Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.15 Information displayed when executing the enas_fsautofo command**

| Item | Description |
|---|---|
| *file-system-name* | Displays the file system name. |
| *status* | Displays whether automatic failover that occurs when the file system is blocked is enabled.<br>On<br>Automatic failover is enabled.<br>Off<br>Automatic failover is disabled. |

## Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ There are too many or too few parameters. Check the command format, specify a correct parameter, and then try again.<br>▪ If a syntax error occurred, check the command format, and then try again.<br>▪ The specified file system is invalid. Specify a correct file system name, and then try again.<br>▪ If multiple file systems are specified, processing might have terminated abnormally for one of the file systems. Specify the name of the file system for which the processing terminated abnormally, and then try again. |
| 10 | ▪ The specified file system is not mounted. If multiple file systems are specified, processing will continue. If the file system is not mounted, mount it or specify a correct file system name, and then try again.<br>▪ An attempt to specify the settings failed because the file system is full. If multiple file systems are specified, processing will continue. Make some free space on the file system, and then try again.<br>▪ An attempt to specify the settings failed because the file system is mounted with read-only permissions. If multiple file systems are specified, processing will continue. Remount the file system with read/write permissions, and then try again. |
| 99 | ▪ The specified file system is not in a normal state. Check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to acquire mount information has failed. There might be a problem in the NAS OS LU or in the processing for acquiring mount information. Check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to access management information about the file system has failed. The specified file system might have a problem or contention with other processing might have occurred. Wait a while, and then try again. If the error occurs again, check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to open the log files has failed. There might be a problem in the log files or contention with other processing might have occurred. Wait a while, and then try again. If the |

| | |
|---|---|
| | error occurs again, check the settings for the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel. |

## Examples

**To enable automatic failover for all the file systems mounted on the node you are logged in to, so that failover occurs when one of the file systems is blocked:**

```
$ sudo enas_fsautofo -s -a
```

**To check whether automatic failover is enabled for `FS_1` and `FS_2`:**

```
$ sudo enas_fsautofo FS_1 FS_2
 FS_1       On
 FS_2       Off
```

### 6.2.17 enas_fscreate (Create a File System)

- **Synopsis**

  enas_fscreate -h|[-i i-node] [-l logsize] [-d agsize]
  [-v {use|do_not_use}] [-c {on|off}] *file-system-name dev-name*[,*dev-name*...] enas_fscreate -h

- **Description**

  Creates a file system.

- **Arguments and Options**

**Table 6.16 enas_fscreate Arguments and Options**

| Item | Use |
|---|---|
| -h | Specify this option if you want to view the command syntax. |
| -i *i-node* | Specify the maximum capacity that can be used for an i-node as a percentage of the file system capacity (in %). Specify a value from 1 to 100. If you omit this option, it defaults to 25%. |
| -l *logsize* | Specify the size of space to be used for logging (in MB). Specify a value from 2 to 128. Specify a value smaller than the file system division size specified in the -d option. If you omit this option, it defaults to 5MB. |
| -d *agsize* | Specify an appropriate file system division size depending on the file system capacity (total capacity of device files). Make sure that you specify the first character of the unit. For example, you must specify 128M if the specified division size is 128MB, and 4G if the size is 4GB.<br>Table 6.17 lists the possible file system division sizes when the file system capacity is *m*. |
| -v {use\|do_not_use} | Specify whether to use a volume manager. When you create a file system from multiple device files, specify use. If you omit this option, it defaults to use.<br>If you want to use NAS Sync Image, the setup source file system of the differential-data storage device must be created using a volume manager. If you might use the created file system in NAS Sync Image, specify use.<br>▪ use<br>Specify to use a volume manager.<br>▪ do_not_use<br>Specify if you do not want to use a volume manager. |
| -c {on\|off} | Specify whether to record the file creation time in the file system. If you omit this option, off is assumed. We recommend that you specify on if you intend to create and use CIFS shares in the file system you are creating.<br>on<br>Records the file creation time.<br>off<br>Does not record the file creation time.<br>If NFS shares are to be created and used in the file system, the file creation times cannot be viewed from the NFS clients even if you specify on. |
| *file-system-name* | Specify the name of the file system to be created. Specify a unique name within a cluster. Specify a string of no more than 16 characters consisting of alphanumeric characters and underscores (_). |
| *dev-name* [,*dev-name*...] | Specify the names of device files to be used in the file system. For example, if the device file path is /dev/enas/lu01, specify lu01. If you want to create a file system |

| | |
|---|---|
| | that consists of multiple device files using a volume manager, separate the device file names with commas ( , ). |

**Table 6.17 File System Division Sizes specified in -d Option**

| File System Capacity | Specifiable File System Division Size | Default Size if Option Omitted |
|---|---|---|
| 128MB <= m < 256MB | 16MB, 32MB, 64MB, 128MB | 128MB |
| 256MB <= m < 512MB | 32MB, 64MB, 128MB, 256MB | 256MB |
| 512MB <= m < 1GB | 64MB, 128MB, 256MB, 512MB | 512MB |
| 1GB <= m < 2GB | 128MB, 256MB, 512MB, 1GB | 1GB |
| 2GB <= m < 4GB | 256MB, 512MB, 1GB, 2GB | 2GB |
| 4GB <= m < 8GB | 512MB, 1GB, 2GB, 4GB | 4GB |
| 8GB <= m < 16GB | 1GB, 2GB, 4GB | 4GB |
| 16GB <= m < 32GB | 2GB, 4GB | 4GB |
| 32GB <= m < 2TB | 4GB | 4GB |

## Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command and use it again specifying a suitable parameter. |

| | |
|---|---|
| 10 | ▪ A file system with the same name already exists. Enter another file system name.<br>▪ The total disk capacity of the selected device files exceeds 2 TB. Select device files whose total disk capacity is no more than 2 TB and use the command again.<br>▪ Two or more device files are selected, even though `-v do_not_use` is specified. Two or more device files can only be selected when using a volume manager. Select only one device file and use the command again.<br>▪ The number of file systems has already reached the maximum number. Delete an unnecessary file system and use the command again.<br>▪ The selected size of the file system division exceeds the file system capacity. Select a size for the file system division that is no larger than the file system capacity and use the command again.<br>▪ Another file system is using the specified device file, so the selected device file cannot be used. Specify another device file and use the command again.<br>▪ The number of file systems using the volume manager has already reached the maximum number. Delete unnecessary file systems using the volume manager and use the command again.<br>▪ An error exists in the combination of the device file, division size, and log size. Specify correct parameters.<br>▪ The specified LU does not exist. Check the specified LU and use the command again.<br>▪ An error occurred in the specified device files. Check the specified device files, and then try again. If this error occurs repeatedly, acquire all Management log files and contact your HDS representative.<br>▪ An attempt was made to create more than the maximum number of logical volumes. Delete unnecessary file systems that are using the volume manager or release differential-data storage devices that are used by NAS Sync Image and use the command again.<br>▪ An attempt was made to create more than the maximum number of volume groups. Delete unnecessary file systems that are using the volume manager and retry.<br>▪ A specified device file is less than 65 MB. When using volume manager, the size of each selected device file must be no less than 65 MB.<br>▪ The total disk capacity of the specified device files is too low to create the file system. Specify device files that satisfy the conditions for creating the file system. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a few minutes and use the command again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | ▪ Recognition of a device file failed because of an unexpected error in internal processing. Another node in the cluster is rebooting, a deleted device file might be specified, or a problem may exist in the recognition processing of a device file. Wait a few minutes and use the command again. If the error occurs again, make sure the specified device file is deleted. If not, acquire all the Management log files and inform your HDS representative.<br>▪ The operations of the file system function cannot be performed because failover occurred. Use manual failover to return to the normal state from the failover state and use the command again.<br>▪ A resource group is OFFLINE. Put the resource group ONLINE and use the command again. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 96 | In the cluster, nodes that cannot synchronize exist. The LAN cable might have been disconnected. Make sure that the LAN cable is connected. Also, the synchronization processing might not have completed because one of the nodes is heavily loaded. In this case, make sure that the state of the node changes to normal (that is, not heavily loaded) and use the command again. If the error occurs again, inform your HDS representative. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform your HDS representative. |
| 98 | Some other error occurred. |

| | |
|---|---|
| 99 | ▪ The file system creation failed because of an unexpected error in internal processing. A problem may exist in the creation processing of a file system. Acquire all the Management log files and inform your HDS representative.<br>▪ Information acquisition of a device file failed because of an unexpected error in internal processing. A problem may exist in the information acquisition processing of a device file. Acquire all the Management log files and inform your HDS representative.<br>▪ Access to the NAS Cluster Management LU failed. Acquire all the Management log files and inform your HDS representative.<br>▪ Acquisition of the device file information from the NAS Cluster Management LU failed. Acquire all the Management log files and inform your HDS representative.<br>▪ Updating of the device file information of the NAS Cluster Management LU failed. Acquire all the Management log files and inform your HDS representative.<br>▪ Acquisition of file system information from the NAS Cluster Management LU failed. Acquire all the Management log files and inform your HDS representative.<br>▪ Updating of the file system information of the NAS Cluster Management LU failed. Acquire all the Management log files and inform your HDS representative.<br>▪ Acquisition of the number of file system information items about the NAS Cluster Management LU failed. Acquire all the Management log files and inform your HDS representative.<br>▪ An internal error occurred. A conflict with another system administrator's operation or system error may have occurred. Use the command again. Acquire all the Management log files if the error occurs again, and then inform your HDS representative.<br>▪ An attempt to acquire resource group information failed. A problem may exist in the internal processing. Acquire all the Management log files and inform your HDS representative.<br>▪ An attempt to register resource information failed. A problem may exist in the internal processing. Acquire all the Management log files and inform your HDS representative.<br>▪ An attempt to create a file system failed. The specification device file may invalid. Make sure the specified device file is valid.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and inform your HDS representative. |

- **Example**

  Following is an example of creating the file system `FS_1` by specifying the device file name `lu1A`:

  **$ sudo enas_fscreate FS_1 lu1A**

### To create a file system according to the following conditions:

- The maximum capacity that can be used as an i-node is 50% of the file system capacity.
- The size of the area used for logging is 128 MB.
- The division size is 4 GB.
- A volume manager is to be used.
- File creation times are to be recorded.
- The file system name is `FS_1`.
- The device files `/dev/enas/lu2B` and `/dev/enas/lu3C` are to be used.

```
$ sudo enas_fscreate -i 50 -l 128 -d 4G -v use -c on FS_1 lu2B,lu3C
```

### 6.2.18 enas_fsdelete (Delete a File System)

- **Synopsis**

  `enas_fsdelete -h|`*`file-system-name`*

- **Description**

  Deletes a file system. You cannot delete the following file systems or snapshots:

  - File systems for which copy devices are defined by NAS Backup Restore
  - Snapshots taken by NAS Backup Restore
  - File systems for which a differential-data storage device has been set by NAS Sync Image
  - Differential-data snapshots created by using NAS Sync Image

  When you want to delete the file systems and snapshots described above, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide* or the *Hitachi AMS/WMS NAS Sync Image User's Guide*.

- **Arguments and Options**

  **`-h`**

  Specify this if you want to output the command format to the standard error.

  ***file-system-name***

  Specify the name of the file system to be deleted.

**Return values**

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command and use it again, specifying a suitable parameter. |
| 10 | ▪ The specified file system does not exist. A file system that is not registered in the system may have been specified. Use the `enas_fslist` command to check the status of the specified file system and use the command again.<br>▪ The file system is mounting, so deleting cannot be performed. Delete the file system again after unmounting.<br>▪ The NAS Backup Restore is currently using this file system, so the file system cannot be operated. Perform the operation from NAS Backup Restore.<br>▪ The file system cannot be operated because NAS Sync Image is currently using this file system. Use the operation from NAS Sync Image.<br>▪ The operation is not possible because the remote copy function of NAS Backup Restore is using the file system. Wait until the remote copy function of NAS Backup Restore is finished and use the command again.<br>▪ The operation cannot be performed because the specified file system is defined by the other node in the cluster. On the other node of the cluster, perform the operation for the specified file system. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then use again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | The operations of the file system function cannot be performed because failover occurred. Use manual failover to return to the normal state from the failover state and use the command again. |

| | |
|---|---|
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 96 | In the cluster, nodes that cannot synchronize exist. The LAN cable might have been disconnected. Make sure that the LAN cable is connected. Also, the synchronization processing might not have completed because one of the nodes is heavily loaded. In this case, make sure that the state of the node changes to normal (that is, not heavily loaded) and use the command again. If the error occurs again, inform your HDS representative. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform your HDS representative. |
| 98 | Some other error occurred. |
| 99 | ▪ Access to the NAS Cluster Management LU failed. Acquire all the Management log files and inform your HDS representative.<br>▪ Acquisition of the device file information from the NAS Cluster Management LU failed. Acquire all the Management log files and inform your HDS representative.<br>▪ Updating of the device file information of the NAS Cluster Management LU failed. Acquire all the Management log files and inform your HDS representative.<br>▪ Acquisition of file system information from the NAS Cluster Management LU failed. Acquire all the Management log files and inform your HDS representative.<br>▪ Updating of the file system information of the NAS Cluster Management LU failed. Acquire all the Management log files and inform your HDS representative.<br>▪ An internal error occurred. A conflict with another system administrator's operation or system error may have occurred. Use the command again. Acquire all the Management log files if the error occurs again, and inform your HDS representative.<br>▪ An attempt to acquire resource group information failed. A problem may exist in the internal processing. Acquire all the Management log files and inform your HDS representative.<br>▪ An attempt to delete resource information failed because the node status is not UP, or a problem exists in internal processing. If the node status is not UP, change the node status to UP, and then re-use. If it is UP, acquire all the Management log files and inform your HDS representative.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and inform your HDS representative. |

- **Example**

  To delete the file system `FS_1`:

  **$ sudo enas_fsdelete FS_1**

### 6.2.19 enas_fsctl (Manage an active file system)

#### Synopsis

```
enas_fsctl -f [-s|-u]
  -a|file-system-name[ file-system-name...]
enas_fsctl -m [-s|-u]
  [-o monitoring-target=warning-threshold
  [,monitoring-target=warning-threshold]]
  -a|file-system-name[ file-system-name...]
enas_fsctl -c [-s|-u] [-o create_time]
  -a|file-system-name[ file-system-name...]
enas_fsctl -c -x
  file-system-name[ file-system-name...]|directory-name[ directory-name...]
enas_fsctl -l -a|file-system-name[ file-system-name...]
enas_fsctl -i
enas_fsctl -h
```

#### Description

Manages the following settings for specific file systems:

- Enables and disables automatic failover that occurs when a file system is blocked (`-f` option). [#1]

  The same operations can be performed as with the `enas_fsautofo` command.

- Enables and disables warning notification that is sent when file system usage exceeds a threshold value (`-m` option). [#1]

  The same operations can be performed as with the `enas_fsfullmsg` command.

- Enables and disables recording of the creation time for files in the file system (`-c` option). [#1]

  This command can also set creation times for existing files (`-x` option).

- Displays the access suppression status for a file system (`-l` option).

  [#1] If you omit both the `-s` option and `-u` option, the current settings are displayed for each file system. You can change settings in either normal mode or interactive mode (`-i` option).

We recommend that you specify the service IP address when you log in if you want to use this command.

#### Options and arguments

**`-a`**

Specify this option if you want to enable or disable automatic failover for all file systems mounted on the node to which you are logged in. If the command processing fails for any file system, processing continues for the other file systems.

**-c**

Specify this option to enable or disable extended attributes for the file system, or to view the extended attribute settings.

**-f**

Specify this option to enable or disable automatic failover that occurs when a file system is blocked, or to view the automatic failover settings.

**-h**

Specify this option if you want to view the command syntax.

**-i**

Specify this option to execute this command in interactive mode.

**-l**

Specify this option to display the access suppression status for a file system.

**-m**

Specify this option to enable or disable the warning notification that is sent when file system usage exceeds a threshold value, or to view the warning notification settings.

**-o create_time**

Specify this to enable or disable recording of the creation time for files in the file system, or to view the creation time settings. Specify this option with the `-c` option.

**-o** ***monitoring-target*=*warning-threshold*** **[** ***, monitoring-target*=*warning-threshold*** **]**

Specify this option with the `-m` option and the `-s` option. Specify a parameter to be monitored and a threshold value for issuing a warning. If you omit this option, the currently set warning threshold value will be inherited.

If you specify `0` as the threshold value, a warning will be issued only when file system usage reaches the upper limit.

`blimit=`*warning-threshold*

Specify the threshold value in bytes or as a percentage (`%`) when you monitor file system usage by the number of blocks used.

To specify the value in bytes:

Specify the numeric value followed by the first letter of the unit such as `M` for megabytes or `G` for gigabytes.

If the unit is MB: `blimit=500M`

If the unit is GB: `blimit=5G`

To specify the value as a percentage (%):

Specify the numeric value followed by the letter p.

Example: blimit=80p

When you specify a percentage (%), the value is converted to bytes and set as the threshold value. Since the byte value is not re-calculated when the file system size is increased, the warning threshold value remains unchanged.

ilimit=*warning-threshold*

Specify the threshold value as the number or percentage (%) of i-nodes that can be used when you monitor file system usage by the i-node count.

To specify the value as the number of i-nodes:

Example: ilimit=9000

To specify the value as a percentage (%):

Specify the numeric value followed by the letter p.

Example: ilimit=80p

When you specify a percentage (%), the value is converted to the number of i-nodes out of the total number of i-nodes available at the time of command execution, and is set as the threshold value.

The total number of i-nodes available in a file system changes dynamically depending on the file system usage. Therefore, since the percentage value is not re-calculated when the file system size is increased, the threshold value remains unchanged.

**-s**

Specify this option in the following cases:

- With the -f option to enable automatic failover that occurs when a file system is blocked
- With the -m option to enable the warning notification that is sent when file system usage exceeds a threshold value
- With the -c option to enable recording of the creation time for files in the file system

**-u**

Specify this option in the following cases:

- With the -f option to disable automatic failover that occurs when a file system is blocked
- With the -m option to disable the warning notification that is sent when file system usage exceeds a threshold value
- With the -c option to disable recording of the creation time for files in the file system

**-x**

Specify this option to set the creation time for existing files. Specify this option with the `-c` option.

The oldest time of the last access time (`atime`), last change time (`ctime`), and last modification time (`mtime`) is set as the creation time. The command processing for this option takes approximately one minute per 100,000 files that are contained in the specified file When you execute the command, `Wait ...` is displayed and then a period (`.`) is displayed each time 10,000 files are processed.

***file-system-name*[ *file-system-name*...]**

Specify the file system names if you want to apply settings to the specified file systems only. You can use an asterisk (`*`) or question mark (`?`) as a wildcard. Delimit multiple file system names with spaces.

***directory-name*[ *directory-name*...]**

Specify directory paths from the mount point if you want the processing to apply to the specified directories only. For example, to set the `dir01` directory (`/mnt/filesystem01/dir01`) under `/mnt/filesystem01`, specify `filesystem01/dir01`. You can use an asterisk (`*`) or question mark (`?`) as a wildcard. Delimit multiple file system names with spaces.

## Subcommands

You can display the associated prompt by specifying `autofo`, `fullmsg`, or `extfunc` after `func`. An execution example in interactive mode and the subcommands are described below.

| Line | Example |
|---|---|
| 1 | `$ sudo enas_fsctl -i` |
| 2 | `fsctl> func fullmsg` |
| 3 | `fsctl fullmsg> list filesystem1` |
| 4 | `filesystem1  Off(50G,50000)` |
| 5 | `fsctl fullmsg> set -o blimit=80G,ilimit=80000 filesystem1` |
| 6 | `fsctl fullmsg> exit` |
| 7 | `fsctl> exit` |

1: Executes the `enas_fsctl` command in interactive mode.

2: Calls for a subcommand to enable or disable warning notification that is sent when file system usage exceeds a threshold value.

3: Displays the settings for file system `filesystem1`.

4: These are the settings for file system `filesystem1`.

5: Sets a warning threshold value for file system `filesystem1`.

6: Ends the subcommand for the enabling/disabling warning notification that is sent when the file system usage exceeds a threshold value.

7: Ends the `enas_fsctl` command.

**`exit`**

Specify this if you want to end the `enas_fsctl` command or its subcommand.

**`func autofo`**

Specify this to enable or disable automatic failover that occurs when a file system is blocked, or to view the automatic failover settings. When the prompt is displayed, you can execute subcommands in the following formats:

```
list [-a|file-system-name[ file-system-name...]]
set -a|file-system-name[ file-system-name...]
unset -a|file-system-name[ file-system-name...]
```

`list`

Displays whether automatic failover is enabled or disabled.

`set`

Enables automatic failover.

`unset`

Disables automatic failover.

File system names and the `-a` option can be specified and are handled the same way as in normal mode.

**`func extfunc`**

Specify this to enable or disable extended attributes for the file system, or to view the extended attribute settings. When the prompt is displayed, you can execute subcommands in the following formats:

```
list [-o create_time] [-a|file-system-name[ file-system-name...]]
set [-o create_time] -a|file-system-name[ file-system-name...]
unset [-o create_time] -a|file-system-name[ file-system-name...]
set_ctime directory-name[ directory-name...]
set_ctime file-system-name[ file-system-name...]|
  directory-name[ directory-name...]
```

`list`

Displays whether recording of file creation times is enabled or disabled.

`set`

Enables recording of file creation times.

`unset`

Disables recording of file creation times.

`set_ctime`

Sets the creation times of existing files.

The command processing for this option takes approximately one minute per 100,000 files that are contained in the specified file system or directory. When you execute the command, `Wait ...` is displayed and then a period (`.`) is displayed each time 10,000 files are processed.

File system names, directory names, the `-a` option and `-o create_time` option can be specified and are handled the same way as in normal mode.

**`func fullmsg`**

Specify this to enable or disable the warning notification that is sent when file system usage exceeds a threshold value, or to view the warning notification settings. When the prompt is displayed, you can execute subcommands in the following formats:

```
list [-a|file-system-name[ file-system-name...]]
set [-o monitoring-target=warning-threshold
  [,monitoring-target=warning-threshold]]
  -a|file-system-name[ file-system-name...]
unset -a|file-system-name[ file-system-name...]
```

`list`

Displays whether the warning notification is enabled or disabled.

`set`

Enables the warning notification.

`unset`

Disables the warning notification.

The `-o` option, `-a` option, and file system names can be specified and are handled the same way as in normal mode.

**`help`**

Specify this to view the syntax of the subcommands that can be executed in interactive mode.

**`quit`**

Specify this if you want to end the `enas_fsctl` command or its subcommand.

## Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.18 Information displayed when executing the enas_fsctl command**

| Item | Description |
|---|---|
| *file-system-name* | Displays the file system name. (when the -f, -m or -i option is specified) |
| *status* | Displays the current settings.<br>`On`<br>The settings are enabled.<br>`Off`<br>The settings are disabled.<br>If the `-m` option has been specified, the thresholds for the block usage and i-node usage are also displayed. |
| `Filesystem` | Displays the file system name. (when the -c option is specified) |
| `Create_time` | Displays whether the recording of the file creation time has been enabled.<br>`On`<br>The recording of the file creation time has been enabled.<br>`Off`<br>The recording of the file creation time has been disabled. |
| `Filesystem` | Displays the file system name (when the -l option is specified) |
| `Status` | Displays the access suppression status for a file system.<br>`Normal`<br>Access from clients has not been suppressed.<br>`Frozen`<br>Access from clients has been suppressed. |

## Return values

### Value returned when the `-f` option is specified:

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ There are too many or too few parameters. Check the command format, specify a correct parameter, and then try again.<br>▪ If a syntax error occurred, check the command format, and then try again.<br>▪ The specified file system is invalid. Specify a correct file system name, and then try again.<br>▪ If multiple file systems are specified, processing might have terminated abnormally for one of the file systems. Specify the name of the file system for which the processing terminated abnormally, and then try again. |
| `10` | ▪ The specified file system is not mounted. If multiple file systems are specified, processing will continue. If the file system is not mounted, mount it or specify a correct file system name, and then try again.<br>▪ An attempt to specify the settings failed because the file system is full. If multiple file systems are specified, processing will continue. Make some free space on the file system, and then try again.<br>▪ An attempt to specify the settings failed because the file system is mounted with read-only permissions. If multiple file systems are specified, processing will continue. Remount the file |

| | |
|---|---|
| | system with read/write permissions, and then try again. |
| 99 | ▪ The specified file system is not in a normal state. Check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to acquire mount information has failed. There might be a problem in the NAS OS LU or in the processing for acquiring mount information. Check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to access management information about the file system has failed. The specified file system might have a problem or contention with other processing might have occurred. Wait a while, and then try again. If the error occurs again, check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to open the log files has failed. There might be a problem in the log files or contention with other processing might have occurred. Wait a while, and then try again. If the error occurs again, check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel. |

### Value returned when the `-m` option is specified:

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ There are too many or too few parameters. Check the command format, specify a correct parameter, and then try again.<br>▪ If a syntax error occurred, check the command format, and then try again.<br>▪ The specified file system is invalid. Specify a correct file system name, and then try again.<br>▪ If multiple file systems are specified, processing might have terminated abnormally for one of the file systems. Specify the name of the file system for which the processing terminated abnormally, and then try again.<br>▪ The method for specifying the warning threshold was invalid. Respecify the warning threshold, and then try again.<br>▪ There is an error in the specification of the `-o` option. Confirm the correct syntax, correct the syntax error, and then re-execute the command. |
| 10 | ▪ The specified file system is not mounted. If multiple file systems are specified, processing will continue. If the file system is not mounted, mount it or specify a correct file system name, and then try again.<br>▪ An attempt to specify the settings failed because the file system is full. If multiple file systems are specified, processing will continue. Make some free space on the file system, and then try again.<br>▪ The specified threshold value that triggers a warning notification exceeds the capacity of the file system. For the threshold that triggers a warning notification, specify a value that is equal to or less than the file system capacity.<br>▪ An attempt to specify the settings failed because the file system is mounted with read-only permissions. If multiple file systems are specified, processing will continue. Remount the file system with read/write permissions, and then try again. |
| 99 | ▪ The specified file system is not in a normal state. Check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to acquire mount information has failed. There might be a problem in the NAS OS LU or in the processing for acquiring mount information. Check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to access management information about the file system has failed. The specified file system might have a problem or contention with other processing might have occurred. Wait a while, and then try again. If the error occurs again, check whether an error occurred in |

| | |
|---|---|
| | the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to open the log files has failed. There might be a problem in the log files or contention with other processing might have occurred. Wait a while, and then try again. If the error occurs again, check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel. |

### Value returned when the `-c` option is specified:

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ There are too many or too few parameters. Check the command format, specify a correct parameter, and then try again.<br>▪ If a syntax error occurred, check the command format, and then try again.<br>▪ The specified file system is invalid. Specify a correct file system name, and then try again.<br>▪ If multiple file systems or directories are specified, processing might have terminated abnormally for one of the file systems or directories. Specify the name of the file system or directory for which the processing terminated abnormally, and then try again.<br>▪ There is a syntax error for the `-o` option. Check the format, correct the syntax error, and then try again. |
| 10 | ▪ The specified file system is not mounted. If multiple file systems are specified, processing will continue. If the file system is not mounted, mount it or specify a correct file system name, and then try again.<br>▪ An attempt to specify the settings failed because the file system is full. If multiple file systems are specified, processing will continue. Make some free space on the file system, and then try again.<br>▪ Recording of creation times is disabled. Enable recording of file creation times, and then try again.<br>▪ The target file system or directory does not exist. Check the specified file system or directory, and then try again.<br>▪ The specified path is not a directory. Specify a directory, and then try again.<br>▪ An attempt to specify the settings failed because the file system is mounted with read-only permissions. If multiple file systems are specified, processing will continue. Remount the file system with read/write permissions, and then try again. |
| 99 | ▪ The specified file system is not in a normal state. Check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to acquire mount information has failed. There might be a problem in the NAS OS LU or in the processing for acquiring mount information. Check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to access management information about the file system has failed. The specified file system might have a problem or contention with other processing might have occurred. Wait a while, and then try again. If the error occurs again, check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to open the log files has failed. There might be a problem in the log files or contention with other processing might have occurred. Wait a while, and then try again. If the error occurs again, check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel. |

### Value returned when the -l option is specified:

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ There are too many or too few parameters. Check the command format, specify a correct parameter, and then try again.<br>▪ If a syntax error occurred, check the command format, and then try again.<br>▪ The specified file system is invalid. Specify a correct file system name, and then try again.<br>▪ If multiple file systems are specified, processing might have terminated abnormally for one of the file systems. Specify the name of the file system for which the processing terminated abnormally, and then try again. |
| 2 | Access from clients to the specified file system has been suppressed. |
| 10 | The specified file system is not mounted. If multiple file systems are specified, processing will continue. If the file system is not mounted, mount it or specify a correct file system name, and then try again. |
| 99 | ▪ The specified file system is not in a normal state. Check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to acquire mount information has failed. There might be a problem in the NAS OS LU or in the processing for acquiring mount information. Check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to access management information about the file system has failed. The specified file system might have a problem or contention with other processing might have occurred. Wait a while, and then try again. If the error occurs again, check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to open the log files has failed. There might be a problem in the log files or contention with other processing might have occurred. Wait a while, and then try again. If the error occurs again, check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel. |

## Examples

### To check whether automatic failover that occurs when file system FS_1 is blocked is enabled or disabled:

```
$ sudo enas_fsctl -f FS_1
 FS_1       On
```

### To enable the warning notification that is sent when usage of file system FS_1 exceeds a threshold value according to the following conditions:

- The warning threshold for block usage is 80G.
- The warning threshold for i-node usage is 20,000.

```
$ sudo enas_fsctl –m -s blimit=80G,ilimit=20000 FS_1
```

### To set the creation times for the existing files (100,000 in total) in file system FS_1:

```
$ sudo enas_fsctl -c -x FS_1
FS_1: Wait ..............  Success
```

**To enable automatic failover that occurs when a file system is blocked (interactive mode):**

1. Start interactive mode.
2. Check whether automatic failover is enabled.
3. Enable automatic failover that occurs when a file system is blocked.

Interactive mode is exited.

```
$ sudo enas_fsctl -i
fsctl> func autofo
fsctl autofo> list -a
 filesystem1   Off
 filesystem2   Off
fsctl autofo> set -a
fsctl autofo> exit
fsctl> exit
```

### 6.2.20 enas_fslist (List File System Information)

- **Synopsis**

  `enas_fslist -h|[-c] [-d] [`*file-system-name*`]`

- **Description**

  Displays information related to one or more file systems. When a resource group is failed over from one node in the cluster, this command also displays information about the file systems belonging to that resource group.

  If the file system uses the NAS Sync Image differential-data snapshot function, the information for the snapshots is also displayed.

**Table 6.19 Information Displayed enas_fslist is Used**

| Item | Description |
|---|---|
| `File system(used by)` | Displays the file system name.<br>If a snapshot has been taken by NAS Backup Restore, the snapshot name is displayed as follows:<br>*snapshot-name*`(Backup Restore)`<br>When using NAS Backup Restore to define a copy device, the file system for which the copy device is defined is displayed as follows:<br>*file-system-name*`(Backup Restore)`<br>If a differential-data snapshot has been created and mounted by NAS Sync Image, the mount point directory name of the differential-data snapshot is displayed as follows:<br>*mount-point-directory-name-of-differential-data-snapshot*`(Sync Image)`<br>The file system for which a differential-data storage device has been set by using NAS Sync Image is displayed as follows:<br>*file-system-name*`(Sync Image)` |
| `Total disk capacity(GB)` | Displays the file system capacity.<br>For a NAS Backup Restore snapshot, the snapshot capacity is displayed.<br>For a NAS Sync Image differential-data snapshot, the file system capacity of the creation source is displayed. |
| `Device status` | Displays the status of device files that constitute the file system.<br>For a NAS Backup Restore snapshot, the status of device files that constitute the copy device is displayed.<br>For a NAS Sync Image differential-data snapshot, the status of device files that constitute the differential-data storage device and the creation source file system is displayed.<br>The following values are displayed:<br>`normal`<br>Displayed if the device is not blocked.<br>`error`<br>Displayed if the device is blocked. |

| Item | Description |
|---|---|
| `Device files` | Displays device file names that are used in the file system.<br>If the `-d` option is specified, the drive type is displayed to the right of the device file name. Either of the following is displayed as the drive type:<br>`(FC)`<br>This is displayed for an FC drive.<br>`(SATA)`<br>This is displayed for a SATA drive.<br>For a NAS Sync Image differential-data snapshot, device file names that are used in the creation source file system and the differential-data storage device are displayed.<br>When multiple device files are displayed, they are separated by spaces.<br>Examples when there is one device file (where *XX* is a hexadecimal number):<br>`lu`*XX*<br>Examples when there is more than one device file (where *XX* is a hexadecimal number):<br>`lu`*XX* `lu`*XX* `...` |
| `Block used(GB)` | Displays the amount of used blocks when the file system is mounted properly.<br>This is not displayed when the file system is not mounted properly. |
| `Block free(GB)` | Displays the amount of unused blocks when the file system is mounted properly.<br>This is not displayed when the file system is not mounted properly. |
| `I-node used` | Displays the number of used i-nodes when the file system is mounted properly.<br>This is not displayed when the file system is not mounted properly. |
| `I-node free` | Displays the number of unused i-nodes when the file system is mounted properly.<br>This is not displayed when the file system is not mounted properly. |
| `Volume manager` | Displays whether the file system uses the volume manager.<br>For a NAS Backup Restore snapshot, it displays whether the taking source file system uses the volume manager.<br>The following values are displayed:<br>`use`<br>Displayed if the file system uses the volume manager.<br>`--`<br>Displayed if the file system does not use the volume manager.<br>For a NAS Sync Image differential-data snapshot, `use` is displayed. |

| Item | Description |
|---|---|
| `Mount status` | Displays the mount status of the file system.<br>For a NAS Backup Restore snapshot, the mount status of the snapshot is displayed.<br>For a NAS Sync Image differential-data snapshot, the status of the mounted differential-data snapshot is displayed.<br>The following values are displayed:<br>`ro`<br>Displayed if the file system is read-only.<br>`rw`<br>Displayed if both read and write operations are permitted.<br>`overflow`<br>Displayed if the capacity of the NAS Sync Image differential-data storage device is insufficient.<br>`error`<br>Displayed if the file system is blocked.<br>Unmount the file system and then mount it again. If this does not resolve the blocked status, contact your HDS representative.<br>If this value is displayed for a NAS Backup Restore snapshot, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide.* If this value is displayed for a NAS Sync Image differential-data snapshot, see the *Hitachi AMS/WMS NAS Sync Image User's Guide.*<br>`fatal error`<br>Displayed if the file system is blocked. Delete the file system and contact your HDS representative.<br>`--`<br>Displayed if the file system is not mounted. |
| `Quota` | Displays the Quota setting at the time of mounting.<br>For a NAS Backup Restore snapshot, the Quota setting when the snapshot was taken is displayed.<br>For a NAS Sync Image differential-data snapshot, the Quota setting when the differential-data snapshot was created is displayed.<br>The following values are displayed:<br>`on`<br>Displayed if the Quota setting is enabled.<br>`off`<br>Displayed if the Quota setting is disabled.<br>`--`<br>Displayed if the file system is not mounted.<br>If the device file or the file system is blocked, the status in effect before the occurrence of the failure is displayed.<br>Additionally, when `off` appears after a failure, one of the following has occurred:<br>▪ The Quota setting from before the failure was disabled, and operations continued.<br>▪ The Quota setting from before the failure was enabled, and operations continued. However, the status was changed when, for example, an unmount operation was performed after the failure. |

- **Arguments and Options**

**Table 6.20 enas_fslist Arguments and Options**

| Item | Use |
|---|---|
| `-h` | Specify this option if you want to view the command syntax. |
| `-c` | Separates the output of each file system's information using colons ( **:** ). For example:<br>*`File-system(used-by):Total-disk-capacity(GB)`*`: - :`*`Quota`*<br>*`File-system(used-by):Total-disk-capacity(GB)`*`: - :`*`Quota`*<br>`:`<br>`: (Information is output for each file system.)`<br>`:`<br>If you omit this option, information is displayed in a detailed format. For example:<br>**List of File Systems**:<br>The number of file systems (counter) (1)<br>*item-name*: value<br>:<br>: (All items are output.)<br>:<br>(One blank line) (2)<br>:<br>: ((1) through (2) is output for each file system.)<br>:<br>counter: The value starts from 1, and a number is assigned to each file system.<br>item-name: An item in Table 6.6 is displayed.<br>value: The value of an item in Table 6.6 is displayed. |
| `-d` | Specify this to enable drive type indication. |
| *file-system-name* | The name of the file system to be displayed. Use to display information on a specific file system. If you do not specify a file system name, information about all the file systems on the node will be displayed. |

- **Examples**
  - To display the information on file systems specifying the `-c` option:

```
$ sudo enas_fslist –c
FS_1:13.754:normal:lu0C lu0D:0.192:13.562:5:14352379:use:rw:on
FS_2:6.877:normal:lu03:::::--:--:--
```

  - To display the information on file systems without specifying the `-c` option:

```
$ sudo enas_fslist
List of File Systems:
The number of file systems(1)
 File system(used by)  : FS_1
 Total disk capacity(GB) : 13.754
 Device status      : normal
 Device files      : lu0C lu0D
 Block used (GB)     : 0.192
 Block free (GB)     : 13.562
 I-node used       : 5
 I-node free       : 14352379
 Volume manager     : use
 Mount status      : rw
 Quota          : on

The number of file systems(2)
 File system(used by)  : FS_2
 Total disk capacity(GB) : 6.877
 Device status      : normal
 Device files      : lu03
 Block used(GB)     :
 Block free(GB)     :
 I-node used       :
 I-node free       :
 Volume manager     : --
 Mount status      : --
 Quota          : --
```

– To display the information on file system FS_1 by specifying the -d option to enable device type indication:

```
$ sudo enas_fslist -d FS_1
List of File Systems:
The number of file systems(1)
 File system(used by)  : FS_1
 Total disk capacity(GB) : 60.000
 Device status      : normal
 Device files      : lu00(FC) lu01(FC) lu10(SATA) lu11(SATA)
 Block used (GB)     : 1.194
 Block free (GB)     : 58.806
 I-node used       : 5
 I-node free       : 14352379
 Volume manager     : use
 Mount status      : rw
 Quota          : on
```

### 6.2.21 enas_fsfullmsg (Manage warning notification functionality)

#### Synopsis

```
enas_fsfullmsg [-s|-u]
  [-o monitoring-target=warning-threshold
  [,monitoring-target=warning-threshold]]
  {-a|file-system-name[ file-system-name...]
enas_fsfullmsg -h
```

#### Description

Enables or disables the warning notification that is sent when file system usage exceeds a threshold value. Also displays the warning notification settings.

We recommend that you specify the service IP address when you log in if you want to use this command.

If you omit the `-s` option and `-u` option, the warning notification settings are displayed for each file system.

Even if you disable the warning notification, the previously set threshold value is saved. You can therefore omit the `-o` option if you want to apply the same threshold value when you next enable the warning notification.

#### Options and arguments

**`-a`**

Specify this option if you want to enable or disable automatic failover for all file systems mounted on the node to which you are logged in. If the command processing fails for any file system, processing continues for other file systems.

**`-h`**

Specify this option if you want to view the command syntax.

**`-o`** ***monitoring-target*=*warning-threshold*** **`[`** ***, monitoring-target*=*warning-threshold*** **`]`**

Specify this option if you specify the `-s` option. Specify the warning threshold value to trigger notification of the monitored target and warnings. If you omit this option, the currently set threshold value will be inherited.

If you specify `0` as the warning threshold value, a warning will be issued only when file system usage reaches the upper limit.

`blimit=`*warning-threshold*

You can monitor file system usage by the number of blocks used. Specify the threshold value in bytes or as a percentage (`%`).

To specify the value in bytes:

Specify the numeric value followed by the first letter of the unit such as `M` for megabytes or `G` for gigabytes.

If the unit is MB: `blimit=500M`

If the unit is GB: `blimit=5G`

To specify the value as a percentage (`%`):

Specify the numeric value followed by the letter `p`.

Example: `blimit=80p`

If the value is specified as a percentage (`%`), the value is converted to bytes and set and displayed as the warning threshold value. Since the byte value is not re-calculated when the file system size is increased, the warning threshold value remains unchanged.

`ilimit=`***warning-threshold***

Specify the threshold value as the number or percentage (`%`) of i-nodes that can be used when you monitor file system usage by the i-node count.

To specify the value as the number of available i-nodes:

Example: `ilimit=9000`

To specify the value as a percentage (`%`):

Specify the numeric value followed by the letter `p`.

Example: `ilimit=80p`

When you specify a percentage (`%`), the value is converted to the number of i-nodes out of the total number of i-nodes available at the time of command execution, and is set as the threshold value.

The total number of i-nodes available in a file system changes dynamically depending on the file system usage. Therefore, since, the percentage value is not re-calculated when the file system size is increased, the threshold value remains unchanged.

**`-s`**

Specify this option to enable the warning notification that is sent when file system usage exceeds the threshold value.

**`-u`**

Specify this option to disable the warning notification that is sent when file system usage exceeds the threshold value.

***file-system-name*`[` *file-system-name*`...]`**

Specify the file system names if you want to apply settings to the specified file systems only. You can use an asterisk (`*`) or question mark (`?`) as a wildcard. Delimit multiple file system names with spaces.

## Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.21 Information displayed when executing the enas_fsfullmsg command**

| Item | Description |
|---|---|
| *file-system-name* | Displays the file system name. |
| *setting* | Displays whether the warning notification that is sent when file system usage exceeds a threshold value is enabled.<br>`On`<br>Warning notification is enabled.<br>`Off`<br>Warning notification is disabled. |
| *block-usage-threshold* | Displays the threshold value for block usage. |
| *i-node-usage-threshold* | Displays the threshold value for i-node usage. |

## Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ The method for specifying the warning threshold was invalid. Respecify the warning threshold, and then try again.<br>▪ There are too many or too few parameters. Check the command format, specify a correct parameter, and then try again.<br>▪ If a syntax error occurred, check the command format, and then try again.<br>▪ The specified file system is invalid. Specify a correct file system name, and then try again.<br>▪ If multiple file systems are specified, processing might have terminated abnormally for one of the file systems. Specify the name of the file system for which the processing terminated abnormally, and then try again.<br>▪ There is an error in the specification of the `-o` option. Confirm the correct syntax, correct the syntax error, and then re-execute the command. |
| `10` | ▪ The specified file system is not mounted. If multiple file systems are specified, processing will continue. If the file system is not mounted, mount it or specify a correct file system name, and then try again.<br>▪ An attempt to specify the settings failed because the file system is full. If multiple file systems are specified, processing will continue. Make some free space on the file system, and then try again.<br>▪ The specified threshold that trigger a warning notification exceeds the capacity of the file system. For the threshold that triggers a warning notification, specify a value that is equal to or less than the capacity of the file system.<br>▪ An attempt to specify the settings failed because the file system is mounted with read-only permissions. If multiple file systems are specified, processing will continue. Remount the file system with read/write permissions, and then try again. |
| `99` | ▪ The specified file system is not in a normal state. Check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to acquire mount information has failed. There might be a problem in the NAS OS LU or in the processing for acquiring mount information. Check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel. |

| | |
|---|---|
| | ▪ An attempt to access management information about the file system has failed. The specified file system might have a problem or contention with other processing might have occurred. Wait a while, and then try again. If the error occurs again, check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to open the log files has failed. There might be a problem in the log files or contention with other processing might have occurred. Wait a while, and then try again. If the error occurs again, check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel. |

## Examples

### To enable the warning notification that is sent when used block space on a file system mounted on the local node exceeds 50 GB:

```
$ sudo enas_fsfullmsg -s blimit=50G -a
```

### To view the warning notification settings for file systems `FS_1` and `FS_2`:

```
$ sudo enas_fsfullmsg FS_1 FS_2
 FS_1       On(50G,50000)
 FS_2       Off(30G,30000)
```

### 6.2.22 enas_fsmount (Mount a File System)

- **Synopsis**

  `enas_fsmount {-r|-w [-u {update|do_not_update}] [-q {on|off}]` ***file-system-name***

  `enas_fsmount -r` ***file-system-name***

  `enas_fsmount -h`

- **Description**

  Mounts a file system. The number of file systems that can be mounted for one cluster is 256.

  Mounts a file system at the following mount point:

  /mnt/file-system-name

  The previous setting does not apply if you unmount and then re-mount the file system. If you omit the -u option or -q option, the default setting applies in each case.

- **Arguments and Options**

**Table 6.22 enas_fsmount Arguments and Options**

| Item | Use |
|---|---|
| `-h` | Specify this option if you want to view the command syntax. |
| `-r` | Do not permit writing to the file system. |
| `-w` | Permit writing to the file system. The `-u` and `-q` options are available only when you specify this option. |
| `-u {update\|do_not_update}` | Updates the last access time when the file system is accessed. This option is available only when you specify the `-w` option. If you omit this option, it defaults to `do_not_update`. When you unmount a file system and then remount it by executing the `enas_fsmoumt` command without specifying the `-u` option, it defaults to `do_not_update` even if `update` was set before the unmount.<br>▪ `update`<br>Use to update the last access time to the i-node access time.<br>▪ `do_not_update`<br>Specify if you do not want to update the last access time. |
| `-q {on\|off}` | Specify whether to enable the Quota function. This option is available only when you specify the `-w` option. If you omit this option, it defaults to `on`.<br>▪ `on`<br>Specify this to enable the quota function.<br>▪ `off`<br>Specify this to disable the quota function. |
| *file-system-name* | Specify the name of the file system to be mounted. |

**Return values**

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry |

| | |
|---|---|
| | specifying a suitable parameter. |
| 10 | ▪ The specified file system does not exist. A file system that is not registered in the system may have been specified. Use the `enas_fslist` command to check the status of the specified file system, and then retry the operation.<br>▪ The file system cannot be operated because NAS Sync Image is currently using this file system. Execute the operation from NAS Sync Image.<br>▪ The operation is not possible because the remote copy function of NAS Backup Restore is using the file system. Wait until the remote copy function of NAS Backup Restore is finished, and then retry execution.<br>▪ The specified file system is already mounted. In the **List of File Systems**, check the mount status of the specified file system.<br>▪ The operation cannot be performed because the specified file system is defined by the other node in the cluster. On the other node of the cluster, perform the operation for the specified file system. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node has stopped during processing, wait about 15 minutes or boot the stopped node. |
| 66 | ▪ The operations of the file system function cannot be performed because failover occurred. Use manual failover to return to the normal state from the failover state, and then retry.<br>▪ A resource group is OFFLINE. Put the resource group ONLINE, and then retry execution. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 80 | The file system is mounted with the Quota setting disabled because the file system is full. Even if you enable the Quota setting, the file system will be mounted with the Quota setting disabled because the file system is full. Delete unnecessary data on the file system or increase the file system capacity, and then enable the Quota setting and mount. |
| 96 | In the cluster, nodes that cannot synchronize exist. The LAN cable might have been disconnected. Make sure that the LAN cable is connected. Also, the synchronization processing might not have completed because one of the nodes is heavily loaded. In this case, make sure that the state of the node changes to normal (that is, not heavily loaded), and then retry the operation. If the error occurs again, inform maintenance personnel. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 98 | Some other error occurred. |
| 99 | ▪ Access to the NAS Cluster Management LU failed. Acquire all the Management log files and contact maintenance personnel.<br>▪ Acquisition of file system information from the NAS Cluster Management LU failed. Acquire all the Management log files and contact maintenance personnel.<br>▪ Updating of the file system information of the NAS Cluster Management LU failed. Acquire all the Management log files and contact maintenance personnel.<br>▪ An internal error occurred. A conflict with another system administrator's operation or a system error may have occurred. Retry execution. Acquire all the Management log files if the error occurs repeatedly, and then contact maintenance personnel.<br>▪ Execution cannot start because the status of the resource group is offline. Alternatively, a resource might have an error. If the resource group is offline, place the resource group online, and then re-execute. If it is not offline, see the explanation for the KAQG72006-E message.<br>▪ An attempt to acquire resource group information failed. A problem may exist in the internal processing. Acquire all the Management log files and contact maintenance personnel.<br>▪ The specified file system is blocked. Unmount and then delete the specified file system. Then, request maintenance personnel to recover the LU error. If necessary, create a new file system and then use backup data to restore the data. If the error occurs repeatedly, acquire all the |

| | |
|---|---|
| | Management log files and contact maintenance personnel.<br>▪ An attempt to register resource information failed. A problem may exist in the internal processing. Acquire all the Management log files and contact maintenance personnel.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and contact maintenance personnel. |

- **Example**

  To mount the file system `FS_1` with the following conditions:

  – Permit writing to `FS_1` (`-w`).

  – Enable the Quota setting (`-q`).

  **$ sudo enas_fsmount -w -q on FS_1**

### 6.2.23 enas_fsumount (Unmount a File System)

- **Synopsis**

  `enas_fsumount -h|`*`file-system-name`*

  `enas_fsumount -h`

- **Description**

  Unmounts a file system.

- **Arguments and Options**

  **`-h`**

  Specify this option if you want to view the command syntax.

  *`file-system-name`*

  Specify the name of the file system to be unmounted.

- **Example**

  To unmount the file system `FS_1`:

  ```
  $ sudo enas_fsumount FS_1
  ```

**Return values**

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| 10 | ▪ The specified file system does not exist. A file system that is not registered in the system may have been specified. Use the `enas_fslist` command to check the status of the specified file system, and then retry the operation.<br>▪ A CIFS file share exists, so unmounting is not possible. Delete the CIFS file share, and then retry unmounting of the file system.<br>▪ An NFS file share exists, so unmounting is not possible. Delete the NFS file share, and the then retry unmounting of the file system.<br>▪ The file system cannot be operated because NAS Sync Image is currently using this file system. Execute the operation from NAS Sync Image.<br>▪ The operation is not possible because the remote copy function of NAS Backup Restore is using the file system. Wait until the remote copy function of NAS Backup Restore is finished, and then retry execution.<br>▪ The specified file system is already unmounted. In the **List of File Systems**, check the mount status of the specified file system.<br>▪ The operation cannot be performed because the specified file system is defined by the other node in the cluster. On the other node of the cluster, perform the operation for the specified file system. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | ▪ The operations of the file system function cannot be performed because failover occurred. Use manual failover to return to the normal state from the failover state, and then retry.<br>▪ A resource group is OFFLINE. Put the resource group ONLINE, and then retry execution. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage* |

| | |
|---|---|
| | *Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 96 | In the cluster, nodes that cannot synchronize exist. The LAN cable might have been disconnected. Make sure that the LAN cable is connected. Also, the synchronization processing might not have completed because one of the nodes is heavily loaded. In this case, make sure that the state of the node changes to normal (that is, not heavily loaded), and then retry the operation. If the error occurs again, inform maintenance personnel. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 98 | Some other error occurred. |
| 99 | ▪ An attempt to determine whether a CIFS file share exists has failed. Acquire all the Management log files and contact maintenance personnel.<br>▪ An attempt to determine whether an NFS file share exists has failed. Acquire all the Management log files and contact maintenance personnel.<br>▪ Access to the NAS Cluster Management LU failed. Acquire all the Management log files and contact maintenance personnel.<br>▪ Acquisition of file system information from the NAS Cluster Management LU failed. Acquire all the Management log files and contact maintenance personnel.<br>▪ Updating of the file system information of the NAS Cluster Management LU failed. Acquire all the Management log files and contact maintenance personnel.<br>▪ An internal error occurred. A conflict with another system administrator's operation or a system error may have occurred. Retry execution. Acquire all the Management log files if the error occurs repeatedly, and then contact maintenance personnel.<br>▪ Execution cannot start because the status of the resource group is offline. Alternatively, a resource might have an error. If the resource group is offline, place the resource group online, and then re-execute. If it is not offline, see the explanation for the KAQG72006-E message.<br>▪ An attempt to acquire resource group information failed. A problem may exist in the internal processing. Acquire all the Management log files and contact maintenance personnel.<br>▪ An attempt to delete resource information failed because the node status is not UP, or a problem exists in internal processing. If the node status is not UP, change the node status to UP, and then re-execute. If it is UP, acquire all the Management log files and inform maintenance personnel.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and contact maintenance personnel. |

### 6.2.24 enas_ndstart (Start a node)

#### Synopsis

```
enas_ndstart [--] node-name
enas_ndstart -h
```

#### Description

Starts a specified node.

You can execute this command when the node is in `INACTIVE` state.

#### Options and arguments

**`-h`**

Specify this option if you want to view the command syntax.

`--`

Specify this to prevent all of the character string following this option from being treated as an option. For example, if you want to specify `-h` as the node name, specify `-- -h`.

***node-name***

Specify the name of the node you want to start.

#### Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| `21` | The specified node does not exist. Specify a node that exists in the cluster, and then try again. |
| `28` | The node status is not `INACTIVE`. Check the node status, stop the node, and then try again. |
| `36` | No service IP address is specified. Specify one or more service IP addresses for the relevant node. |
| `65` | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| `66` | The processing of the failover function has failed. If this message is displayed when performing a manual failover, make sure that the failover-destination node has started. In other cases, check (in all nodes in the cluster) whether a KAQG7*nnnn* message was output to the system messages. If a system message was output, take appropriate action. If you cannot identify the cause, acquire all the Management log files and Cluster log files, and then inform maintenance personnel. |
| `70` | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |

| | |
|---|---|
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | An internal error occurred. Acquire all the Management log files and inform maintenance personnel. |

## Example

### To start the node `nodennc2`:

```
$ sudo enas_ndstart nodennc2
```

## 6.2.25 enas_ndstatus (Display node status)

### Synopsis

```
enas_ndstatus [-c] [--] [node-name]
enas_ndstatus -h
```

### Description

Displays the status of a node.

### Options and arguments

**-c**

Specify this option if you want to display node status information separated with colons (:). When the -c option is specified, any colon (:) contained in the node names is replaced with a number sign (#).

**-h**

Specify this option if you want to view the command syntax.

**--**

Specify this to prevent all of the character string following this option from being treated as an option. For example, if you want to specify -h as the node name, specify -- -h.

***node-name***

To view the status of a particular node in the cluster, specify the node name.

### Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.23 Information displayed when executing the enas_ndstatus command**

| Item | Description |
|---|---|
| --Node Status-- | The node information is displayed.<br>If you do not specify a node name, the command displays the status of the node to which you are logged in and the status of the other node in the cluster, in that order. |
| *NAS-Unit-name*, *NNC-name* | The NAS Unit name and NNC name are displayed in the following format:<br>*NAS-Unit-name*(*NNC-name*) |
| Node name | Name of the node is displayed: |
| Node status | Status of the node is displayed:#1<br>UP<br>The node is running normally. |

| | |
|---|---|
| | INACTIVE<br>The node is stopped.<br>DOWN<br>The node ended abnormally and has shut down.<br>UNKNOWN#2<br>The status cannot be determined. |

#1:

If an error occurs in the NAS Modular system, the status of nodes may not be displayed. In this case, collect error information and contact maintenance personnel.

#2:

If you execute the `enas_ndstatus` command while you are logged in to a stopped node, the other node in the cluster is shown as having `UNKNOWN` status, regardless of its actual status. To check the status of the other node and the resource group, log on to the active node (the other node), and then execute the `enas_clstatus` command.

### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| 21 | The specified node does not exist. Specify a node that exists in the cluster, and then try again. |
| 65 | Another user is exclusively using a resource of the status display processing, or an exclusively used node has stopped. Wait a while, and then retry. If a processing node stops, wait about 15 minutes or boot the stopped node. |
| 66 | The processing of the failover function has failed. If this message is displayed when performing a manual failover, make sure that the failover-destination node has started. In other cases, check (in all nodes in the cluster) whether a KAQG7*nnnn* message was output to the system messages. If a system message was output, take appropriate action. If you cannot identify the cause, acquire all the Management log files and Cluster log files, and then inform maintenance personnel. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | An internal error occurred. Acquire all the Management log files and inform maintenance personnel. |

### Examples

#### To display the statuses of both nodes by specifying the `-c` option:

```
$ sudo enas_ndstatus -c
NNC2:D730100045:nodennc2:UP:NNC0:D730100041:nodennc0:UP
```

**To display the statuses of both nodes without specifying the `-c` option:**

```
$ sudo enas_ndstatus

--Node Status--
NNC2(D730100045)
Node name    : nodennc2
Node status   : UP

NNC0(D730100041)
Node name    : nodennc0
Node status   : UP
```

**To display the status of the node `nodennc2` only by specifying the `-c` option:**

```
$ sudo enas_ndstatus -c nodennc2
NNC2:D730100045:nodennc2:UP
```

**To display the status of the node `nodennc2` only without specifying the `-c` option:**

```
$ sudo enas_ndstatus nodennc2

--Node Status--
NNC2(D730100045)
Node name    : nodennc2
Node status   : UP
```

### 6.2.26 enas_ndstop (Stop a node)

#### Synopsis

```
enas_ndstop [-f] [--] node-name
enas_ndstop -h
```

#### Description

Stops a specified node.

You can execute this command when the status of the node and resource group is as follows:

- The node to be stopped is in `UP` state.
- The status of the resource group on the node to be stopped is `Online/No error`, `Offline/No error`, or `Online Maintenance/No error`.

#### Options and arguments

**`-f`**

Specify this option if you want to forcibly stop the specified node. If an error occurs during node startup or stop operation and prevents processing from continuing, you can forcibly stop the node by executing this command with the `-f` option specified.

**`-h`**

Specify this option if you want to view the command syntax.

**`--`**

Specify this to prevent all of the character string following this option from being treated as an option. For example, if you want to specify `-h` as the node name, specify `-- -h`.

***node-name***

Specify the name of the node you want to stop or forcibly stop.

#### Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| `21` | The specified node does not exist. Specify a node that exists in the cluster, and then try again. |
| `27` | The node status is not `UP`. Check the node status, start the node, and then try again. |
| `65` | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |

| | |
|---|---|
| 66 | The processing of the failover function has failed. If this message is displayed when performing a manual failover, make sure that the failover-destination node has started. In other cases, check (in all nodes in the cluster) whether a KAQG7*nnnn* message was output to the system messages. If a system message was output, take appropriate action. If you cannot identify the cause, acquire all the Management log files and Cluster log files, and then inform maintenance personnel. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | An internal error occurred. Acquire all the Management log files and inform maintenance personnel. |

## Examples

### To stop the node `nodennc2`:

```
$ sudo enas_ndstop nodennc2
```

### 6.2.27 enas_netstat (Displays the network setting information)

#### Synopsis

```
enas_netstat [-r|-g|-i|-s] [-v] [-n] [--numeric-hosts]
  [--numeric-ports] [--numeric-users]
  [--protocol=family[,family...]]
  [-c] [-e [-e]] [-o] [-p] [-l] [-a] [-F] [-C]
```

#### Description

Displays the network information set in the GUI. The displayed information is the same as that displayed by the by the `netstat` command.

By executing this command, you can check whether the network settings are set correctly in the NAS OS.

The displayed information is added to the beginning of the log file. When the log file exceeds 1 MB, information equivalent to the amount by which the maximum size was exceeded is deleted from the end of the log file. You can obtain the log by downloading all the log data from the **List of RAS Information** (Batch-download) window.

If VLAN is used in the NAS Modular system, this command displays the name of the VLAN interface in the following format:

```
physical-interface-name.VLAN-ID
```

For example, if the name of the VLAN physical interface is `gbe1` and the VLAN ID is `10`, `gbe1.0010` appears as a VLAN interface name.

#### Note

- Multiple processes cannot execute the `enas_netstat` command concurrently. If the `enas_netstat` command is executed concurrently by multiple processes, an exclusive control error occurs and `failed to lock` is displayed. If you want to execute the `enas_netstat` command, execute the command after making sure that the process executing the `enas_netstat` command has ended. If no process is executing the `enas_netstat` command but the exclusive control error occurs, execute the `enas_eraselog` command and then execute the `enas_netstat` command.
- Information may not appear immediately due to internal buffering.
- If command processing does not complete within 30 seconds, a timeout occurs and processing is canceled. If a timeout occurs, re-execute the command with the `-n` option specified.

#### Options and arguments

**`-a`**

Specify this option to view all the sockets in use regardless of their connection status.

**-c**

Specify this option to refresh the displayed information at one-second intervals.

**-C**

Specify this option to view routing information in the routing cache.

**-e [-e]**

Specify this option to view detailed information. Specify the option twice to obtain even more detailed information.

**-F**

Specify this option to view routing information in the FIB.

**-g**

Specify this option to view information about IPv4 and IPv6 multicast group membership.

**-i**

Specify this option to view information about all network interfaces.

**-l**

Specify this option to view only the sockets that are waiting for connections.

**-n**

Specify this option to view numerical addresses without resolving host names, port names, or user names.

**--numeric-hosts**

Specify this option to view hosts by IP address, not host name.

**--numeric-ports**

Specify this option to view ports by port number, not port name.

**--numeric-users**

Specify this option to view users by user ID, not user name.

**-o**

Specify this option to view information about the networking timer.

**-p**

Specify this option to view the name and PID of the program that each socket belongs to.

**--protocol=*family*[,*family*...]**

Specify this option to view the connection status of a specified address family. In *family*, specify one of the following keywords: `inet`, `unix`, `ipx`, `ax25`, `netrom`, or `ddp`. `inet` includes the protocol sockets (`raw`, `udp`, and `tcp`).

**-r**

Specify this option to view the routing table.

**-s**

Specify this option to view statistical information for each protocol.

**-v**

Specify this option to view information in detail mode.

### Return values

| | |
|---|---|
| 0 | The command terminated normally. |
| 1 | ▪ The specified option is invalid. Specify the valid option.<br>▪ An internal error occurred. Retry execution. |

### Example

**To display information about all network interfaces:**

```
$ sudo enas_netstat -i
Kernel Interface table
Iface      MTU Met   RX-OK RX-ERR RX-DRP RX-OVR  TX-OK TX-ERR TX-DRP TX-OVR Flg
agr0      1500  02078250496   0   0   01616205327   0   0   0 BMsmRU
agr1      1500  0 1085569   0   0   0  26421   0   0   0 BMOsmRU
mtp1      1500  0  18816   0   0   0  4270   0   0   0 BMRU
mng1      1500  0 344026   0   0   0 197488   0   0   0 BMRU
gbe1      1500  01137649328   0   0   0894093613   0   0   0 BMsRU
gbe2      1500  0 543161   0   0   0  13211   0   0   0 BMOsRU
gbe3      1500  0940601168   0   0   0722111714   0   0   0 BMsRU
gbe4      1500  0 542408   0   0   0  13210   0   0   0 BMsRU
lo     16436  0499247407   0   0   0499247407   0   0   0 LRU
rdn0      1500  02079336065   0   0   01616231748   0   0   0 BMmRU
rdn0.0002  1500  02077674250   0   0   01616178767   0   0   0 BMmRU
rdn0.0002:0 1500  0   - no statistics available -            BMmRU
stnet0    2016  0 404739   0   0   0 421185   0   0   0 ORU
stnet1    2016  0 619195   0   0   0 621104   0   0   0 ORU
```

### 6.2.28 enas_nfs_locks_clear (Delete file lock information for an NFS client host)

#### Synopsis

```
enas_nfs_locks_clear [-F] host-name [host-name...]
```

#### Description

Deletes the file lock information remaining in the NAS OS after an error occurs on the NFS client host or network. Use this command when an NFS client machine, which has the file lock information, terminates abnormally while holding the lock information, and that machine cannot restart for some reason.

> ***Note:***
>
> When a file is locked normally by an NFS client, if the NFS file lock information is deleted on the NAS Modular system, the lock on the file is lost, leaving the file vulnerable to damage.
>
> After deleting the file lock information that has remained on the NAS OS because of a network error occurring while an NFS client host was normally operating, restart the NFS client host before reconnecting the client to the network.

When you execute this command, a message asks whether you are sure you want to delete the file lock information. Type `y` to delete the information, or `n` to cancel.

#### Options and arguments

**`-F`**

Specify this option to forcibly delete the file lock information for the specified NFS client host. No confirmation message appears when you specify this option.

***host-name* [*host-name...*]**

Specify the host names of the NFS client hosts of which to delete the file lock information. Delimit multiple host system names with spaces.

#### Return values

| | |
|---|---|
| 0 | Completed successfully.<br>The command completes successfully even if no file lock information exists on the specified host. |
| 1 | An error occurred during part or all of the processing.<br>A communication timeout may have occurred during conversion of host names to IP addresses. |

### Example

**To delete the file lock information for an NFS client host (host name: `ClientHost`):**

```
$ sudo enas_nfs_locks_clear ClientHost
Do you really want to clear locks held for ClientHost (y/n)?
```

### 6.2.29 enas_nfs_mount_del (Delete mount information for an NFS client host)

#### Synopsis

```
enas_nfs_mount_del [-r] [-c client] directory[ directory...]
```

#### Description

This command deletes mount information for NFS clients from the NAS OS.

If one of the following events occurs or the following operation is performed, use this command on both nodes in a cluster to delete or rename the subdirectory of an NFS-shared directory.

- When an NFS client has mounted a subdirectory of a shared directory, the client machine goes down or is stopped without unmounting the subdirectory
- When an NFS client has mounted a subdirectory of a shared directory, a failover or failback occurs, and then an NFS client unmounts the subdirectory from the node on which the subdirectory was originally mounted

***Note:***

If you delete the mount information for an NFS client whose NFS shares are correctly mounted, the NFS client will no longer be able to access file shares (`ESTALE` error).

When you want to delete not only mount information from the NAS OS, but also mounted directories themselves, delete their subdirectories first. If you delete the directories first, you can no longer delete the subdirectories.

#### Options and arguments

**`-c` *client***

Specify this option to delete mount information for a specific NFS client. If you do not know the value to be specified in this option, execute the `enas_nfs_mount_list` command. You can specify any character string displayed in the `client` column in the execution results of the command.

**`-r`**

Specify this option to delete not only mount information for NFS clients from the NAS OS, but also the specified directories themselves.

***directory*`[` *directory*`...]`**

Specify one or more NFS-mounted subdirectories by using their absolute paths. When you specify multiple subdirectories, use a space to separate each subdirectory.

#### Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ The specified directory cannot be deleted because it is a NFS shared directory.<br>▪ The specified directory cannot be deleted because it is being used by a client host |

| | |
|---|---|
| | ▪ There is no mount information for the specified directory. Check the mount information by using the `enas_nfs_mount_list` command. Specify the correct directory name, and then retry the operation.<br>▪ An attempt to create a child process by the command has failed. Acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ An attempt to delete the specified directory has failed. Check whether the specified directory is in a read-only file system, or whether there is a file or a directory under the specified directory. Check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel. |
| 2 | ▪ The file is locked by another process. Wait a while, and then try again. If the error occurs again, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ There might be a problem in the NAS OS LU. Check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel. |
| 3 | ▪ The user must have administrator permissions to execute this command. Use the `sudo` command, and then try the operation again.<br>▪ The command syntax will be displayed. Make sure the command syntax is correct, and then try again. |

## Example

### To delete the mount information on the `/mnt/FS_1/share01` directory for the NFS client host (host name: `ClientHost`):

```
$ sudo enas_nfs_mount_del -c ClientHost /mnt/FS_1/share01
```

### 6.2.30 enas_nfs_mount_list (List mount information for an NFS client host)

#### Synopsis

```
enas_nfs_mount_list [-c client] [directory[ directory...]]
```

#### Description

This command displays information about directories mounted on an NFS client or NFS clients. If you omit all arguments and options, the command displays information about all directories that NFS clients have mounted on the node you log in to.

#### Options and arguments

**`-c` *client***

Specify the IP address or host name of the NFS client for which you want to display mount information.

***directory*`[` *directory*`...]`**

Specify the absolute paths of the directories that have been mounted on NFS clients and for which you want to display mount information. When you specify multiple paths, use a space to separate each path.

#### Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.24 Information displayed when executing the enas_nfs_mount_list command**

| Item | Description |
|---|---|
| client | Information about the NFS clients on which the directories have been mounted is displayed. |
| directory | The absolute paths of directories mounted on NFS clients are displayed. |

#### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 3 | The command syntax will be displayed. Make sure the command syntax is correct, and then try again. |

#### Example

**To display the mount information for the NFS client host (host name: `ClientHost`):**

```
$ sudo enas_nfs_mount_list -c ClientHost
client:         directory:
ClientHost       /mnt/filesystem01/nfs01
ClientHost       /mnt/filesystem01/nfs02
```

### 6.2.31 enas_nfs_opt_list (List the NFS environment settings of the NAS OS)

#### Synopsis

```
enas_nfs_opt_list
```

#### Description

This command displays the information about the NFS environment set for the NAS OS.

#### Options and arguments

There are no arguments or options.

#### Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.25 Information displayed when executing the enas_nfs_opt_list command**

| Item | Description |
|---|---|
| nfsd_hierarchical_export | Displays whether an NFS share can be created in the higher-level and lower-level directories of a directory in which an NFS share has already been created.<br>0<br>Creation of another NFS share is not allowed.<br>1<br>Creation of another NFS share is allowed. |

#### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | The command terminated abnormally due to an error. |
| 2 | The command failed to write to the /etc/sysctl.conf file. Wait a while, and then re-execute the command. |
| 3 | The command syntax will be displayed. Make sure the command syntax is correct, and then try again. |

#### Example

**To display the information about the NFS environment set in the NAS OS:**

```
$ sudo enas_nfs_opt_list
nfsd_hierarchical_export = 0
```

### 6.2.32 enas_nfs_opt_set (Set an NFS environment for the NAS OS)

#### Synopsis

```
enas_nfs_opt_set nfsd_hierarchical_export={0|1}
```

#### Description

This command sets an NFS environment for the NAS OS.

#### Options and arguments

**nfsd_hierarchical_export={0|1}**

This option lets you specify whether to allow creation of an NFS share in the higher-level and lower-level directories of a directory in which an NFS share has already been created.

0

Does not allow creation of another NFS share.

1

Allows creation of another NFS share.

#### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | The command terminated abnormally due to an error. |
| 2 | The command failed to write to the /etc/sysctl.conf file. Wait a while, and then re-execute command. |
| 3 | The command syntax will be displayed. Make sure the command syntax is correct, and then try again. |

#### Example

**To disallow creation of an NFS share in the higher-level and lower-level directories of a directory in which an NFS share has already been created:**

```
$ sudo enas_nfs_opt_set nfsd_hierarchical_export=0
```

### 6.2.33 enas_nfscreate (Create an NFS share)

#### Synopsis

```
enas_nfscreate -d shared-directory -H host[,host...]
  [-p {ro|rw_sync|rw_sync_opt}] [-a {everyone|root_only|none}]
  [-u UID] [-g GID] [-t {perform|do_not_perform}]
  [-s {perform|do_not_perform}] [-l {perform|do_not_perform}]
enas_nfscreate -h
```

#### Description

Creates an NFS share using the specified attributes.

To make a directory public with different attributes on multiple hosts, execute this command on each target host. However, for attributes set in the following options, the attribute you specify the last time you execute this command will apply to all NFS shares in that directory.

- `-u` option
- `-g` option
- `-t` option
- `-s` option
- `-l` option

#### Options and arguments

**`-a {everyone|root_only|none}`**

Specify whether to map the user as an anonymous user when an NFS client accesses the NAS Modular system. If you omit this option, `root_only` applies.

`everyone`

Specify this when you map all users as anonymous users.

`root_only`

Specify this when you map only the root user as an anonymous user.

`none`

Specify this when you do not want to map users as anonymous users.

**`-d` *shared-directory***

Specify 6 to 63 characters for the absolute path of the directory in which you want to create an NFS share. When the automatic creation schedule (automatic creation of shares) of NAS Sync Image is used, the absolute path can be a maximum of 48 characters.

**-g** ***GID***

Specify the group ID to be used in an anonymous user access. Specify a value within the range from 0 to 65,535. If you omit this option, it defaults to 65534.

**-h**

Specify this option if you want to view the command syntax.

**-H** ***host*[,*host*...]**

Specify the NFS share public destination. Specify a string of or no more than 255 characters. You can specify multiple destinations, although you cannot specify the same host multiple times. When you specify multiple public destinations, separate the destinations with commas (,). In addition to the host name and IP address, you can specify the destinations in the following formats.

Netgroup

Specify an NIS netgroup.

IP network

Specify the IP address and netmask. Specify the netmask as decimal values for each 8-bit octet separated by periods (.), or specify the bit count.

Wildcard

When you specify all hosts, you can use an asterisk (*) as the wildcard.

If some or all of the NFS client machines have multiple network interfaces that are used to communicate with the NAS Modular system, specify all the host names corresponding to all the IP addresses (for those interfaces) for the NFS clients. If you specify a wildcard (*), IP networks, or netgroups, NFS clients might not be able to access the NFS share.

The total of the input sizes of host names or network names (input length + 4 bytes) must be less than 1,005 bytes. When the specified IP addresses can be resolved by using methods such as the `hosts` file or DNS, the total of sizes calculated based on host names corresponding to the IP address portion (host name length + 4 bytes) must also be less than 1,005 bytes. If an NFS share has already been created for the shared directory specified in the `-d` option, the hosts on which that NFS share is made public must also be included in the calculation.

To check the sizes (host name length + 4 bytes) of the host names or network names on which the existing NFS share was made public, execute the `enas_nfslist` command. Specify the `-d` option when executing the `enas_nfslist` command. Calculate the total size, adding 4 bytes to each of the lengths output in `Public destination host/network`.

**-l {perform|do_not_perform}**

Specify whether to check permissions for a lock request. If you omit this option, it defaults to `do_not_perform`.

If you use a machine that does not send authentication information for a lock request (the machine OS is HP-UX or a machine on which the `rpcinfo -p` command displays `100020` in `program)` or that sends authentication information of a user other than the user who requests a lock (the machine OS is AIX), as an NFS client, specify `do_not_perform`. If you specify `perform`, the lock might not be obtained (an ENOLCK error might occur) unless anonymous users of the NAS Modular system have read permission (r) for all directories from the parent directory of the file to be locked to the NFS mounted directory.

`perform`

Specify this if you want to check permissions (authorize) of each lock request. If anonymous mapping is not set for the user, permissions for the user who locked the files are checked. If anonymous mapping is set for the user, permissions for the anonymous user in the NAS Modular system are checked. The owner of the locked files can lock them without permissions. Also, if the user has read permissions, they can write lock the files.

`do_not_perform`

Specify this if you do not want to check permissions (authorize) of each lock request. Permissions for an anonymous user in the NAS Modular system are checked.

**`-p {ro|rw_sync|rw_sync_opt}`**

Specify access permissions for the NFS share. If you omit this option, it defaults to `rw_sync`.

When you permit writing, specify whether to optimize synchronous writing as well. Optimization of synchronous writing is a function that slightly delays a disk update by a write request, when the write request has been received from an NFS client while another relevant write request is being performed (or is about to be performed). Optimization can improve performance because the disk is updated by multiple write requests in one operation. If the NFS server receives multiple data write requests that are relatively unrelated, optimizing synchronous writing may actually lower performance. In this situation, specify synchronous writing without optimization (`rw_sync`).

`ro`

Specify this to permit the NFS share to be read-only.

`rw_sync`

Specify this to permit read and write operations on the NFS share, and to set synchronous writing without optimization.

`rw_sync_opt`

Specify this to permit read and write operations on the NFS share, and to set synchronous writing with optimization.

**`-s {perform|do_not_perform}`**

Specify whether to check that not only do the file and directory to be accessed have access permission (x permission), but also, all directories (subtrees) from the shared directory to the directory in which the file and directories to be accessed exist have execute permission (x permission). If you omit this option, it defaults to perform.

If you use a machine that does not send authentication information for a lock request (the machine OS is HP-UX or a machine on which the rpcinfo -p command displays 100020 in program) or that sends authentication information of a user other than the user who requests a lock (the machine OS is AIX), as an NFS client, specify do_not_perform. If you specify perform, the lock might not be obtained (an ENOLCK error might occur) unless anonymous users of the NAS Modular system have execute permission (x) for all directories from the parent directory of the file to be locked to the NFS mounted directory.

perform

Specify this if you want to perform a subtree check.

do_not_perform

Specify this if you do not want to perform a subtree check.

**-t {perform|do_not_perform}**

Specify whether to accept only the requests from an Internet port lower than 1,024. To make the file system open to machines that use an Internet port assigned 1,024 or a higher port number, specify do_no_perform. If you omit this option, it defaults to do_not_perform.

perform

Specify this if you want to limit sending ports.

do_not_perform

Specify this if you do not want to limit sending ports.

In AIX, an Internet port whose port number is 1,024 or higher is used by default. If you use AIX for the NFS client host and choose to use the default Internet port setting, specify do_no_perform. In HP-UX, an Internet port whose port number is 1,024 or higher is used for file locking. If you use HP-UX for the NFS client host, specify do_no_perform.

**-u *UID***

Specify the user ID to be used in an anonymous user access. Specify a value within the range from 0 to 65,535. If you omit this option, it defaults to 65534.

## Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| 10 | ▪ A name already registered in the system was specified for the argument of an option. Check |

| | |
|---|---|
| | the name and retry.<br>▪ The specified directory does not exist. Specify an already created directory.<br>▪ The specified shared directory is already used by another CIFS/NFS file share. Specify a directory not already made public by another file share, and then retry the operation.<br>▪ The specified network address of the client to be made public was not found. Specify an existing host or network.<br>▪ A value exceeding the maximum size that can be specified for a public destination host/network was specified. Enter a suitable value.<br>▪ An operation failed because the file system corresponding to the specified shared directory does not exist. In the **List of File Systems** check the file system name, and then specify the correct file system name.<br>▪ This operation cannot be performed because the capacity of the differential-data storage device is insufficient. Resolve the problem by using a NAS Sync Image operation.<br>▪ The number of created NFS file shares has reached the upper limit. Delete any unnecessary NFS file shares, and then create a new NFS file share. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | ▪ An attempt to acquire information about file shares has failed. A conflict with another system administrator's operation or an internal error may have occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel.<br>▪ The NFS file share creation failed. An error exists in the entered data or an unexpected error occurred during creation of an NFS share. Revise the entered values. Acquire all the Management log files if this error occurs again, and inform maintenance personnel. |
| 70 | ▪ An operation cannot be performed because the file system corresponding to the specified directory is defined by the other node in the cluster. Specify a file share corresponding to a file system created on the operating node.<br>▪ The file system specified for the shared directory is not mounted. The resource group is in the OFFLINE state, or the resource group may be undergoing failover. If the resource group is in the OFFLINE state or the resource group is undergoing failover, remove the problem and then retry. If the file system is not mounted, mount the file system, and then retry.<br>▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 98 | Some other error occurred. |
| 99 | ▪ An internal error occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel.<br>▪ The processing of the failover function has failed. Acquire all the Management log files, and Cluster log files, and contact maintenance personnel.<br>▪ An attempt to acquire resource group information failed. Acquire all the Management log files, and Cluster log files, and contact maintenance personnel.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and contact maintenance personnel.<br>▪ A file sharing operation failed because the file system corresponding to the specified directory is blocked. Acquire all the Management log files, and Cluster log files, and contact maintenance personnel.<br>▪ The specified operation failed. The file system or device file may be blocked. In the **List of File Systems**, check the state of the file system. If the file system has an error status, inform maintenance personnel. If the file system does not have an error status, acquire all the Management log files and inform maintenance personnel. |

## Examples

### To create an NFS share according to the following conditions:

- The shared directory is `/mnt/FS1/dir_case1`.
- Specify the public destination hosts to `host1`, `host2`, `host3`, and `host4`.

```
$ sudo enas_nfscreate -d /mnt/FS1/dir_case1 -H
host1,host2,host3,host4
```

### To create an NFS share according to the following conditions:

- The shared directory is `/mnt/FS1/dir_case1`.
- Specify the public destination hosts to all hosts.

```
$ sudo enas_nfscreate -d /mnt/FS1/dir_case1 -H "*"
```

### 6.2.34 enas_nfsdelete (Delete NFS shares)

#### Synopsis

```
enas_nfsdelete -d shared-directory {-a|-H host[,host...]}
enas_nfsdelete -h
```

#### Description

Deletes an NFS share.

#### Options and arguments

**-a**

Specify this option to delete all NFS shares in the shared directory specified in the `-d` option.

**-d *shared-directory***

Specify the absolute path for the directory from which NFS shares are to be deleted. Specify a path that does not include a symbolic link.

**-h**

Specify this option if you want to view the command syntax.

**-H *host*[,*host*...]**

Specify the public destination hosts from which the NFS shares are to be deleted. When you specify multiple public destinations, separate the destinations with commas (,).

#### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| 10 | ▪ A name not registered in the system was specified for the argument of an option. Retry specifying a parameter name registered in the system.<br>▪ The specified file share does not exist. Display the **List of File Shares** again and specify a name of file share that exists in the list. Acquire all the Management log files if the error occurs again, and inform maintenance personnel.<br>▪ The specified network address of the client to be made public was not found. Specify an existing host or network. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | ▪ An attempt to acquire information about file shares has failed. A conflict with another system administrator's operation or an internal error may have occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel. |

| | |
|---|---|
| | ▪ The NFS file share deletion failed. A conflict with another system administrator's operation or an internal error may have occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel. |
| 70 | ▪ An operation cannot be performed because the file system corresponding to the specified directory is defined by the other node in the cluster. Specify a file share corresponding to a file system created on the operating node.<br>▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first.<br>▪ The specified file share does not exist on the operating node. The file share was created on the other node, the resource group is in the OFFLINE state, or the resource group is undergoing failover. Make sure that the following items corresponding to the specified file share are correct: the file system name, and the resource group state. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 98 | Some other error occurred. |
| 99 | ▪ An internal error occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel.<br>▪ The processing of the failover function has failed. Acquire all the Management log files, and Cluster log files, and contact maintenance personnel.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and inform maintenance personnel. |

## Example

### To delete all NFS shares in the directory `/mnt/FS1/dir_case1`:

```
$ sudo enas_nfsdelete -d /mnt/FS1/dir_case1 -a
```

### 6.2.35 enas_nfsedit (Edit NFS share information)

#### Synopsis

```
enas_nfsedit -d shared-directory -H host[,host...]
  [-p {ro|rw_sync|rw_sync_opt}] [-a {everyone|root_only|none}]
  [-u UID] [-g GID] [-t {perform|do_not_perform}]
  [-s {perform|do_not_perform}] [-l {perform|do_not_perform}]
enas_nfsedit -h
```

#### Description

Edits NFS share information according to the specified attributes.

When you edit the attributes set in the following options, the attribute you specify the last time you execute this command will apply to all NFS shares in that directory.

- `-u` option
- `-g` option
- `-t` option
- `-s` option
- `-l` option

#### Options and arguments

**`-a {everyone|root_only|none}`**

Specify whether to map the user as an anonymous user when an NFS client accesses the NAS Modular system. If you omit this option, the current setting information applies.

`everyone`

Specify this when you map all users as anonymous users.

`root_only`

Specify this when you map only the root user as an anonymous user.

`none`

Specify this when you do not want to map users as anonymous users.

**`-d`** ***shared-directory***

Specify the absolute path for the directory of the NFS share whose attributes are to be changed.

**`-g`** ***GID***

Specify the group ID to be used in an anonymous user access. Specify a value within the range from 0 to 65,535. If you omit this option, the current setting information applies.

**-h**

Specify this option if you want to view the command syntax.

**-H *host*[,*host*...]**

Specify the public destination hosts set for the target NFS share. When you specify multiple public destinations, separate the destinations with commas (,).

**-l {perform|do_not_perform}**

Specify whether to check permissions for a lock request. If you omit this option, the current setting information applies.

If you use a machine that does not send authentication information for a lock request (the machine OS is HP-UX or a machine on which the `rpcinfo -p` command displays `100020` in `program)` or that sends authentication information of a user other than the user who requests a lock (the machine OS is AIX), as an NFS client, specify `do_not_perform`. If you specify `perform`, the lock might not be obtained (an ENOLCK error might occur) unless anonymous users of the NAS Modular system have read permission (r) for all directories from the parent directory of the file to be locked to the NFS mounted directory.

`perform`

Specify this if you want to check permissions (authorize) of each lock request. If anonymous mapping is not set for the user, permissions for the user who locked the files are checked. If anonymous mapping is set for the user, permissions for the anonymous user in the NAS Modular system are checked. The owner of the locked files can lock them without permissions. Also, if the user has read permissions, they can write lock the files.

`do_not_perform`

Specify this if you do not want to check permissions (authorize) of each lock request. Permissions for an anonymous user in the NAS Modular system are checked.

**-p {ro|rw_sync|rw_sync_opt}**

Set access permissions for the NFS share. If you omit this option, the current setting information applies.

When you permit writing, specify whether to optimize synchronous writing as well. Optimization of synchronous writing is a function that slightly delays a disk update by a write request, when the write request has been received from an NFS client while another relevant write request is currently being performed (or is about to be performed). Optimization can improve performance because the disk is updated by multiple write requests in one operation. If the NFS server receives multiple data write requests that are relatively unrelated, optimizing synchronous writing may actually lower performance. In this situation, specify synchronous writing without optimization (`rw_sync`).

`ro`

Specify this to permit the NFS share to be read-only.

rw_sync

Specify this to permit read and write operations on the NFS share, and to set synchronous writing without optimization.

rw_sync_opt

Specify this to permit read and write operations on the NFS share, and to set synchronous writing with optimization.

**-s {perform|do_not_perform}**

Specify whether to check that not only do the file and directory to be accessed have access permission (x permission), but also, all directories (subtrees) from the shared directory to the directory in which the file and directories to be accessed exist have execute permission (x permission). If you omit this option, the current setting information applies.

If you use a machine that does not send authentication information for a lock request (the machine OS is HP-UX or a machine on which the rpcinfo -p command displays 100020 in program) or that sends authentication information of a user other than the user who requests a lock (the machine OS is AIX), as an NFS client, specify do_not_perform. If you specify perform, the lock might not be obtained (an ENOLCK error might occur) unless anonymous users of the NAS Modular system have execute permission (x) for all directories from the parent directory of the file to be locked to the NFS mounted directory.

perform

Specify this if you want to perform a subtree check.

do_not_perform

Specify this if you do not want to perform a subtree check.

**-t {perform|do_not_perform}**

Specify whether to accept only the requests from an Internet port lower than 1,024. To make the file system open to machines that use an Internet port assigned 1,024 or a higher port number, specify do_not_perform. If you omit this option, the current setting information applies.

perform

Specify this if you want to limit sending ports.

do_not_perform

Specify this if you do not want to limit sending ports.

In AIX, an Internet port whose port number is 1,024 or higher is used by default. If you use AIX for the NFS client host and choose to use the default Internet port setting, specify do_no_perform. In HP-UX, an Internet port whose port number is 1,024 or higher is used for file locking. If you use HP-UX for the NFS client host, specify do_no_perform.

`-u` ***UID***

Specify the user ID to be used in an anonymous user access. Specify a value within the range from 0 to 65,535. If you omit this option, the current setting information applies.

## Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| 10 | ▪ A name not registered in the system was specified for the argument of an option. Retry specifying a parameter name registered in the system.<br>▪ The specified file share does not exist. Display the **List of File Shares** again and specify a name of file share that exists in the list. Acquire all the Management log files if the error occurs again, and inform maintenance personnel.<br>▪ The specified network address of the client to be made public was not found. Specify an existing host or network.<br>▪ A value exceeding the maximum size that can be specified for a public destination host/network was specified. Enter a suitable value.<br>▪ A relative path or symbolic link is contained in the value specified for the shared directory. Specify an absolute pathname. Moreover, for a shared directory, specify a path that does not include a symbolic link.<br>▪ This operation cannot be performed because the capacity of the differential-data storage device is insufficient. Resolve the problem by using a NAS Sync Image operation. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | ▪ An attempt to acquire information about file shares has failed. A conflict with another system administrator's operation or an internal error may have occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel.<br>▪ The NFS file share editing failed. An error exists in the entered data or an unexpected error occurred while an NFS share was being edited. Revise the entered values. Acquire all the Management log files if this error occurs again, and inform maintenance personnel. |
| 70 | ▪ An operation cannot be performed because the file system corresponding to the specified directory is defined by the other node in the cluster. Specify a file share corresponding to a file system created on the operating node.<br>▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first.<br>▪ The specified file share does not exist on the operating node. The file share was created on the other node, the resource group is in the OFFLINE state, or the resource group is undergoing failover. Make sure that the following items corresponding to the specified file share are correct: the file system name, and the resource group state. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 98 | Some other error occurred. |
| 99 | ▪ An internal error occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel.<br>▪ The processing of the failover function has failed. Acquire all the Management log files, and Cluster log files, and contact maintenance personnel. |

| | |
|---|---|
| | ▪ An attempt to acquire resource group information failed. Acquire all the Management log files, and Cluster log files, and contact maintenance personnel.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and inform maintenance personnel.<br>▪ The specified operation failed. The file system or device file may be blocked. In the **List of File Systems**, check the state of the file system. If the file system has an error status, inform maintenance personnel. If the file system does not have an error status, acquire all the Management log files and inform maintenance personnel. |

## Example

### To change information about the NFS shares in the directory `mnt/FS1/dir_case1` according to the following conditions:

- An NFS share with write permissions set has been created and made public on `host01`.
- Change the settings to be read-only.

```
$ sudo enas_nfsedit -d /mnt/FS1/dir_case1 -H host01 -p ro
```

### 6.2.36 enas_nfslist (List NFS share information)

#### Synopsis

```
enas_nfslist [-d shared-directory] [-c]
enas_nfslist -h
```

#### Description

Lists information about the NFS shares on the node to which you are logged in. Information is listed for each NFS share in ascending order of the shared directory paths. When multiple NFS shares have been created in one directory, the information appears in ascending order of the public destination hosts.

#### Options and arguments

**-c**

Specify this if you want to display NFS share information separated with colons (:).

**-d *shared-directory***

Specify the absolute path for the target directory to view the settings for a specific NFS share. If you omit this option, the command displays information about all NFS shares on the local node.

**-h**

Specify this option if you want to view the command syntax.

#### Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.26 Information displayed when executing the enas_nfslist command**

| Item | Description |
|---|---|
| Shared directory | Displays the absolute path for the directory of the created NFS shares. |
| Public destination host/network | Displays the name of a host or network accessing the NFS share. |
| Permission mode / Synchronous writing | Displays information about the access permission for the NFS share and the synchronous write mode.<br>ro<br>The NFS share is read-only.<br>rw_sync<br>Read and write operations are permitted on the NFS share, and synchronous writing without optimization is set.<br>rw_sync_opt<br>Read and write operations are permitted on the NFS share, and synchronous writing with optimization is set. |

| | |
|---|---|
| Anonymous mapping | Displays users who are mapped as anonymous users.<br>everyone<br>All users are mapped as anonymous users.<br>root_only<br>Only the root user is mapped as an anonymous user.<br>none<br>Users are not mapped as anonymous users. |
| Anonymous UID | Displays the user ID to be used when accessing the NFS share as an anonymous user. When no ID is set, -- is displayed. |
| Anonymous GID | Displays the group ID to be used when accessing the NFS share as an anonymous user. When no ID is set, -- is displayed. |
| Transmission port restriction | Displays whether to accept only the requests from an Internet port lower than 1,024.<br>perform<br>Transmission ports are restricted.<br>do_not_perform<br>No restriction on transmission ports. |
| Subtree check | Displays whether to check that not only the file and directory to be accessed have access permission (x permission), but also, all directories (subtrees) from the shared directory to the directory in which the file and directories to be accessed exist have execute permission (x permission).<br>perform<br>A subtree check is performed.<br>do_not_perform<br>A subtree check is not performed. |
| Access check with lock request | Displays whether to perform an authorization check (permission check) of a lock request when one is received.<br>perform<br>Authorization is performed.<br>do_not_perform<br>Authorization is not performed. |

## Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | An attempt to acquire information about file shares has failed. A conflict with another system administrator's operation or an internal error may have occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |

| | |
|---|---|
| | ▪ The specified file share does not exist on the operating node. The file share was created on the other node, the resource group is in the OFFLINE state, or the resource group is undergoing failover. Make sure that the following items corresponding to the specified file share are correct: the file system name, and the resource group state. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 98 | Some other error occurred. |
| 99 | ▪ An internal error occurred. Retry execution. Acquire all the Management log files if this error occurs again, and inform maintenance personnel.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and contact maintenance personnel. |

## Examples

### To view information about NFS shares in the directory `/mnt/FS1/SUBDIR1` by specifying the `-c` option:

```
$ sudo enas_nfslist -d /mnt/FS1/SUBDIR1 -c
/mnt/FS1/SUBDIR1:*:rw_sync:root_only:--:--
:do_not_perform:perform:do_not_perform
```

### To view information about NFS shares in the directory `/mnt/FS1/SUBDIR1` without specifying the `-c` option:

```
$ sudo enas_nfslist -d /mnt/FS1/SUBDIR1
List of File Shares:
The number of NFS share(1)
  Shared directory             : /mnt/FS1/SUBDIR1
    Public destination host/network    : *
    Permission mode / Synchronous writing : rw_sync
    Anonymous mapping           : root_only
    Anonymous UID              : --
    Anonymous GID              : --
    Transmission port restriction     : do_not_perform
    Subtree check              : perform
    Access check with lock request    : do_not_perform
```

### 6.2.37 enas_ping (Display the connection to a specified host)

#### Synopsis

```
enas_ping [-c count] [-p pattern] [-s packetsize] host
```

#### Description

Displays the connection status of the specified host. The displayed information is the same as that displayed by the `ping` command.

The displayed information is added to the beginning of the log file. When the log file exceeds 1 MB, information equivalent to the amount by which the maximum size was exceeded is deleted from the end of the log file. The packet dump file is also output as a log file at the same time. You can obtain the log by downloading all the log data from the **List of RAS Information** (Batch-download) window.

#### Note

- Multiple processes cannot execute the `enas_ping` command concurrently. If the `enas_ping` command is executed concurrently by multiple processes, an exclusive control error occurs and `failed to lock` is displayed. If you want to execute the `enas_ping` command, execute the command after making sure that the process executing the `enas_ping` command has ended. If an exclusive control error occurs while no other processes are executing the `enas_ping` command, execute the `enas_eraselog` command, and then execute the `enas_ping` command again.
- Information may not appear immediately due to internal buffering.

#### Options and arguments

**`-c`** ***count***

Specify the number of packets to be sent. The maximum number of send packets is 10. If you omit this option, this option is set to 10.

**`-p`** ***pattern***

Specify a pattern for filling the ping packet to be sent. You can specify a maximum of 16 bytes. You can use this option for diagnosing data-dependent network problems. For example, if you specify `-p ff`, the packet will be filled entirely with 1s.

**`-s`** ***packetsize***

Specify the byte size of the data to be sent. When you omit this option, the default is 56.

***host***

Specify the target host name or IP address.

### Return values

| | |
|---|---|
| 0 | The command terminated normally. |
| 1 | ▪ There are 11 or more packets specified for the `-c` option. Set a value of 10 or less, and then re-execute.<br>▪ The specified option is invalid. Specify a valid option.<br>▪ An internal error occurred. Retry execution. |

### Example

**To check the connection to the host `raid01`:**

```
$ sudo enas_ping raid01
PING raid01 (10.208.151.100): 56 data bytes
64 bytes from 10.208.151.100: icmp_seq=0 ttl=255 time=1.4 ms
64 bytes from 10.208.151.100: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from 10.208.151.100: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=4 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=5 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=6 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=7 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=8 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=9 ttl=255 time=0.3 ms

--- raid01 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.3/1.4 ms
```

### 6.2.38 enas_netstat (Check the Network Settings)

- **Synopsis**

  enas_netstat [-r|-g|-i|-s] [-v] [-n] [--numeric-hosts]
  [--numeric-ports] [--numeric-users] [--protocol=*family* [,*family*...]]
  [-c] [-e [-e]] [-o] [-p] [-l] [-a] [-F] [-C]

- **Description**

  Checks that the network settings performed by the GUI have been applied correctly. The displayed contents are the same as when the Linux® netstat command is used. The contents are accumulated in the log file. The output information is added to the beginning of the log file. If a file size exceeds 1 MB, then an amount of information, equal to the amount of information by which the maximum was exceeded, is deleted from the end of the log file.

  A log file can be downloaded and obtained. All log data can be downloaded and obtained from the **List of RAS Information** (Batch-download) window. For details on downloading all log data, see section 4.13.10.

  If VLAN is used in the NAS Modular system, the name of the VLAN interface displayed by executing the enas_netstat command is as follows:

  *physical-interface-name.VLAN-ID*

  For example, if the name of the VLAN physical interface is gbe1 and the VLAN ID is 10, gbe1.0010 appears as a VLAN interface name.

***Notes:***

- Multiple processes cannot use the enas_netstat command concurrently. If the enas_netstat command is used concurrently by multiple processes, an exclusive control error occurs and failed to lock is displayed. If you want to use the enas_netstat command, use the command after making sure that the process executing the enas_netstat command has ended. If no process is executing the enas_netstat command but the exclusive control error occurs, use the enas_eraselog command and then use the enas_netstat command.
- There are cases in which the standard output is buffered and command output might not appear immediately.
- If the command does not finish within 30 seconds, the command finishes 30 seconds after it was used.

- **Arguments and Options**

**Table 6.27 enas_netstat Arguments and Options**

| Item | Use |
|---|---|
| `-r` | Displays the path table for the kernel. |
| `-g` | Displays information about the IPv4 and IPv6 multicast group membership. |
| `-i` | Displays the status table for all network interfaces. |
| `-s` | Displays a list of statistics for each protocol. |
| `-v` | Use this command in a detailed-display mode. |
| `-n` | Displays the numerical address without resolving host names, port names, and user names.<br>--numeric-hosts<br>Displays the host address numerically, with resolving port names and user names.<br>--numeric-ports<br>Displays the port number numerically, with resolving of host names and user names.<br>--numeric-users<br>Displays the user ID numerically, with resolving of host names and port names.<br>--protocol=family [,family...]<br>Displays the connection status of an address family. Specify the address family keyword in family. You can specify inet, unix, ipx, ax25, netrom, and ddp as keywords. inet includes the protocol sockets (raw, udp, and tcp). |
| `-c` | Displays the specified information per second. |
| `-e [-e]` | Displays the detailed information. If this option is specified twice, the most detailed information possible is displayed. |
| `-o` | Displays information about the networking timer. |
| `-p` | Displays the PID and name of the program to which each socket belongs. |
| `-l` | Displays only the sockets that are waiting for connections. |
| `-a` | Displays the sockets that are waiting for connections as well as the sockets that are not waiting for connections. |
| `-F` | Displays path information from FIB. |
| `-C` | Displays path information from the path cache. |

- **Return Values**

  If the return value is 0, the processing finishes normally. Otherwise, it finishes abnormally. For details on the return value and error message, see the Linux® documentation.

- **Example**

  Following illustrates the display of the status table of all network interfaces:

```
$ sudo enas_netstat -i
Kernel Interface table
Iface     MTU Met  RX-OK RX-ERR RX-DRP RX-OVR  TX-OK TX-ERR TX-DRP TX-OVR
Flg
agr0     1500  02078250496   0   0   01616205327   0   0   0 BMsmRU
agr1     1500  0 1085569   0   0   0  26421   0   0   0 BMOsmRU
mtp1     1500  0  18816   0   0   0  4270   0   0   0 BMRU
mng1     1500  0 344026   0   0   0 197488   0   0   0 BMRU
gbe1     1500  01137649328   0   0   0894093613   0   0   0 BMsRU
gbe2     1500  0 543161   0   0   0  13211   0   0   0 BMOsRU
gbe3     1500  0940601168   0   0   0722111714   0   0   0 BMsRU
gbe4     1500  0 542408   0   0   0  13210   0   0   0 BMsRU
lo      16436  0499247407   0   0   0499247407   0   0   0 LRU
rdn0     1500  02079336065   0   0   01616231748   0   0   0 BMmRU
rdn0.0002  1500  02077674250   0   0   01616178767   0   0   0 BMmRU
rdn0.0002:0 1500  0   - no statistics available -            BMmRU
stnet0    2016  0 404739   0   0   0 421185   0   0   0 ORU
stnet1    2016  0 619195   0   0   0 621104   0   0   0 ORU
```

### 6.2.39 enas_nfscreate (Create an NFS Share)

- **Synopsis**

  enas_nfscreate -h|-d *shared-directory* -H *host*[,*host*...]
  [-p {ro|rw_sync|rw_sync_opt}] [-a {everyone|root_only|none }]
  [-u *UID*] [-g *GID*] [-t {perform|do_not_perform}]
  [-s {perform|do_not_perform}] [-l {perform|do_not_perform}]

- **Description**

  Creates an NFS share using the specified attributes. You can specify multiple public destinations at once in a command execution. You can also use the command once for each public destination. However, if you use the `enas_nfscreate` command multiple times on the same shared directory, the values specified in the following options are overwritten by the values specified in the last `enas_nfscreate` command execution.

  When an automatic creation schedule is set up in NAS Sync Image for a file system for which an NFS share was created, if a file share is automatically created for a differential-data snapshot, that NFS share is created based on the NFS share information created by this command:

  `-u` option

  `-g` option

  `-t` option

  `-s` option

  `-l` option

- **Arguments and Options**

**Table 6.28 enas_nfscreate Arguments and Options**

| Item | Use |
|---|---|
| `-h` | Specify this option if you want to view the command syntax. |
| `-d` *shared-directory* | Specify the directory to be made public as an NFS share in the `/mnt/`*file-system-name* or `/mnt/`*file-system-name*`/`*subdirectory* format. The directory to be specified must already exist. Specify the shared directory so that it is unique within the cluster. Be sure to specify an absolute pathname.<br>Specify a string from 6 to 63 characters. When the automatic creation schedule (automatic creations of shares) of NAS Sync Image is used, the NFS shared directory can be a maximum of 48 characters.<br>When specifying a subdirectory under a file system:<br>`/mnt/`*file-system-name*`/`*subdirectory*<br>When specifying the whole of each file system:<br>`/mnt/`*file-system-name* |

| Item | Use |
|---|---|
| `-H host[,host...]` | Specify the NFS share public destination. Specify a string of or less no more than 255 characters. You can specify multiple destinations, although you cannot specify the same host multiple times. When you specify multiple public destinations, separate the destinations with commas (`,`). In addition to the host name and IP address, you can specify the destinations in the following formats.<br>▪ Netgroup<br>Specify an NIS netgroup.<br>▪ IP network<br>When you make the NFS share public to all hosts in a subnetwork, specify the IP address and netmask in the *address/netmask* format. You can either specify *netmask* as a decimal value separated with periods (`.`) or as a consecutive mask length.<br>▪ Wildcard<br>When you specify all hosts, you can use an asterisk (`*`) as the wildcard.<br>The total of the input sizes of host names or network names (input length + 4 bytes) must be less than 1,005 bytes. When the specified IP addresses can be resolved by using methods such as the `hosts` file or DNS, the total of sizes calculated based on host names corresponding to the IP address portion (host name length + 4 bytes) must also be less than 1,005 bytes.<br>If an NFS share has already been created for the shared directory specified in the `-d` option, the public destinations that have already been registered must also be included in the calculation.<br>You can check the sizes of the public destination host names or network names that have already been registered (host name length + 4 bytes) using the `enas_nfslist` command. Use the `enas_nfslist` command specifying the `-d` option and calculate the total of the values (number-of-characters values output in `Public destination host/network` + 4 bytes). |
| `-p {ro\|rw_sync\|rw_sync_opt}` | Specify access permissions for the NFS share.<br>When you permit writing, specify whether to optimize synchronous writing as well. If you omit this option, it defaults to `rw_sync`.<br>Optimization of synchronous writing is a function that slightly delays a disk update by a write request, when the write request has been received from an NFS client while another relevant write request is being performed (or is about to be performed). Optimization can improve performance because the disk is updated by multiple write requests in one operation. If a write request of the data received by the NFS server is not very relevant, optimization may degrade performance. In this situation, specify synchronous writing without optimization (`rw_sync`).<br>▪ `ro`<br>Specify this if you do not want to permit writing to the NFS share.<br>▪ `rw_sync`<br>Specify this for synchronous writing without optimization.<br>▪ `rw_sync_opt`<br>Specify this for synchronous writing with optimization. |

| Item | Use |
|---|---|
| -a {everyone\|root_only\|none} | Specify this when you want to specify the users who access the NAS Modular system from the NFS client host and they are to be mapped as anonymous users. If you omit this option, root_only applies.<br>▪ everyone<br>Specify this when you map all users as anonymous users.<br>▪ root_only<br>Specify this when you map only the root user as an anonymous user.<br>▪ none<br>Specify this when you do not want to map users as anonymous users. |
| -u *UID* | Specify the user ID to be used in an anonymous user access. Specify a value within the range from 0 to 65535. If you omit this option, it defaults to 65534. |
| -g *GID* | Specify the group ID to be used in an anonymous user access. Specify a value within the range from 0 to 65535. If you omit this option, it defaults to 65534. |
| -t {perform\|do_not_perform} | Specify whether to accept only the requests from internet port lower than 1,024. If machines are to use internet port 1,024 or higher to access the file system, select do_not_perform. If you omit this option, it defaults to do_not_perform.<br>▪ perform<br>Specify this if you want to limit sending ports.<br>▪ do_not_perform<br>Specify this if you do not want to limit sending ports.<br>In AIX, internet port 1,024 or higher is used by default. Select do_not_perform when AIX is used as an NFS client host and you want to use the default internet port setting. In HP-UX, internet port 1,024 or higher is used for locking a file. Specify do_not_perform to use HP-UX as an NFS client host. |
| -s {perform\|do_not_perform} | Specify whether to verify that the accessed file exists in the shared directory subtree. If you omit this option, it defaults to perform.<br>▪ perform<br>Specify this if you want to perform a subtree check.<br>▪ do_not_perform<br>Specify this if you do not want to perform a subtree check. |
| -l {perform\|do_not_perform} | Specify whether to perform authentication on a lock request. If you omit this option, it defaults to do_not_perform.<br>▪ perform<br>Specify this if you want to perform authentication on a lock request.<br>▪ do_not_perform<br>Specify this if you do not want to perform authentication on a lock request |

## Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command and use it again, specifying a suitable parameter. |

| | |
|---|---|
| 10 | ▪ A name already registered in the system was specified for the argument of an option. Check the name and use the command again.<br>▪ The specified directory does not exist. Specify an already created directory.<br>▪ The specified shared directory is already used by another CIFS/NFS file share. Specify a directory not already made public by another file share use the command again.<br>▪ The specified network address of the client to be made public was not found. Specify an existing host or network.<br>▪ A value exceeding the maximum size that can be specified for a public destination host/network was specified. Enter a suitable value.<br>▪ An operation failed because the file system corresponding to the specified shared directory does not exist. In the **List of File Systems** check the file system name, and then specify the correct file system name.<br>▪ This operation cannot be performed because the capacity of the differential-data storage device is insufficient. Resolve the problem by using a NAS Sync Image operation.<br>▪ The number of created NFS file shares has reached the upper limit. Delete any unnecessary NFS file shares, and then create a new NFS file share. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then use again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | ▪ An attempt to acquire information about file shares has failed. A conflict with another system administrator's operation or an internal error may have occurred. Use the command again. Acquire all the Management log files if this error occurs again, and inform your HDS representative.<br>▪ The NFS file share creation failed. An error exists in the entered data or an unexpected error occurred during creation of an NFS share. Revise the entered values. Acquire all the Management log files if this error occurs again, and inform your HDS representative. |
| 70 | ▪ An operation cannot be performed because the file system corresponding to the specified directory is defined by the other node in the cluster. Specify a file share corresponding to a file system created on the operating node.<br>▪ The file system specified for the shared directory is not mounted. The resource group is in the OFFLINE state, or the resource group may be undergoing failover. If the resource group is in the OFFLINE state or the resource group is undergoing failover, remove the problem and use the command again. If the file system is not mounted, mount the file system and use the command again.<br>▪ The license of NAS Manager is not set. For details on license setup, see the *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform your HDS representative. |
| 98 | Some other error occurred. |

| | |
|---|---|
| 99 | ▪ An internal error occurred. Use the command again. Acquire all the Management log files if this error occurs again, and inform your HDS representative.<br>▪ The processing of the failover function has failed. Acquire all the Management log files, and Cluster log files, and contact your HDS representative.<br>▪ An attempt to acquire resource group information failed. Acquire all the Management log files, and Cluster log files, and contact your HDS representative.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and contact your HDS representative.<br>▪ A file sharing operation failed because the file system corresponding to the specified directory is blocked. Acquire all the Management log files, and Cluster log files, and contact your HDS representative.<br>▪ The specified operation failed. The file system or device file may be blocked. In the **List of File Systems**, check the state of the file system. If the file system has an error status, inform your HDS representative. If the file system does not have an error status, acquire all the Management log files and inform your HDS representative. |

- **Example**

  To create an NFS share with the following conditions:

  – Specify the directory to be made public as an NFS share to `/mnt/FS1/dir_case1` (`-d`).

  – Specify the public destination hosts to `host1`, `host2`, `host3`, and `host4` (`-H`).

  – Do not permit writing to the NFS share (`-p`).

```
$ sudo enas_nfscreate -d /mnt/FS1/dir_case1 -H
host1,host2,host3,host4 –p
ro
```

### 6.2.40 enas_nfsdelete (Delete NFS Shares)

- **Synopsis**

  `enas_nfsdelete -h|-d` *`shared-directory`* `{-a|-H` *`host`*`[,`*`host`*`...]}`

- **Description**

  Deletes an NFS share.

- **Arguments and Options**

**Table 6.29 enas_nfsdelete Arguments and Options**

| Item | Use |
|---|---|
| `-h` | Specify this option if you want to view the command syntax. |
| `-d` *`shared-directory`* | Specify the directory from which NFS shares are to be deleted.<br>When specifying a subdirectory under a file system:<br>`/mnt/`*`mounted-file-system-name/subdirectory`*<br>When specifying the whole of each file system:<br>`/mnt/`*`mounted-file-system-name`* |
| `-a` | Deletes all NFS shares specified in the `-d` option. |
| `-H` *`host`*`[,`*`host`*`...]` | Specify the public destinations for which public NFS shares are canceled.<br>Specify the public destinations specified in the `-H` option of the `enas_nfscreate` command. When you specify multiple public destinations, separate the destinations with commas (`,`). |

- **Example**

  Following is an example of deleting NFS shares of `/mnt/FS1/dir_case1` when the public destination is hosts to `host1` and `host2`:

```
$ sudo enas_nfsdelete -d /mnt/FS1/dir_case1 -H host1,host2
```

### 6.2.41 enas_nfsedit (Edit NFS Share Information)

- **Synopsis**

  enas_nfsedit -h|-d *shared-directory* -H *host*[,*host*...]
  [-p {ro|rw_sync|rw_sync_opt}] [-a {everyone|root_only|none }]
  [-u *UID*] [-g *GID*] [-t {perform|do_not_perform}]
  [-s {perform|do_not_perform}] [-l {perform|do_not_perform}]

- **Description**

  Edits the NFS share attributes. You can specify multiple public destinations at once in a command execution. You can also use the command once for each public destination. However, if you use the `enas_nfsedit` command multiple times on the same shared directory, the values specified in the following options are overwritten by the values specified in the last `enas_nfsedit` command execution.

  When an automatic creation schedule is set up in NAS Sync Image for a file system for which an NFS share was created, if a file share is automatically created for a differential-data snapshot, that NFS share is created based on the NFS share information edited by this command:

  `-u` option

  `-g` option

  `-t` option

  `-s` option

  `-l` option

- **Arguments and Options**

**Table 6.30 enas_nfsedit Arguments and Options**

| Item | Use |
|---|---|
| `-h` | Output the command format to the standard error. |
| `-d` *shared-directory* | Specify the public directory of NFS shares whose setting attributes are to be changed.<br>When specifying a subdirectory under a file system:<br>`/mnt/`*file-system-name*`/`*subdirectory*<br>When specifying the whole of each file system:<br>`/mnt/`*file-system-name* |
| `-H` *host*`[,`*host*`...]` | Specify the NFS share public destinations. Specify the public destinations specified in *public-destination* of the `enas_nfscreate` command. When you specify multiple public destinations, separate the destinations with commas (`,`).<br>The public destinations of the public directory to be specified must have already been registered. |

| Item | Use |
|---|---|
| -p {ro\|rw_sync\|rw_sync_opt} | Set access permissions for the NFS share.<br>When you permit writing, specify whether to optimize synchronous writing as well. If you omit this option, the current setting information applies.<br>Optimization of synchronous writing is a function that slightly delays a disk update by a write request, when the write request has been received from an NFS client while another relevant write request is currently being performed (or is about to be performed). Optimization can improve performance because the disk is updated by multiple write requests in one operation. If a write request of the data received by the NFS server is not very relevant, optimization may degrade performance. In this case, specify synchronous writing without optimization (rw_sync).<br>▪ ro<br>Specify this if you do not want to permit writing to the NFS share.<br>▪ rw_sync<br>Specify this for synchronous writing without optimization.<br>▪ rw_sync_opt<br>Specify this for synchronous writing with optimization. |
| -a {everyone\|root_only\|none} | Specify this when you want to specify the users who access the NAS Modular system from the NFS client host and they are to be mapped as anonymous users. If you omit this option, the current setting information applies.<br>▪ everyone<br>Specify this when you map all users as anonymous users.<br>▪ root_only<br>Specify this when you map only the root user as an anonymous user.<br>▪ none<br>Specify this when you do not want to map users as anonymous users. |
| -u *UID* | Specify the user ID to be used in an anonymous user access. Specify a value within the range from 0 to 65535. If you omit this option, the current setting information applies. |
| -g *GID* | Specify the group ID to be used in an anonymous user access. Specify a value within the range from 0 to 65535. If you omit this option, the current setting information applies. |
| -t {perform\|do_not_perform} | Specify whether to accept only the requests from internet port lower than 1,024. Select do_not_perform if machines will use internet port 1,024 or higher to access the file system. If you omit this option, the current setting information applies.<br>▪ perform<br>Specify this if you want to limit sending ports.<br>▪ do_not_perform<br>Specify this if you do not want to limit sending ports.<br>In AIX, internet port 1,024 or higher is used by default. Select do_not_perform when AIX is used as an NFS client host and you want to use the default internet port setting. In HP-UX, internet port 1,024 or higher is used for locking a file. Specify do_not_perform to use HP-UX as an NFS client host. |

| Item | Use |
|---|---|
| `-s {perform\|do_not_perform}` | Specify whether to check that the accessed file exists in the shared directory subtree. If you omit this option, the current setting information applies.<br>▪ `perform`<br>Specify this if you want to perform a subtree check.<br>▪ `do_not_perform`<br>Specify this if you do not want to perform a subtree check. |
| `-l {perform\|do_not_perform}` | Specify whether to perform authentication on a lock request. If you omit this option, the current setting information applies.<br>▪ `perform`<br>Specify this if you want to perform authentication on a lock request.<br>▪ `do_not_perform`<br>Specify this if you do not want to perform authentication on a lock request. |

- **Example**

  To change information on NFS shares of `mnt/FS1/dir_case1` to the following conditions:

  – Specify the public destinations to `host1`, `host2`, `host3`, and `host4` (`-H`).

  – Do not perform user mapping for anonymous users (`-a`).

```
$ sudo enas_nfsedit -d /mnt/FS1/dir_case1 -H
host1,host2,host3,host4 -a none
```

### 6.2.42 enas_nfslist (List NFS Share Information)

- **Synopsis**

  `enas_nfslist -h|[-d` *shared-directory*`] [-c]`

- **Description**

  Displays a list of information on the NFS shares that are made public on the node you are operating. The information is displayed by combination of NFS share shared directory and public destination in ascending order.

**Table 6.31 Information Displayed when Executing the enas_nfslist Command**

| Item | Description |
|---|---|
| `Shared directory` | Displays the full path of the NFS shared directory. |
| `Public destination host/network` | Displays the name of a host or network accessing the NFS share. |
| `Permission mode / Synchronous writing` | Displays information about the access permission for the NFS share and the synchronous write mode. |
| `Anonymous mapping` | Displays users who are mapped as anonymous users. |
| `Anonymous UID` | Displays the user ID to be used when accessing the NFS share as an anonymous user. |
| `Anonymous GID` | Displays the group ID to be used when accessing the NFS share as an anonymous user. |
| `Transmission port restriction` | Displays whether to accept only the requests from internet port lower than 1,024. |
| `Subtree check` | Displays whether to check if the accessed file is in a subtree of the shared directory. |
| `Access check with lock request` | Displays whether to authenticate lock requests. |

- **Arguments and Options**

**Table 6.32 enas_nfslist Arguments and Options**

| Item | Use |
|---|---|
| `-h` | Output the command format to the standard error. |
| `-d` *shared-directory* | Specify the shared directory of the NFS shares on which you want to display the information. If you omit this option, the command displays all the information on the NFS shares on the node you are operating. |
| `-c` | Specify to display NFS share information separated with colons (`:`). For example:<br>*Shared-directory*`: - :`*Access-check-with-lock-request*<br>`:`<br>`:` (Repeatedly displayed for each NFS share directory and public destination.)<br>`:`<br>If you omit this option, information is displayed in a detailed format:<br>`List of File Shares:`<br>`The number of NFS share(`*counter*`) (1)`<br>*item-name*`: `*value*<br>`:` |

| | |
|---|---|
| | :(All items are output.)<br>:<br>(One blank line) (2)<br>:<br>: ((1) through (2) is output for each NFS share name and public destination.)<br>:<br>*counter*: The value starts from 1, and a number is assigned to each NFS share name and public destination.<br>*item-name*: An item in Table 6.11 is displayed.<br>*value*: The value of an item in Table 6.11 is displayed. |

### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command and use the command again, specifying a suitable parameter. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then use again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | An attempt to acquire information about file shares has failed. A conflict with another system administrator's operation or an internal error may have occurred. Use the command again. Acquire all the Management log files if this error occurs again, and inform your HDS representative. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first.<br>▪ The specified file share does not exist on the operating node. The file share was created on the other node, the resource group is in the OFFLINE state, or the resource group is undergoing failover. Make sure that the following items corresponding to the specified file share are correct: the file system name, and the resource group state. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform your HDS representative. |
| 98 | Some other error occurred. |
| 99 | ▪ An internal error occurred. Use the command again.. Acquire all the Management log files if this error occurs again, and inform your HDS representative.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and contact your HDS representative. |

- **Examples**
  - To display the information on NFS shares of `/mnt/FS1/SUBDIR1` specifying the `-c` option:

    ```
    $ sudo enas_nfslist -d /mnt/FS1/SUBDIR1 -c
    /mnt/FS1/SUBDIR1:*:rw_sync:root_only:--:--
    :do_not_perform:perform:do_not_perform
    ```

  - To display the information on NFS shares of `/mnt/FS1/SUBDIR1` without specifying the `-c` option:

```
$ sudo enas_nfslist -d /mnt/FS1/SUBDIR1
List of File Shares:
The number of NFS share(1)
  Shared directory             : /mnt/FS1/SUBDIR1
    Public destination host/network    : *
    Permission mode / Synchronous writing : rw_sync
    Anonymous mapping           : root_only
    Anonymous UID             : --
    Anonymous GID             : --
    Transmission port restriction     : do_not_perform
    Subtree check             : perform
    Access check with lock request    : do_not_perform
```

### 6.2.43 enas_ping (Display the connection to a specified host

Displays the connection status of the specified host. The displayed information is the same as that displayed by the Linux `ping` command.

The displayed information is added to the beginning of the log file. When the log file exceeds 1 MB, information equivalent to the amount by which the maximum size was exceeded is deleted from the end of the log file. The packet dump file is also output as a log file at the same time. You can obtain the log by downloading all the log data from the **List of RAS Information** (Batch-download) window. For details on downloading all log data, see section )

- **Synopsis**

  enas_ping [-c count] [-p pattern] [-s packetsize] host

- **Description**

  Checks the connection to the specified IP address. The displayed contents are the same as when the Linux® ping command is used. The contents are accumulated in the log file. The output information is added to the beginning of the log file. If a file size exceeds 1 MB, then an amount of information, equal to the amount of information by which the maximum was exceeded, is deleted from the end of the log file. The packet dump file is also output as a log file at the same time.

  A log file can be downloaded and obtained. All log data can be downloaded and obtained from the **List of RAS Information** (Batch-download) window. For details on downloading all log data, see section 4.13.10.

  ***Notes:***

- Multiple processes cannot use the enas_ping command concurrently. If the enas_ping command is used concurrently by multiple processes, an exclusive control error occurs and failed to lock is displayed. If you want to use the enas_ping command, use the command after making sure that the process executing the enas_ping command has ended. If an exclusive control error occurs while no other processes are executing the `enas_ping` command, execute the `enas_eraselog` command, and then execute the `enas_ping` command again.
  - Information may not appear immediately due to internal buffering.

- **Arguments and Options**

**Table 6.33 enas_ping Arguments and Options**

| Item | Use |
|---|---|
| -c count | Specify the number of packets to be sent. The maximum specifiable number of packets is 10. If you omit this option, this option is set to 10. |
| -p pattern | Specify a pattern for filling the ping packet to be sent. You can specify a maximum of 16 bytes. You can use this option for diagnosing data-dependent network problems. For example, if you specify `-p ff`, the packet will be filled entirely with 1s. |
| -s packetsize | Specify the number of bytes to be sent. The default is 56. |
| host | Specify the target host name or IP address. |

- **Return Values**

| | |
|---|---|
| 0 | The command terminated normally. |
| 1 | ▪ There are 11 or more packets specified for the `-c` option. Set a value of 10 or less, and then re-execute.<br>▪ The specified option is invalid. Specify a valid option.<br>▪ An internal error occurred. Retry execution. |

- **Example**

**To check the connection to the host `raid01`:**

```
$ sudo enas_ping raid01
PING raid01 (10.208.151.100): 56 data bytes
64 bytes from 10.208.151.100: icmp_seq=0 ttl=255 time=1.4 ms
64 bytes from 10.208.151.100: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from 10.208.151.100: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=4 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=5 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=6 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=7 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=8 ttl=255 time=0.2 ms
64 bytes from 10.208.151.100: icmp_seq=9 ttl=255 time=0.3 ms

--- raid01 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.3/1.4 ms
```

### 6.2.44 enas_quotaget (Display the quota information set for a file system)

- **Synopsis**

  enas_quotaget [-c] [-u [user-name|user-ID][,[user-name|user-ID]...]|
  -g [group-name|group-ID][,[group-name|group-ID]...]]
  file-system-name

  enas_quotaget [-c] [-u|-g] -v file-system-name

  enas_quotaget [-c] [-u|-g] -w file-system-name

  enas_quotaget [-c] -d file-system-name

  enas_quotaget [-c] -t file-system-name

  enas_quotaget [-c] -m file-system-name

  enas_quotaget -h

- **Description**

Displays the quota information set for a file system.

When you want to view the quota information of a user or group, the displayed information varies, depending on the combination of an option and an argument. Use options and arguments appropriately according to your purpose.

When specifying a specific user or group

The quota information of a specified user or group is displayed.

When specifying the `-v` option

The quota information of all users or groups registered by NAS Manager, the NIS server, and the LDAP server for user authentication is displayed.

When you specify the `-w` option

The information of users and groups that have exceeded the soft limit or grace period, among all users or groups registered by NAS Manager, the NIS server, and the LDAP server for user authentication, is displayed.

When you omit the `-v` option and `-w` option without specifying a specific user or group

The following information is displayed:

– The quota information of all users or groups that are using the file system

The information of all users or groups that are set quotas

- **Arguments and Options**

**-c**

Specify this if you want to **Display Quota** information separated with colons (:).

**-d**

Specify this to display the default quota information set for a specified file system.

**-g**

Specify this option if you want to view group quota information.

**-g** {***group-name***|***group-ID***}**[,**{***group-name***|***group-ID***}**...]**

If you want to view the specific group information only, specify the target group names or group IDs.

You can specify any of the following groups by group name:

- Groups registered by NAS Manager (group IDs: 97 and 104 to 2,147,483,147)
- Groups registered in the NIS server or LDAP server for user authentication (other than groups whose group ID is 0)
- Groups registered by user mapping

When you specify a group ID, specify a valid value within the range 0 to 2,147,483,147. Note that you cannot specify 0 at the beginning of a group ID that begins with a value other than 0.

When specifying multiple group names or group IDs, separate them with commas (,). Multiple group names or group IDs can coexist.

If multiple groups are specified and one of the group names or group IDs is invalid, quota information will not be displayed for any groups.

**-h**

Specify this option if you want to view the command syntax.

**-m**

Specify this option to view the settings for quota monitoring.

**-t**

Specify this option to view the grace period after the soft limit is exceeded.

**-u**

Specify this option to view user quota information.

**-u** {***user-name***|***user-ID***}**[,**{***user-name***|***user-ID***}**...]**

Specify this option to view the information of a specific user.

You can specify any of the following users by the user name:

- Users registered by NAS Manager (user IDs: 97 and 104 to 2,147,483,147)
- Users registered in the NIS server or LDAP server for user authentication (other than users whose user ID is 0)
- Users registered by user mapping

When you specify a user ID, specify a valid value within the range 0 to 2,147,483,147. Note that you cannot specify 0 at the beginning of a user ID that begins with a value other than 0.

When specifying multiple user names or user IDs, separate them with commas (,). Multiple user names or user IDs can coexist.

If multiple users are specified and one of the user names or user IDs is invalid, quota information will not be displayed for any users.

**-v**

Specify this option to view the quota information of all users or groups registered by NAS Manager, the NIS server, and the LDAP server for user authentication.

**-w**

Specify this option to view only the information of users or groups that have exceeded the soft limit or grace period.

***file-system-name***

Specify the name of the file system.

## Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.34 Display When Executing enas_quotaget Command (quota info user or group)**

| Item | Description |
|---|---|
| `List of Quota Information of File System` | The file system name is displayed. |
| `User name` or `Group name` | The user name or the group name is displayed.<br>If the user ID or group ID cannot be converted to a user name or group name, |

| | |
|---|---|
| | a hyphen (-) is displayed. |
| UID or GID | The user ID or the group ID is displayed. |
| Block(MB) | Block usage by individual users or each group is displayed.<br>Used capacity<br>Block space used (units: MB).<br>Soft limit<br>Soft limit for block usage (units: MB)<br>Hard limit<br>Hard limit for block usage (units: MB)<br>Grace period<br>Remaining grace time until files can no longer be created or updated after the block usage exceeds the soft limit. Displayed in one of the following formats:<br>*n* days<br>The remaining grace time is 24 hours or longer. For example, 1 days appears if there are 24 hours or more, but less than 48 hours remaining.<br>*n* hours<br>The remaining grace time is less than 24 hours. For example, 0 hours appears if less than 1 hour remains.<br>over<br>Either the grace period has expired or block usage has reached the hard limit. over is displayed.<br>-<br>The user's block usage is within the soft limit. |
| i-node | i-node usage by individual users or each group is displayed.<br>Used count<br>Number of i-nodes used.<br>Soft limit<br>Soft limit for i-node usage.<br>Hard limit<br>Hard limit for i-node usage.<br>Grace period<br>Remaining grace time until files can no longer be created after the user's i-node usage exceeds the soft limit. Displayed in one of the following formats:<br>*n* days<br>The remaining grace time is 24 hours or longer. For example, 1 days appears if there are 24 hours or more, but less than 48 hours remaining.<br>*n* hours<br>The remaining grace time is less than 24 hours. For example, 0 hours appears if less than 1 hour remains.<br>over<br>Either the grace period has expired or i-node usage has reached the hard limit.<br>-<br>The user's i-node usage is within the soft limit. |

**Table 6.35 Display When Executing enas_quotaget Command (default quota)**

| Item | Description |
|---|---|
| `Default Quota Information of File System` | The file system name is displayed. |
| `Block(MB)` | The soft and hard limits for block usage that are set as default quotas are displayed.<br>`Soft limit`<br>Soft limit for block usage (units: MB)<br>`Hard limit`<br>Hard limit for block usage (units: MB) |
| `i-node` | The soft and hard limits values for i-node usage that are set as default quotas are displayed.<br>`Soft limit`<br>Soft limit for i-node usage.<br>`Hard limit`<br>Hard limit for i-node usage. |

**Table 6.36 Display When Executing enas_quotaget Command (grace period)**

| Item | Description |
|---|---|
| `Grace Period Information of File System` | The file system name is displayed. |
| `Block grace period` | Displays the grace period until files can no longer be created or updated after block usage exceeds the soft limit. |
| `i-node grace period` | Displays the grace period until files can no longer be created after i-node usage exceeds the soft limit. |

**Table 6.37 Info Dsplayed When Executing enas_quotaget Command (monitoring method)**

| Item | Description |
|---|---|
| `Monitoring Time of File System` | The file system name is displayed. |
| `SNMP notification mode` | Displays the SNMP trap notification mode that applies when a quota is exceeded.<br>`Use a summary notification`<br>Summary notification mode is set.<br>`Use individual notifications`<br>Individual notification mode is set. |
| *monitoring-times* | Displays quota monitoring times.<br>If you specified the `-c` option, the polling times are displayed without a colon (`:`) between the hour and minute. If several times are set, those times are displayed, separated by a comma (,). |

## Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| 10 | ▪ The specified file system does not exist. Check the target file system by using the `enas_fslist` command, and then retry the operation.<br>▪ A file system with Quota applied is unmounted. Mount the target file system, and then retry.<br>▪ Quota is not applied as a mount option of the target file system. Apply Quota as a mount option of the target file system, and then retry.<br>▪ The specified user or group might have been deleted by another system administrator. When using an NIS server or user mapping, connection to the server might not have been possible. A user or group that is not registered in the system or that cannot perform quota settings might have been specified.<br>When using an NIS server or user mapping, make sure that connection to the server is possible. If you are not using a server or if connection to the server was possible, make sure that the specified user or group is registered in the system and that the specified user or group can perform quota settings, and then retry the operation.<br>▪ This operation cannot be performed because the capacity of the differential-data storage device is insufficient. Resolve the problem by using a NAS Sync Image operation.<br>▪ The specified notification mode cannot be changed. Only the notification mode cannot be changed, because a monitoring time is not set. Set one or more monitoring times, and then try again. |
| 65 | ▪ Some of the resources to be used for the requested processing are being used by another user. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node.<br>▪ An internal error occurred. A conflict with another system administrator's operation or system error may have occurred. Retry. Acquire all the Management log files if the error occurs again, and then inform maintenance personnel. |
| 66 | ▪ Acquisition of quota setting information failed because of an unexpected error in internal processing. A problem may exist in the acquisition processing of the quota information. Acquire all the Management log files, and then inform maintenance personnel.<br>▪ An attempt to access a system file (crontab) failed. Acquire all the Management log files, and then inform maintenance personnel.<br>▪ Acquisition of the grace period information failed because of an unexpected error in internal processing. Acquire all the Management log files, and then inform maintenance personnel. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first.<br>▪ An error has occurred in the file system or differential-data storage device. Alternatively, a failover has occurred or the resource group was placed offline during processing. If a failover has occurred, perform a failback and then re-execute the command. If the resource group is offline, place it online and then re-execute the command. If the resource group is operating normally, contact maintenance personnel and ask them to check for an error. |
| 99 | ▪ The specified file system is blocked. Unmount and then delete the specified file system. Then, request maintenance personnel to recover the LU error. If necessary, create a new file system and then use backup data to restore the data. If the error occurs repeatedly, acquire all the Management log files and contact maintenance personnel.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and contact maintenance personnel. |

## Examples

### To view quota information of a specific user according to the following conditions, by specifying the -c option:

- The file system name is FS1.
- Display information for User1 (user ID: 6000) and User2 (user ID: 6001).

```
$ sudo enas_quotaget -c -u User1,6001 FS1
FS1:User1:6000:0:100:200:-:0:300:400:-
FS1:User2:6001:200:100:300:6 days:300:200:400:over
```

### To view quota information of a specific user according to the following conditions without specifying the -c option:

- The file system name is FS1.
- Display information for User1 (user ID: 6000) and User2 (user ID: 6001).

```
$ sudo enas_quotaget -u User1,6001 FS1
List of Quota Information of File System(FS1):
The number of quota information(1)
User name : User1
UID    : 6000
Block (MB) Used capacity : 0
      Soft limit  : 100
      Hard limit  : 200
      Grace period : -
i-node   Used count  : 0
      Soft limit  : 300
      Hard limit  : 400
      Grace period : -

The number of quota information(2)
User name : User2
UID    : 6001
Block (MB) Used capacity : 200
      Soft limit  : 100
      Hard limit  : 300
      Grace period : 6 days
i-node   Used count  : 300
      Soft limit  : 200
      Hard limit  : 400
      Grace period : over
```

### To view the quota information of a specific group according the following conditions without specifying the -c option:

- The file system name is FS1.
- Display information for Group1 (group ID: 5000) and Group2 (group ID: 5001).

```
$ sudo enas_quotaget -g Group1,5001 FS1
List of Quota Information of File System(FS1):
The number of quota information(1)
Group name : Group1
GID    : 5000
Block (MB) Used capacity : 0
```

```
      Soft limit  : 100
      Hard limit  : 200
      Grace period : -
i-node   Used count  : 0
      Soft limit  : 300
      Hard limit  : 400
      Grace period : -

The number of quota information(2)
Group name : Group2
GID    : 5001
Block (MB) Used capacity : 200
      Soft limit  : 100
      Hard limit  : 300
      Grace period : 6 days
i-node   Used count  : 300
      Soft limit  : 200
      Hard limit  : 400
      Grace period : over
```

**To view the default quota information of the `FS1` file system without specifying the `-c` option:**

```
$ sudo enas_quotaget -d FS1
Default Quota Information of File System(FS1):
Block (MB) Soft limit(default) : 100
      Hard limit(default) : 200
i-node   Soft limit(default) : 300
      Hard limit(default) : 400
```

**To view the grace period of the quota set for the `FS1` file system without specifying the `-c` option:**

```
$ sudo enas_quotaget -t FS1
Grace Period Information of File System(FS1):
Block grace period : 10 days
i-node grace period : 20 days
```

**To view the monitoring settings of the quota set for the `FS1` file system without specifying the `-c` option:**

```
$ sudo enas_quotaget -m FS1
Monitoring Time of File System(FS1):
SNMP notification mode: Use a summary notification
10:15
13:25
```

### 6.2.45 enas_quotaset (Set quotas for a file system)

- **Synopsis**

  enas_quotaset
  {-u {user-name|user-ID}[,{user-name|user-ID}...]|
  -g {group-name|group-ID}[,{group-name|group-ID}...]}
  [-b block-soft-limit,block-hard-limit]
  [-i *i-node-block-soft-limit,i-node-block-hard-limit*]
  file-system-name

  enas_quotaset -d
  [-b block-soft-limit,block-hard-limit]
  [-i *i-node-block-soft-limit,i-node-block-hard-limit*]
  file-system-name

  enas_quotaset -t
  [-b block-grace-period]
  [-i i-node-grace-period]
  file-system-name

  enas_quotaset -m
  {[-s monitoring-time[,monitoring-time...]]
  [-n {summary|individual}]|
  -s default}
  file-system-name

  enas_quotaset -h

- **Description**

  Sets quotas for a file system.

- **Arguments and Options**

**Table 6.38 enas_quotaset Arguments and Options**

| Item | Use |
|---|---|
| -h | Specify to output the command format to the standard error. |
| -g<br>{*group-name* \| *group-ID*} [, {*group-name* \| *group-ID*}...] | Specify the group names or group IDs for which you want to set quotas.<br>You can specify any of the following groups by group name:<br>Groups registered by NAS Manager (group IDs: 97 and 104 to 2,147,483,147)<br>Groups registered in the NIS server or LDAP server for user authentication (other than groups whose group ID is 0)<br>Groups registered by user mapping<br>When you specify a group ID, specify a valid value within the range 0 to 2,147,483,147. Note that you cannot specify 0 at the beginning of a group ID that begins with a value other than 0.<br>When specifying multiple group names or group IDs, separate them with commas (,). Multiple group names and group IDs can coexist.<br>If multiple groups are specified and one of the specified group names or group IDs is invalid, a quota is not set for any of the specified groups. |
| -d | Specify to set the default quota for the specified file system. |
| -u<br>{*uname*\|*uid*}[,*uname*\|*uid*...] | Specify the user names or user IDs for which you want to set quota.<br>You can specify any of the following users by the user name:<br>Users registered by NAS Manager (user IDs: 97 and 104 to 2,147,483,147)<br>Users registered in the NIS server or LDAP server for user authentication (other than groups whose group ID is 0)<br>Users registered by user mapping<br>When you specify a user ID, specify a valid value within the range 0 to 2,147,483,147. Note that you cannot specify 0 at the beginning of a user ID that begins with a value other than 0.<br>When specifying multiple user names or user IDs, separate them with commas (,). Multiple user names and user IDs can coexist.<br>If multiple users are specified and one of the specified user names or user IDs is invalid, a quota is not set for any of the specified users. |
| -b *block-soft-limit,block-hard-limit* | Specify the soft limit and hard limit for block usage, separated with commas (,) (units: MB). If t Specify the soft and hard limits for block usage, separated with commas (,) (units: MB). Specify a valid value within the range 0 to 2,097,151<br>If this option is omitted, the soft and hard limits for block usage are set as follows:<br>When the -d option is specified:<br>If the default quota is already specified, the current setting value is inherited.<br>If no default quota is set, the soft and hard limits for block usage will be set to 0 (no limits).<br>When the -g option is specified:<br>If a quota is already specified for the group, the current setting value is inherited.<br>If no quota is set for the specified group, the soft and hard limits for block usage will be set to 0 (no limits).<br>When the -u option is specified:<br>If a quota is already specified for the user, the current setting value is inherited.<br>If only a default quota is set and no quota is set for the user, the set default quota will apply.<br>If no default quota is set and no quota is set for the specified user, the soft and hard limits for block usage by the specified user will be set to 0 (no limits). |

| Item | Use |
|---|---|
| -i *i-node-soft-limit,i-node-hard-limit* | Specify the soft limit and hard limit for i-node usage, separated with commas (,).Specify a valid value within the range 0 to 2,147,483,647. If this option is specified, the soft limit and hard limit for i-node usage are set as follows:<br>▪ When the -d option is specified:<br>If the default quota is already set, the current setting value is inherited.<br>If the default quota is not set, the soft limit and hard limit for i-node usage will be 0 (no limits).<br>▪ When the -g option is specified:<br>If a quota is already set for the group, the current setting value is inherited.<br>If no quota is set for the specified group, the soft and hard limits for i-node usage by the specified group will be set to 0 (no limits).<br>▪ When the -u option is specified:<br>If a quota is already set for the user, the current setting value is inherited.<br>If a quota is not set for each user and default quota is set, the default quota setting is applied.<br>If neither a quota for each user nor the default quota is set, the soft limit and hard limit for i-node usage will be 0 (no limits). |
| -b *block-grace-period* | Specify the grace period (number of days) until files can no longer be created or updated after block usage exceeds the soft limit. Specify a value from 1 to 9,999. The value cannot begin with 0 (no limits).<br>The initial setting is 7 days. If you omit this argument, the current setting applies. |

| Item | Use |
|---|---|
| -i *i-node-grace-period* | Specify the grace period (number of days) until files can no longer be created after i-node usage exceeds the soft limit. Specify a value from 1 to 9,999. The value cannot begin with 0.<br>The initial setting is 7 days. If you omit this argument, the current setting applies.<br>-m<br>Specify this option to enable or disable quota monitoring.<br>-n {summary\|individual}<br>Specify this option to set the SNMP trap notification mode when NAS Manager detects users or groups that exceed the soft limit or grace period.<br>The initial setting disables the SNMP trap notification. If you omit this option with no monitoring times set, the summary notification mode is applied. Also, if you omit this option with one or more monitoring times set, the current setting is inherited.<br>summary<br>Specify this to output an SNMP trap in summary notification mode. You can also specify s instead of summary.<br>individual<br>Specify this to output an SNMP trap in individual notification mode. You can also specify i instead of individual.<br>-s<br>Specify this option to set or clear monitoring times for NAS Manager to monitor quotas.<br>The initial setting is no quota monitoring. If you omit this option, the current setting applies.<br>*monitoring-time* [ , *monitoring-time* . . . ]<br>Specify the times at which NAS Manager monitors quotas. All previously set monitoring times are cleared, and then the specified times are set.<br>Specify a value from 00 hours 00 minutes to 23 hours 55 minutes (format: *hhmm*) in units of 5 minutes. If specifying a value by using a colon ( : ) as a delimiter, you can omit 0 at the uppermost digit of hours and minutes of the monitoring time. For example, to specify 01 hour 05 minutes as a monitoring time, write 01:05, 01:5, 1:05, 1:5, or 0105.<br>Separate multiple monitoring times with commas. You can specify a maximum of 48 monitoring times.<br>default<br>Specify this option to clear all monitoring times and set quota monitoring to the initial state (no monitoring).<br>-t<br>Specify this option to set a grace period. |
| | |
| *file-system-name* | Specify the name of the file system. |

## Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| 10 | ▪ A character other than a numerical value is entered in the block limit value. Enter a numerical value.<br>▪ A character other than a numerical value is entered in the i-node limit value. Enter a numerical value.<br>▪ A value larger than the hard limit was specified for the soft limit. The setting of a soft limit value exceeding the hard limit value cannot be performed. Enter a soft limit value no greater |

| | |
|---|---|
| | than the hard limit value.<br>▪ The specified file system does not exist. Check the target file system by using the `enas_fslist` command, and then retry the operation.<br>▪ The block limit value exceeds the maximum, so execution cannot start. Retry after entering a value no greater than the maximum setting for a block limit value (2,097,151).<br>▪ The i-node limit value exceeds the maximum, so execution cannot start. Retry after entering a value no greater than the maximum setting value for an i-node limit value (2,147,483,647).<br>▪ A file system with Quota applied is unmounted. Mount the target file system, and then retry.<br>▪ Quota is not applied as a mount option of the target file system. Apply Quota as a mount option of the target file system, and then retry.<br>▪ The specified user or group might have been deleted by another system administrator. When using an NIS server or user mapping, connection to the server might not have been possible. A user or group that is not registered in the system or that cannot perform quota settings might have been specified.<br>When using an NIS server or user mapping, make sure that connection to the server is possible. If you are not using a server or if connection to the server was possible, make sure that the specified user or group is registered in the system and that the specified user or group can perform quota settings, and then retry the operation.<br>▪ This operation cannot be performed because the capacity of the differential-data storage device is insufficient. Resolve the problem by using a NAS Sync Image operation.<br>▪ This operation cannot be performed because the specified file system is a differential-data snapshot.<br>▪ The entered value for the grace period exceeds the maximum. Retry after entering a value no greater than the maximum setting value for a grace period (9,999).<br>▪ A value smaller than the current usage amount cannot be set for the hard limit for block usage or hard limit for i-node usage. Enter a value equal to or larger than the current usage amount.<br>▪ The specified notification mode cannot be changed. Only the notification mode cannot be changed, because a monitoring time is not set. Set one or more monitoring times, and then try again.<br>▪ A zero cannot be specified at the beginning of a grace period. Specify a numerical value that does not start with 0. |
| `65` | An internal error occurred. A conflict with another system administrator's operation or system error may have occurred. Retry. Acquire all the Management log files if the error occurs again, and then inform maintenance personnel. |
| `66` | ▪ Acquisition of quota setting information failed because of an unexpected error in internal processing. A problem may exist in the acquisition processing of the quota information. Acquire all the Management log files, and then inform maintenance personnel.<br>▪ The setting of the quota information failed because of an unexpected error in internal processing. A problem may exist in the setting processing of the quota information. Acquire all the Management log files, and then inform maintenance personnel.<br>▪ The setting of the quota information failed because of an unexpected error in internal processing. Acquire all the Management log files, and then inform maintenance personnel.<br>▪ The updating of the grace period failed because of an unexpected error in internal processing. Acquire all the Management log files, and then inform maintenance personnel.<br>▪ An attempt to access a system file (crontab) failed. Acquire all the Management log files, and then inform maintenance personnel.<br>▪ Editing of the monitoring time failed because of an unexpected error in internal processing. Acquire all the Management log files, and then inform maintenance personnel. |
| `70` | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| `99` | ▪ The specified file system is blocked. Unmount and then delete the specified file system. Then, |

| | |
|---|---|
| | request maintenance personnel to recover the LU error. If necessary, create a new file system and then use backup data to restore the data. If the error occurs repeatedly, acquire all the Management log files and contact maintenance personnel.<br>▪ An error occurred in the shared processing of commands. Acquire all the Management log files and contact maintenance personnel. |

- **Examples**

### To set user quotas according to the following conditions:

- The file system name is `FS1`.
- Set quotas for `User1` (user ID: 6000) and `User2` (user ID: 6001).
- Set the soft limit of block usage to 1.5 GB and the hard limit to 2 GB.
- Set the soft limit of i-node usage to `300` and the hard limit to `400`.

```
$ sudo enas_quotaset -u User1,6001 -b 1536,2048 -i 300,400 FS1
```

### To set user quotas according to the following conditions:

- The file system name is `FS1`.
- Set quotas for `user3`, which was registered by user mapping.
- Set the soft limit of block usage to 1.5 GB and the hard limit to 2 GB.
- Set the soft limit of i-node usage to `300` and the hard limit to `400`.

```
$ sudo enas_quotaset -u "DOMAIN02\user3" -b 1536,2048 -i 300,400 FS1
```

### To set group quotas according to the following conditions:

- The file system name is `FS1`.
- Set quotas for `Group1` (group ID: 5000) and `Group2` (group ID: 5001).
- Set the soft limit of block usage to 1.5 GB, and the hard limit to 2 GB.
- Set the soft limit of i-node usage to `300`, and the hard limit to `400`.

```
$ sudo enas_quotaset -g Group1,5001 -b 1536,2048 -i 300,400 FS1
```

### To set a default quota according to the following conditions:

- The file system name is `FS1`.
- Set the soft limit of block usage to 1.5 GB and the hard limit to 2 GB.
- Set the soft limit of i-node usage to `300` and the hard limit to `400`.

```
$ sudo enas_quotaset -d -b 1536,2048 -i 300,400 FS1
```

### To set grace periods according to the following conditions:

- The file system name is `FS1`.
- Set the grace period for block usage to 10 days.
- Set the grace period for i-node usage to 10 days.

```
$ sudo enas_quotaset -t -b 10 -i 10 FS1
```

**To set quota monitoring according to the following conditions:**

- The file system name is `FS1`.
- Set the quota monitoring times to 01:05 and 13:15.
- Report summary information in SNMP traps.

```
$ sudo enas_quotaset -m -s 0105,1315 -n summary FS1
```

### 6.2.46 enas_rgmon (Disable and restart resource group monitoring)

#### Synopsis

```
enas_rgmon {-on|-off} [--] resource-group-name
enas_rgmon -h
```

#### Description

Disables or restarts monitoring of a resource group.

You can execute this command when the resource group status is as follows:

To disable resource group monitoring:

The resource group status is `Online/No error`.

To restart resource group monitoring:

The resource group status is `Online Maintenance/No error`.

#### Options and arguments

**`-h`**

Specify this option if you want to view the command syntax.

**`-off`**

Specify this option if you want to disable monitoring of the resource group.

**`-on`**

Specify this option if you want to restart monitoring of the resource group.

**`--`**

Specify this to prevent all of the character string following this option from being treated as an option. For example, if you want to specify `-h` as the resource group name, specify `-- -h`.

***resource-group-name***

Specify the name of the resource group you want to disable or restart monitoring of.

#### Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |

| | |
|---|---|
| 22 | The specified resource group does not exist. Specify an existing resource group, and then try again. |
| 32 | The node status is not UP or the resource group status is not Online/No error. Check the status of the node and resource group, start the node and the resource group, and then try again. |
| 33 | The node status is not UP or the resource group status is not Online Maintenance/No error. Check the status of the node and resource group, place the node and the resource group in a monitoring status, and then try again. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | The processing of the failover function has failed. If this message is displayed when performing a manual failover, make sure that the failover-destination node has started. In other cases, check (in all nodes in the cluster) whether a KAQG7*nnnn* message was output to the system messages. If a system message was output, take appropriate action. If you cannot identify the cause, acquire all the Management log files and Cluster log files, and then inform maintenance personnel. |
| 68 | Another user might be performing a cluster or resource group operation. Check the status of the cluster, node, and resource group, and then try again once the status allows execution. If an error occurs again, acquire all of the Management log files and contact maintenance personnel. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | An internal error occurred. Acquire all the Management log files and inform maintenance personnel. |

## Examples

### To disable monitoring of the resource group nodennc2:

```
$ sudo enas_rgmon -off nodennc2
```

### To restart monitoring of the resource group nodennc2:

```
$ sudo enas_rgmon -on nodennc2
```

### 6.2.47 enas_rgmove (Change the execution node of a resource group)

#### Synopsis

```
enas_rgmove [--] resource-group-name
enas_rgmove -h
```

#### Description

Changes the execution node of a resource group.

You can execute this command when the status of the destination node and resource group is as follows:

- The status of the destination node is `UP`.
- The status of the resource group is `Online/No error` or `Online Maintenance/No error`.

#### Options and arguments

**`-h`**

Specify this option if you want to view the command syntax.

**`--`**

Specify this to prevent all of the character string following this option from being treated as an option. For example, if you want to specify `-h` as the resource group name, specify `-- -h`.

***resource-group-name***

Specify the name of the resource group whose execution node you want to change.

#### Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| `22` | The specified resource group does not exist. Specify an existing resource group, and then try again. |
| `30` | The resource group status is not `Online/No error`, `Online Ready/No error`, or `Online Maintenance/No error`. Check the resource group status, start the resource group, and then try again. |
| `37` | Another user might be operating the cluster or resource group, or a failover might be occurring. Check the status of the cluster, node, and resource group, and then try again once the statuses allow execution. If an error occurs again, acquire all of the Management log files and contact maintenance personnel. |
| `38` | The status of the node operating the resource group is not `UP`. Start the node operating the resource group, and then try again. If an error occurs again, acquire all of the Management log files and |

| | |
|---|---|
| | contact maintenance personnel. |
| 39 | The status of the node that is the move destination of the resource group is not UP. Start the node that is the move destination of the resource group, and then try again. If an error occurs again, acquire all of the Management log files and contact maintenance personnel. |
| 66 | The processing of the failover function has failed. If this message is displayed when performing a manual failover, make sure that the failover-destination node has started. In other cases, check (in all nodes in the cluster) whether a KAQG7*nnnn* message was output to the system messages. If a system message was output, take appropriate action. If you cannot identify the cause, acquire all the Management log files and Cluster log files, and then inform maintenance personnel. |
| 68 | Another user might be performing a cluster or resource group operation. Check the status of the cluster, node, and resource group, and then try again once the status allows execution. If an error occurs again, acquire all of the Management log files and contact maintenance personnel. |
| 69 | An attempt to start the resource group failed because the NFS service of the node that is the move destination of the resource group is not running. Start the NFS service of the node that is the move destination of the resource group, and then try again. If an error occurs again, acquire all of the Management log files and contact maintenance personnel. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | An internal error occurred. Acquire all the Management log files and inform maintenance personnel. |

## Example

### To change the execution node of the resource group `nodennc2`:

```
$ sudo enas_rgmove nodennc2
```

### 6.2.48 enas_rgstart (Start a resource group)

#### Synopsis

```
enas_rgstart [--] resource-group-name
enas_rgstart -h
```

#### Description

Starts a specified resource group.

You can execute this command when the status of the cluster, nodes, and resource groups is as follows:

- `ACTIVE` is displayed in `Cluster status`.
- `UP` is displayed in `Node status` for the node of the resource group to be started.
- `Offline/No error` or `Online Ready/No error` is displayed in `Resource group status` for the resource group to be started.

#### Options and arguments

**`-h`**

Specify this option if you want to view the command syntax.

**`--`**

Specify this to prevent all of the character string following this option from being treated as an option. For example, if you want to specify `-h` as the resource group name, specify `-- -h`.

***resource-group-name***

Specify the name of the resource group you want to start.

#### Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| `22` | The specified resource group does not exist. Specify an existing resource group, and then try again. |
| `31` | The resource group status is not `Offline/No error` or `Online Ready/No error`. Check the resource group status, stop the resource group, and then try again. |
| `35` | A service IP address is not set for the specified resource group. Set one or more service IP addresses for the specified resource group. |
| `65` | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops |

| | |
|---|---|
| | during processing, wait about 15 minutes or boot the stopped node. |
| 66 | The processing of the failover function has failed. If this message is displayed when performing a manual failover, make sure that the failover-destination node has started. In other cases, check (in all nodes in the cluster) whether a KAQG7*nnnn* message was output to the system messages. If a system message was output, take appropriate action. If you cannot identify the cause, acquire all the Management log files and Cluster log files, and then inform maintenance personnel. |
| 68 | Another user might be performing a cluster or resource group operation. Check the status of the cluster, node, and resource group, and then try again once the status allows execution. If an error occurs again, acquire all of the Management log files and contact maintenance personnel. |
| 69 | An attempt to start the resource group failed because the NFS service is not running. Start the NFS service of the node where an attempt was made to start the resource group, and then try again. If an error occurs again, acquire all of the Management log files and contact maintenance personnel. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | An internal error occurred. Acquire all the Management log files and inform maintenance personnel. |

## Example

### To start the resource group `nodennc2`:

```
$ sudo enas_rgstart nodennc2
```

### 6.2.49 enas_rgstatus (Display resource group status)

#### Synopsis

```
enas_rgstatus [-c] [--] [resource-group-name]
enas_rgstatus -h
```

#### Description

This command displays the status of a specified resource group.

#### Options and arguments

**-c**

Specify this option if you want to display resource group status information separated with colons (:). When the -c option is specified, any colon (:) contained in the resource group names is replaced with a number sign (#).

**-h**

Specify this if you want to output the command syntax to the standard error output.

**--**

Specify this to prevent all of the character string following this option from being treated as an option. For example, if you want to specify -h as the resource group name, specify -- -h.

***resource-group-name***

Specify this argument to view the status of a particular resource group.

#### Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.39 Information displayed when executing the enas_rgstatus command**

| Item | Description | |
|---|---|---|
| --Resource Group Status-- | Status of the resource group is displayed.<br>If you do not specify a resource group, the command displays the status of the resource group belonging to the node you are logged in to, and the status of the resource group belonging to the other node in the cluster, in that order. | |
| Resource group | Name of a resource group is displayed. | |
| Resource group status | Status and error information about a resource group, displayed in the following format:<br>*resource-group-status/error-information* | |
| | *resource-group-status* | Online Ready<br>The resource group cannot start because the |

| | | |
|---|---|---|
| | | cluster is inactive, or an error was detected when the cluster was stopping.<br>`Initializing`<br>The resource group is initializing.<br>`Discovery (exclusivity)`<br>Online processing is being performed for the resource group, before operations begin.<br>`Online Pending`<br>The resource group is starting.<br>`Online`<br>The resource group is active.<br>`Online Maintenance`<br>Automatic failover is impossible because monitoring is disabled.<br>`Offline Pending`<br>The resource group is stopping.<br>`Offline`<br>The resource group is stopped.<br>`Internal Error`<br>An internal error was detected. Contact the maintenance personnel. |
| | *error-information* | `No error`<br>No errors occurred.<br>`Internal error - not recoverable`<br>An unrecoverable internal error occurred. Contact the maintenance personnel.<br>`Monitor activity unknown`<br>An error occurred during monitoring or while monitoring was being disabled. If you retry operation and the error persists, perform a forced stop and fix the problem.<br>`No available nodes` or `No available nodes in failure domain after monitor failure`<br>An error occurred, but a failover could not be performed because it is already in a failover status. Perform a forced stop and remove the error that caused failover.<br>`Node not available (exclusivity)`<br>Failover is impossible because the `Node status` of the alternate node is not `ACTIVE`. Perform a forced stop and start the alternate node. If you cannot start the alternate node, perform a forced stop for the alternate node and fix the problem.<br>`Node unknown`<br>The resource group cannot be started because the `Node status` of the node is `UNKNOWN`. Perform a forced stop and start the node whose resource group you want to start. If you cannot start the node, perform a |

| | | |
|---|---|---|
| | | forced stop for the node and fix the problem.<br>`Split resource group (exclusivity)`<br>A duplicate resource group is active in the cluster. Perform a forced stop for the cluster, and then ask maintenance personnel to shut down and restart the NAS OS of the NAS Unit in the cluster.<br>`srmd executable error`<br>An error occurred during start or stop processing. Perform a forced stop and fix the problem. |
| `Running node` | Name of the node on which the resource group is running is displayed. | |

### Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| `22` | The specified resource group does not exist. Specify an existing resource group, and then try again. |
| `65` | Another user is exclusively using a resource of the status display processing, or an exclusively used node has stopped. Wait a while, and then retry. If a processing node stops, wait about 15 minutes or boot the stopped node. |
| `66` | The processing of the failover function has failed. If this message is displayed when performing a manual failover, make sure that the failover-destination node has started. In other cases, check (in all nodes in the cluster) whether a KAQG7*nnnn* message was output to the system messages. If a system message was output, take appropriate action. If you cannot identify the cause, acquire all the Management log files and Cluster log files, and then inform maintenance personnel. |
| `68` | Another user might be performing a cluster or resource group operation. Check the status of the cluster, node, and resource group, and then try again once the status allows execution. If an error occurs again, acquire all of the Management log files and contact maintenance personnel. |
| `70` | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| `97` | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| `99` | An internal error occurred. Acquire all the Management log files and inform maintenance personnel. |

### Examples

#### To display the statuses of resource groups on both nodes with specifying the `-c` option:

```
$ sudo enas_rgstatus -c
nodennc2:Online/No error: nodennc2:nodennc0:Online/No error:nodennc0
```

**To display the statuses of resource groups on both nodes without specifying the `-c` option:**

```
$ sudo enas_rgstatus


--Resource Group Status--
Resource group name   : nodennc2
Resource group status  : Online/No error
Running node       : nodennc2

Resource group name   : nodennc0
Resource group status  : Online/No error
Running node       : nodennc0
```

**To display the status of the resource group `nodennc2` by specifying the `-c` option:**

```
$ sudo enas_rgstatus -c nodennc2
nodennc2:Online/No error:nodennc2
```

**To display the status of the resource group `nodennc2` without specifying the `-c` option:**

```
$ sudo enas_rgstatus nodennc2


--Resource Group Status--
Resource group name  : nodennc2
Resource group status : Online/No error
Running node     : nodennc2
```

### 6.2.50 enas_rgstop (Stop a resource group)

#### Synopsis

```
enas_rgstop [-f] [--] resource-group-name
enas_rgstop -h
```

#### Description

Stops services such as NFS shares and CIFS shares provided by a resource group.

You can execute this command when the status of the resource group is `Online/No error`, `Online Ready/No error`, or `Online Maintenance/No error`.

#### Options and arguments

**`-f`**

Specify this option if you want to forcibly stop the specified resource group. If processing is discontinued due to an error during startup or stopping of a cluster, node, or resource group, you can forcibly stop the affected resource group by specifying this option.

**`-h`**

Specify this option if you want to view the command syntax.

**`--`**

Specify this to prevent all of the character string following this option from being treated as an option. For example, if you want to specify `-h` as the resource group name, specify `-- -h`.

***resource-group-name***

Specify the name of the resource group you want to stop or forcibly stop.

#### Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | ▪ If a syntax error occurs, check the format of the command, and then retry.<br>▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter. |
| `22` | The specified resource group does not exist. Specify an existing resource group, and then try again. |
| `30` | The resource group status is not `Online/No error`, `Online Ready/No error`, or `Online Maintenance/No error`. Check the resource group status, start the resource group, and then try again. |
| `65` | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |

| | |
|---|---|
| 66 | The processing of the failover function has failed. If this message is displayed when performing a manual failover, make sure that the failover-destination node has started. In other cases, check (in all nodes in the cluster) whether a KAQG7*nnnn* message was output to the system messages. If a system message was output, take appropriate action. If you cannot identify the cause, acquire all the Management log files and Cluster log files, and then inform maintenance personnel. |
| 68 | Another user might be performing a cluster or resource group operation. Check the status of the cluster, node, and resource group, and then try again once the status allows execution. If an error occurs again, acquire all of the Management log files and contact maintenance personnel. |
| 70 | ▪ The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*.<br>▪ The command cannot be used because a cluster configuration is not defined. Define the cluster configuration first. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | An internal error occurred. Acquire all the Management log files and inform maintenance personnel. |

## Examples

### To stop the resource group `nodennc2`:

```
$ sudo enas_rgstop node-1e
```

### To forcibly stop the resource group `nodennc2`:

```
$ sudo enas_rgstop -f nodennc2
```

### 6.2.51 enas_rmfile (Delete a specified file)

#### Synopsis

```
enas_rmfile [--] file-name
enas_rmfile -h
```

#### Description

Deletes a file stored in the home directory for the SSH account (/home/nasroot/).

You can use this command to delete the file you mistakenly transferred to the /home/nasroot directory when registering an SSH public key. This command cannot delete files in other directories.

#### Options and arguments

**-h**

Specify this option if you want to view the command syntax.

**--**

Specify this to prevent all of the character string following this option from being treated as an option. For example, if you want to specify a file named -h, specify -- -h.

***file-name***

Specify the name of the public key file you want to delete from the home directory for the SSH account (/home/nasroot/).

#### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter.<br>▪ If a syntax error occurs, check the format of the command, and then retry. |
| 5 | A character that cannot be used for the public key file is entered. Enter a valid name for the public key file, and then try again. |
| 13 | The specified file does not exist in the home directory. Confirm whether the specified file exists in the home directory. |
| 14 | The specified file cannot be deleted because it is a directory. |
| 16 | The specified file cannot be deleted because it is a system file. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 95 | The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*. |

| | |
|---|---|
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | The command execution with the root permission failed. Acquire all the Management log files, and then inform maintenance personnel. |

## Example

**To delete the file `ssh-key-nasroot.pub`:**

```
$ sudo enas_rmfile ssh-key-nasroot.pub
```

### 6.2.52 enas_sshkeyadd (Register a public key)

#### Synopsis

```
enas_sshkeyadd [-1|-2] -c comment public-key
enas_sshkeyadd -h
```

#### Description

Registers a public key for an SSH account.

Register the public key on both nodes so that the settings are the same in the cluster.

When registration completes successfully, the specified public key file is deleted from the home directory for the SSH account.

#### Options and arguments

**-1|-2**

Specify the version of the SSH protocol. If you omit this option, version 2 is applied.

**-c** ***comment***

Specify a comment for a public key by using a maximum of 32 characters. Note that comments should not be duplicated within the same protocol. Any comment string must be written in alphanumeric characters and hyphens (-). You cannot set a space at the beginning or end of the comment.

**-h**

Specify this option if you want to view the command syntax.

***public-key***

Specify the name of the public key file you want to register. To register a public key file, its file name must meet the following conditions:

- The maximum number of characters that can be used for the name of the public key file is 256.
- The characters that can be used for the name of the public key file are alphabetic characters, exclamation marks (!), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses (), right parentheses (), plus signs (+), commas (,), hyphens (-), periods (.), semicolons (;), equal signs (=), at marks (@), left square brackets ([), right square brackets (]), carets (^), underscores (_), grave accent (`), left curly brackets ({), right curly brackets (}), and swung dashes (~).You can also specify spaces, but not at the beginning or end of the character string.
- The following names cannot be used for the public key file name:
  - A name consisting of only the character 0
  - A name starting with the character -

– A name already used for a directory or file that exists in the home directory for the SSH account (`/home/nasroot`)

### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter.<br>▪ If a syntax error occurs, check the format of the command, and then retry. |
| 3 | The length of the specified parameter is invalid. Check the command format, specify a valid parameter value, and then try again. |
| 4 | A character that cannot be used for the comment is entered. Enter a valid comment, and then try again. |
| 5 | A character that cannot be used for the public key file is entered. Enter a valid name for the public key file, and then try again. |
| 6 | A space cannot be specified at the beginning or end of the comment. Enter a valid comment, and then try again. |
| 7 | A space cannot be specified at the beginning or end of the public key file. Enter a valid name for the public key file, and then try again. |
| 8 | 0 cannot be specified for the name of the public key file. Enter a valid name for the public key file, and then try again. |
| 9 | The specified comment for a public key is inappropriate. The same comment cannot be assigned to each key with the same SSH protocol. Assign a differently comment to each key. |
| 10 | An invalid public key file is specified. The specified file does not exist or the file is empty. Enter the name of a valid public key file and retry the operation. |
| 11 | The number of public keys with the same SSH protocol has already reached the maximum number (128). Delete an unnecessary public key with the same SSH protocol, and then retry. |
| 17 | The size of the specified file exceeds 1,000,000 bytes. |
| 23 | The specified file cannot be specified as a public key file because the specified file is a system file. Specify the name of a valid public key file, and then retry the operation. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 66 | An attempt to add the public key failed. Retry execution. Acquire all the Management log files if you still cannot execute the operation, and inform maintenance personnel. |
| 68 | An attempt to open the system file failed. A problem may exist in the processing of the NAS OS LU or the system file. Check the settings and whether or not a problem exists on the NAS OS LU. Acquire all the Management log files if there is no problem, and inform maintenance personnel. |
| 95 | The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | The command execution with the root permission failed. Acquire all the Management log files, and then inform maintenance personnel. |

### Example

**To register the file `ssh-key-nasroot.pub` with a `ssh key` comment:**

```
$ sudo enas_sshkeyadd -2 -c "ssh key" ssh-key-nasroot.pub
```

### 6.2.53 enas_sshkeydel (Delete a public key)

#### Synopsis

```
enas_sshkeydel [-1|-2] -c comment
enas_sshkeydel -h
```

#### Description

Deletes a public key.

Delete the target public key from both nodes to have the same settings in the cluster.

If you (system administrator) execute this command to delete the public key that you are currently using, you will not be able to log in with that key again. If you mistakenly delete all public keys, register a public key again via the NAS Manager GUI.

#### Options and arguments

**-1|-2**

Specify the version of the SSH protocol for the public key you want to delete. If you omit this option, version 2 is applied.

-1

Specify this when the version of the SSH protocol for the public key you want to delete is 1.

-2

Specify this when the version of the SSH protocol for the public key you want to delete is 2.

**-c *comment***

Specify a comment for the public key file.

**-h**

Specify this option if you want to view the command syntax.

#### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter.<br>▪ If a syntax error occurs, check the format of the command, and then retry. |
| 3 | The length of the specified parameter is invalid. Check the command format, specify a valid parameter value, and then try again. |
| 4 | A character that cannot be used for the comment is entered. Enter a valid comment, and then try again. |

| | |
|---|---|
| 6 | A space cannot be specified at the beginning or end of the comment. Enter a valid comment, and then try again. |
| 12 | An SSH public key does not exist for the specified comment. Confirm whether the specified comment exists in the specified SSH protocol, and then try again. |
| 15 | A problem may exist in the processing of the NAS OS LU or the system file. Check the settings and whether or not a problem exists on the NAS OS LU. Acquire all the Management log files if there is no problem, and inform maintenance personnel. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 67 | An attempt to delete the public key failed. A problem may have occurred during processing of the system file or the deletion of the public key. Retry execution. Acquire all the Management log files if you still cannot execute the operation, and inform maintenance personnel. |
| 68 | An attempt to open the system file failed. A problem may exist in the processing of the NAS OS LU or the system file. Check the settings and whether or not a problem exists on the NAS OS LU. Acquire all the Management log files if there is no problem, and inform maintenance personnel. |
| 95 | The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | The command execution with the root permission failed. Acquire all the Management log files, and then inform maintenance personnel. |

## Example

### To delete a public key, which was registered with a `nasroot-key` comment:

```
$ sudo enas_sshkeydel -c nasroot-key
```

## 6.2.54 enas_sshkeylist (List public key information)

### Synopsis

```
enas_sshkeylist
enas_sshkeylist -h
```

### Description

Lists information about registered public keys.

### Options and arguments

**-h**

Specify this option if you want to view the command syntax.

### Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.40 Information displayed when executing the enas_sshkeylist command**

| Item | Description |
|---|---|
| User | Displayed nasroot. |
| Ver. | Displays the SSH protocol version for the public key.<br>SSH1<br>The SSH protocol is version 1.<br>SSH2<br>The SSH protocol is version 2. |
| Comment | Displays the comment set for the public key. |

### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry specifying a suitable parameter.<br>▪ If a syntax error occurs, check the format of the command, and then retry. |
| 15 | A problem may exist in the processing of the NAS OS LU or the system file. Check the settings and whether or not a problem exists on the NAS OS LU. Acquire all the Management log files if there is no problem, and inform maintenance personnel. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 68 | An attempt to open the system file failed. A problem may exist in the processing of the NAS OS LU or the system file. Check the settings and whether or not a problem exists on the NAS OS LU. Acquire all the Management log files if there is no problem, and inform maintenance personnel. |

| | |
|---|---|
| 95 | The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | The command execution with the root permission failed. Acquire all the Management log files, and then inform maintenance personnel. |

## Example

### To reference the list of information for the registered public key:

```
$ sudo enas_sshkeylist
User     Ver.    Comment
nasroot    SSH1    nasroot-key
nasroot    SSH1    ssh1-050802
nasroot    SSH1    ssh1-admin
nasroot    SSH1    ssh1-nasroot2
nasroot    SSH1    ssh1-admin3
nasroot    SSH2    ssh2-nasroot1
nasroot    SSH2    ssh2-admin3
nasroot    SSH2    ssh2-050817
```

### 6.2.55 enas_traceroute (Check path leading to specified IP address)

- **Synopsis**

  enas_traceroute [-d] [-F] [-I] [-r] [-n] [-v] [-x]
  [-g gateway[,gateway]...] [-i iface] [-f first-ttl] [-m max_ttl] [-p port] [-q nqueries] [-s src-addr] [-t tos] [-w waittime] host

- **Description**

  Checks the path that leads to the specified IP address. The displayed contents are the same as that displayed by the `traceroute` command.

  The output information is added to the beginning of the log file. When the log file exceeds 1 MB, information equivalent to the amount by which the maximum size was exceeded is deleted from the end of the log file. The packet dump file is also output as a log file at the same time. You can obtain the log file by downloading All the log data can be downloaded and obtained from the **List of RAS Information** (Batch-download) window. For details on downloading all log data, see 4.13.10.

***Notes:***

- Multiple processes cannot use the enas_traceroute command concurrently. If the enas_traceroute command is used concurrently by multiple processes, an exclusive control error occurs and failed to lock is displayed. If you want to use the enas_traceroute command, use the command after making sure that the process executing the enas_traceroute command has ended. If no process is executing the enas_traceroute command but the exclusive control error occurs, use the enas_eraselog command and then use the enas_traceroute command.
- There are cases in which the standard output is buffered and command output might not appear immediately. If command processing does not complete within 30 seconds, a timeout occurs and processing is canceled. If a timeout occurs, re-execute the command with the `-n` option specified.

- **Arguments and Options**

**Table 6.41 enas_traceroute Arguments and Options**

| Item | Use |
|---|---|
| -d | Specify to use the command in debug mode. |
| -F | Specify to prohibit IP-packet fragmentations. |
| -I | Specify to use ICMP Echo Request. If you omit this option, UDP packets are used. |
| -r | Specify to ignore the routing table and send packets directly to the specified host. |
| -n | Specify to display only the IP addresses without performing name resolution. |
| -v | Specify to use this command in a detailed-display mode. |
| -x | Specify to estimate ICMP CheckSum. |
| -g gateway [,gateway]... | Specify the address of the gateway (router) to be passed through. The maximum specifiable number of addresses is 8. |
| -i iface | Specify to use the specified interface (network card name) to use this command. |

| Item | Use |
|---|---|
| -f first-ttl | Specify the initial value for TTL (Time To Live: time that indicates how long a packet should be allowed to exist) to be used. From the hop count (TTL) specified in this option, the network information is displayed. |
| -m max_ttl | Specify the maximum value of TTL (Time To Live: time that indicates how long a packet should be allowed to exist) to be used. The network information up to the hop count (TTL) specified in this option is displayed. |
| -p port | Specify to set the port number for a UDP packet to be used. Specify this only when a UDP packet is used. |
| -q nqueries | Specify the retry count for one gateway. If you omit this option, this option is set to 3. |
| -s src-addr | Use the command from the specified IP address. Specify the source address. |
| -t tos | Specify to set the packet TOS (Type Of Service: service type). |
| -w waittime | Specify the timeout value (in units of seconds). If you omit this option, this option is set to 5. |
| host | Specify the target host name or IP address. |

- **Return Values**

## Return values

| | |
|---|---|
| 0 | The command terminated normally. |
| 1 | ▪ The timeout period is set to 31 seconds or more for the `-w` option. Set it to 30 seconds or less, and then re-execute.<br>▪ The specified option is invalid. Specify a valid option.<br>▪ An internal error occurred. Retry execution. |

## Example

### To display the path that leads to the host `raid01` by using only the IP address:

```
$ sudo enas_traceroute -n raid01
traceroute to raid01 (10.208.151.100), 30 hops max, 38 byte packets
 1 10.208.151.100 0.683 ms 0.202 ms 0.123 ms
```

### 6.2.56 enas_umidget (Check IDs and names mapped using RIDs)

#### Synopsis

```
enas_umidget -u {user-name|user-ID}
enas_umidget -g {group-name|group-ID}
enas_umidget -s {user-name|group-name|SID}
enas_umidget -r {user-name|group-name}
enas_umidget -h
```

#### Description

Checks the following items when you use user mapping using RIDs:

- User IDs and group IDs assigned to user names and group names
- SIDs and RIDs assigned to user names and group names
- User names or group names associated with user IDs, group IDs, and SIDs

#### Options and arguments

**-g {*group-name*|*group-ID*}**

Specify this to check the group ID assigned to a group name, or to check the group name associated with the group ID.

**-h**

Specify this option if you want to view the command syntax.

**-r {*user-name*|*group-name*}**

Specify this to check the RID assigned to a user name or group name.

A message appears if the RID for the specified user name or group name is outside the range of user IDs and group IDs set for the domain.

**-s {*user-name*|*group-name*|*SID*}**

Specify this to check the SID assigned to a user name or group name, or to check the user name or group name associated with the SID.

**-u {*user-name*|*user-ID*}**

Specify this to check the user ID assigned to a user name, or to check the user name associated with the user ID.

#### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A syntax error exists in the specified parameter. Specify valid syntax.<br>▪ There are too many or too few parameters. Check the format of the command, and retry |

| | |
|---|---|
| | specifying a suitable parameter.<br>▪ If a syntax error occurs, check the format of the command, and then retry. |
| 24 | The specified CIFS service's authentication mode was neither NT domain authentication nor Active Directory authentication. Set the CIFS service's authentication mode as either NT domain authentication or Active Directory authentication, and then try again. |
| 25 | The CIFS service settings specify user mapping that does not use RIDs. Specify that the user mapping of the CIFS service is to use RIDs, and then try again. |
| 26 | The CIFS service has not started. Start or restart the CIFS service. |
| 27 | An account that is not registered in the authentication server was specified, or communication with the authentication server was not possible. Check whether there is any error in the specified account, and/or make sure the authentication server is correctly connected, and then try again. |
| 28 | The ID assigned to the specified user name or group name is outside the range of UIDs or GIDs set for the domain (in user mapping using RIDs). Revise the range of UIDs or GIDs set for the domain (in user mapping using RIDs), and/or make sure that the specified name or group name is correct, and then try again. |
| 29 | The specified ID is outside the range of the user IDs or group IDs set for the domain (in user mapping using RIDs). Make sure the specified ID is correct, and then try again. |
| 65 | Some of the resources to be used for processing are being used exclusively by another user, or the node being used exclusively has stopped. Wait a while, and then execute again. If the node stops during processing, wait about 15 minutes or boot the stopped node. |
| 68 | An attempt to open the system file failed. A problem may exist in the processing of the NAS OS LU or the system file. Check the settings and whether or not a problem exists on the NAS OS LU. Acquire all the Management log files if there is no problem, and inform maintenance personnel. |
| 95 | The license of NAS Manager is not set. For details on license setup, see the manual *Storage Navigator Modular User's Guide*. |
| 97 | An error occurred in the NAS Cluster Management LU or the NAS Cluster Management LU is blocked. Inform maintenance personnel. |
| 99 | An error occurred in the shared processing of commands. Acquire all the Management log files and contact maintenance personnel. |

## Examples

### To check the user ID assigned to user `User1`:

```
$ sudo enas_umidget -u "DOMAIN001\User1"
100032
```

### To check the group name associated with group ID `100031`:

```
$ sudo enas_umidget -g 100031
DOMAIN001\Group1
```

### To check the SID assigned to user `User1`:

```
$ sudo enas_umidget -s "Domain001\User1"
S-1-5-333-32
```

### To check the group names associated with SID `S-1-5-333-31`:

```
$ sudo enas_umidget -s S-1-5-333-31
DOMAIN001\Group1
```

**To check the RID assigned to user `User1`:**

```
$ sudo enas_umidget -r "DOMAIN001\User1"
32
```

**To check the RID assigned to user `User2` (message displayed because the RID is out of the range):**

```
$ sudo enas_umidget -r "DOMAIN001\User2"
1000 (The user is outside the range for user mapping using RIDs.)
```

### 6.2.57 stquota (Display the quota information set for a directory)

#### Synopsis

```
stquota [-c] [-w] file-system-name
stquota [-c] [-u] [-w] file-system-name user...
stquota [-c] -g [-w] file-system-name group...
stquota -d [-c] file-system-name
stquota -t [-c] [-u|-g] file-system-name
stquota -h
```

#### Description

This command displays the information about the quota (subtree quota) set for a directory. We recommend that you specify the service IP address when you log in if you want to use this command.

When a specific user or group is specified, the command displays the user or group quota information set for the directory.

#### Options and arguments

**-c**

Specify this option to display the quota information items set for the directory in a colon-separated format.

When this option is specified, the name and ID are displayed for user and group information, the values for block usage are displayed in kilobytes, and the grace period is displayed in seconds.

**-d**

Specify this option to display the default quota set for the directory.

**-g**

Specify this option to display the group quota information set for the directory.

**-h**

Specify this option if you want to view the command syntax.

**-t**

Specify this option to view the grace period after the soft limit is exceeded.

**-u**

Specify this option to display the user quota information set for the directory.

**-w**

Specify this option to display the quota information for the directories, users, or groups that have exceeded their soft limit or that have reached their hard limits.

***file-system-name***

Specify the name of the file system.

***user...***

When you want to display the quota information for one or more specific users, specify their names or IDs.

You can specify any of the following users by the user name:

- Users registered by NAS Manager (user IDs: 97 and 104 to 2,147,483,147)
- Users registered in the NIS server or LDAP server for user authentication (other than groups whose group ID is 0)
- Users registered by user mapping

When you specify a user ID, specify a valid value within the range 0 to 2,147,483,147.

When specifying multiple user names or user IDs, separate them with space. Multiple user names and user IDs can coexist.

***group...***

When you want to display the quota information for one or more specific groups, specify their names or IDs.

You can specify any of the following groups by group name:

- Groups registered by NAS Manager (group IDs: 97 and 104 to 2,147,483,147)
- Groups registered in the NIS server or LDAP server for user authentication (other than groups whose group ID is 0)
- Groups registered by user mapping

When you specify a group ID, specify a valid value within the range 0 to 2,147,483,147.

When specifying multiple group names or group IDs, separate them with space. Multiple group names and group IDs can coexist.

## Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.42 Info Displayed When Executing stquota Command (quota of directory, user, or group)**

| Item | Description |
|---|---|
| `Report for subtree user/group quotas on file system`[#1] | `The file system name is displayed.` |
| `User` or `Group`[#2] | The user or group names are displayed.<br>When user or group IDs are displayed instead of names, a number sign (#) is prefixed to the IDs. |
| `Directory` | The names of directories for which quotas have been set are displayed.<br>The directory names are followed by two symbols, each of which can be a plus sign (+) or a minus sign (-). The first symbol indicates block usage and the second symbol indicates i-node usage.<br>Plus sign (+)<br>The block usage or i-node usage has exceeded the soft limit or has reached the hard limit.<br>Minus sign (-)<br>The block usage or i-node usage has neither exceeded the soft limit nor reached the hard limit. |
| `Block limits` | Block usage is displayed.<br>`Used`<br>Block space used.<br>`Soft`<br>Soft limit for block usage.<br>`Hard`<br>Hard limit for block usage.<br>`Grace`<br>Remaining grace time until files can no longer be created or updated after the block usage exceeds the soft limit. Displayed in one of the following formats:<br>*n* `days`<br>The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.<br>*hh*`:`*mm*<br>The remaining grace time is less than 24 hours. For example, `10:00` appears if there are ten hours remaining.<br>`over`<br>Either the grace period has expired or block usage has reached the hard limit. `over` is displayed. |
| `i-node limits` | i-node usage is displayed.<br>`Used`<br>Number of i-nodes used.<br>`Soft`<br>Soft limit for i-node usage.<br>`Hard`<br>Hard limit for i-node usage.<br>`Grace`<br>Remaining grace time until files can no longer be created after the i-node usage exceeds the soft limit. Displayed in one of the following formats: |

| | |
|---|---|
| | *n* days<br>The remaining grace time is 24 hours or longer. For example, 1 days appears if there are 24 hours or more, but less than 48 hours remaining.<br>*hh*:*mm*<br>The remaining grace time is less than 24 hours. For example, 10:00 appears if there are ten hours remaining.<br>over<br>Either the grace period has expired or i-node usage has reached the hard limit. |

***Note:***

If a directory name has 10 or more characters, the symbols that indicate whether limits have been exceeded, the block usage value, and the i-node usage value are displayed on the next line.

#1:

For the directory quota information, Report for subtree quotas on file system will appear instead.

#2:

For the directory quota information, this item will not appear.

**Table 6.43 Info Displayed When Executing stquota Command (default quota)**

| Item | Description |
|---|---|
| Report for subtree user quotas on file system | The file system name is displayed. |
| Directory | The names of directories for which quotas have been set are displayed. |
| Default block limits | The soft and hard limits for block usage that are set as default quotas are displayed.<br>Soft<br>Soft limit for block usage.<br>Hard<br>Hard limit for block usage. |
| Default i-node limits | The soft and hard limits values for i-node usage that is set as default quotas are displayed.<br>Soft<br>Soft limit for i-node usage.<br>Hard<br>Hard limit for i-node usage. |

**Table 6.44 Information Displayed When Executing stquota Command (grace period)**

| Item | Description |
|---|---|
| Report for subtree user/group quotas on file system | The file system name is displayed. |

| | |
|---|---|
| Directory | The names of directories for which quotas have been set are displayed. |
| Block grace time | Displays the grace period until files can no longer be created or updated after block usage exceeds the soft limit. |
| i-node grace time | Displays the grace period until files can no longer be created after i-node usage exceeds the soft limit. |

### Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 10 | ▪ The operation cannot be performed because the target file system is mounted with the quota setting disabled. Enable the quota setting, mount the target file system, and then retry the operation.<br>▪ The specified user does not exist. Make sure the user name is correct, and then retry the operation.<br>▪ The specified group does not exist. Make sure the group name is correct, and then retry the operation.<br>▪ The specified file system is not mounted. If the file system is not mounted, mount it or specify a correct file system name, and then try again. |
| 99 | ▪ An attempt to acquire mount information has failed. There might be a problem in the processing for either the NAS OS LU or the acquisition of mount information. Check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ The specified file system is not in a normal state. Check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel. |

### Examples

#### To display the quota information set for the directories in the FS1 file system with the -c option specified:

```
$ sudo stquota -c FS1
dir01:106496:51200:153600:36000:7270:8192:10000:-
long_dirname:170917888:157286400:188743680:518400:262144:256000:307200:over
```

#### To display the quota information set for the directories in the FS1 file system with the -c option not specified:

```
$ sudo stquota FS1
*** Report for subtree quotas on file system FS1
        Block limits              i-node limits
Directory    Used  Soft  Hard Grace    Used  Soft  Hard Grace
-------------------------------------------------------------------------------
dir01   +-  104M   50M  150M 10:00    7270  8192  10000
long_dirname
     ++  163G  150G  180G 6days   262144 256000 307200  over
```

#### To display the quota information under the following conditions without the -c option specified:

- The name of the target file system is FS1.
- The target users are User1 and User2.

```
$ sudo stquota -u FS1 User1 User2
*** Report for subtree user quotas on file system FS1
*** User: User1
        Block limits            i-node limits
Directory    Used  Soft  Hard Grace    Used  Soft  Hard Grace
--------------------------------------------------------------------------------
dir01   +-  104M   50M  150M 10:00    7270  10240  20480
long_dirname
     ++  163G  150G  180G 6days   262114 256000 307200  over
*** User: User2
        Block limits            i-node limits
Directory    Used  Soft  Hard Grace    Used  Soft  Hard Grace
--------------------------------------------------------------------------------
dir01   +-  100M   20M  160M 10days     70M  110M  350M
```

**To display the default quota information set for the directories in the `FS1` file system with the `-c` option not specified:**

```
$ sudo stquota -d FS1
*** Report for subtree user quotas on file system FS1
        Default block limits  Default i-node limits
Directory        Soft  Hard  Soft  Hard
--------------------------------------------------------------------------------
dir01          50M  100G  100M  100G
dir02          15G   18G  250M  300M
```

**To display the grace periods of the quotas for directories under the following conditions with the `-c` option not specified:**

- The name of the target file system is `FS1`.
- The grace periods for users are to be displayed.

```
$ sudo stquota -t -u FS1
*** Report for subtree user quotas on file system FS1
Directory        Block grace time  i-node grace time
--------------------------------------------------------------------------------
dir01                7days        24:00
dir02               100days        24:00
dir03                3days        6days
```

### 6.2.58 stquotalist (List the user or group quota information set for a directory)

#### Synopsis

```
stquotalist [-c] [-u|-g] [-w] file-system-name/directory-name
stquotalist -h
```

#### Description

This command displays the quota (subtree quotas) information set for the specified directory for each user or group.

We recommend that you specify the service IP address when you log in if you want to use this command.

#### Options and arguments

**-c**

Specify this option to display the quota information items set for the specified directory in a colon-separated format.

When this option is specified, the name and ID are displayed for user and group information, the values for block usage are displayed in kilobytes, and the grace period is displayed in seconds.

**-g**

Specify this option to display the group quota information set for the specified directory.

**-h**

Specify this option if you want to view the command syntax.

**-u**

Specify this option to display the user quota information set for the specified directory.

**-w**

Specify this option to display the quota information for the users or groups that have exceeded their soft limit or that have reached their hard limits.

***file-system-name/directory-name***

Specify the directory for which you want to display the quota information. Specify the directory name (immediately under the mount point directory) after the file system name with a forward slash (/) placed between them. For example, to display the quota information for the `/mnt/FS1/dir01` directory, specify `FS1/dir01`.

## Displayed information

The following table lists the information displayed when you execute the command.

**Table 6.45 Information displayed when executing the stquotalist command**

| Item | Description |
|---|---|
| `Report for subtree user/group quotas on directory` | The specified directory name is displayed. |
| `User or Group` | The user or group names are displayed.<br>When user or group IDs are displayed instead of names, a number sign (#) is prefixed to the IDs.<br>Each user or group name is followed by two symbols, each of which can be a plus sign (+) or a minus sign (-). The first symbol indicates block usage and the second symbol indicates i-node usage.<br>Plus sign (+)<br>The block usage or i-node usage has exceeded the soft limit or has reached the hard limit.<br>Minus sign (-)<br>The block usage or i-node usage has neither exceeded the soft limit nor reached the hard limit. |
| `Block limits` | Block usage is displayed.<br>`Used`<br>Block space used.<br>`Soft`<br>Soft limit for block usage.<br>`Hard`<br>Hard limit for block usage.<br>`Grace`<br>Remaining grace time until files can no longer be created or updated after the block usage exceeds the soft limit. Displayed in one of the following formats:<br>*n* `days`<br>The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.<br>*hh*`:`*mm*<br>The remaining grace time is less than 24 hours. For example, `10:00` appears if there are ten hours remaining.<br>`over`<br>Either the grace period has expired or block usage has reached the hard limit. `over` is displayed. |
| `i-node limits` | i-node usage is displayed.<br>`Used`<br>Number of i-nodes used.<br>`Soft`<br>Soft limit for i-node usage.<br>`Hard`<br>Hard limit for i-node usage. |

| | |
|---|---|
| | `Grace`<br>Remaining grace time until files can no longer be created after the i-node usage exceeds the soft limit. Displayed in one of the following formats:<br>*n* `days`<br>The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.<br>*hh*`:`*mm*<br>The remaining grace time is less than 24 hours. For example, `10:00` appears if there are ten hours remaining.<br>`over`<br>Either the grace period has expired or i-node usage has reached the hard limit. |

***Note:***

If a user or group name has 10 or more characters, the symbols that indicate whether limits have been exceeded, the block usage value, and the i-node usage value are displayed on the next line.

### Return values

| | |
|---|---|
| `0` | Completed successfully. |
| `1` | The specified directory does not exist. Make sure the path of the target directory is correct, and then retry the operation. |
| `10` | The specified file system is not mounted. If the file system is not mounted, mount it or specify a correct file system name, and then try again. |
| `99` | ▪ An attempt to acquire mount information has failed. There might be a problem in the processing for either the NAS OS LU or the acquisition of mount information. Check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ The specified file system is not in a normal state. Check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel. |

### Examples

**To display the user quota information set for the `/mnt/FS1/dir01` directory with the `-c` option specified:**

```
$ sudo stquotalist -c FS1/dir01
dir01:user1:1000:106496:51200:153600:36000:7270:8192:10240:-
dir01:user2:2000:170917888:157286400:1887438680:518400:262144:256000:307200:over
```

**To display the user quota information set for the `/mnt/FS1/dir01` directory without the `-c` option specified:**

```
$ sudo stquotalist -u FS1/dir01
*** Report for subtree user quotas on directory FS1/dir01
        Block limits              i-node limits
User      Used  Soft  Hard Grace    Used  Soft  Hard Grace
--------------------------------------------------------------------------------
user1   +-  104M   50M  150M 10:00    7270  8192  10240
user2   ++  163G  150G  180G 6days   262144 256000 307200  over
```

### 6.2.59 stquotaset (Set quotas for directories)

#### Synopsis

```
stquotaset limit-options file-system-name/directory-name
stquotaset [-u] limit-options file-system-name/directory-name user...
stquotaset -g limit-options file-system-name/directory-name group...
stquotaset -d limit-options file-system-name/directory-name
stquotaset -t [-u|-g] grace-period-options file-system-name/directory-name
stquotaset -t [-u|-g] grace-period file-system-name/directory-name
stquotaset -x|-r [-q] file-system-name/directory-name
stquotaset -h
```

*limit-options*:

```
-b block-soft-limit
-B block-hard-limit
-i i-node-soft-limit
-I i-node-hard-limit
```

*grace-period-options*:

```
-b block-grace-period
-i i-node-grace-period
```

#### Description

This command sets quotas (subtree quotas) for directories immediately under the mount point directory. The command can set quotas for a maximum of 255 directories per file system.

We recommend that you specify the service IP address when you log in if you want to use this command.

The soft limit, hard limit, and grace period can be set for each directory, user, or group.

The command operates differently depending on whether the `-u` or `-g` option is specified, as described below.

When the `-u` option is specified

The command sets the soft limit, hard limit, or grace period for users.

When the `-g` option is specified

The command sets the soft limit, hard limit, or grace period for groups.

When neither the `-u` option nor the `-g` option is specified

The command sets the soft limit, hard limit, or grace period for directory.

#### Options and arguments

**`-d`**

Specify this option to set the default quota for the specified directory.

**-g**

Specify this option to set the group quota for the specified directory.

**-h**

Specify this option if you want to view the command syntax.

**-q**

Specify this option if you do not want to display the processing progress. This option is enabled only when the `-r` or `-x` option is specified.

**-r**

Specify this option to remove the quotas set for the specified directory.

The processing time varies depending on the number of directories and files residing under the specified directory.

If you execute the command with this option specified when the total number of directories and files is 100,000, it takes about 30 seconds to complete the processing. At this time, the command first displays the directory path and the string `Wait...`, and then displays one period (`.`) every time the command removes quotas for 10,000 files.

If the command executed with this option specified stops, the specified directory might contain files that have different quota information. Re-execute the command with the same specification when the command executed with this option specified has stopped.

**-t**

Specify this option to set the grace time until files can no longer be created after the block usage or i-node usage exceeds the soft limit.

**-u**

Specify this option to set the user quotas for the specified directory.

**-x**

Specify this option to apply a quota for the existing directories.

When this option is specified, the block space and the number of i-nodes used by the directories and files under the target directory will be counted as the quota usage.

The command execution time varies depending on the total number of directories and files under the specified directory. If you execute the command when the total number of directories and files is 100,000, it takes about 30 seconds to complete the processing. At this time, the command first displays the directory path and the string `Wait...`, and then displays one period (`.`) every time the command processes 10,000 files.

If the command executed with this option specified stops, the specified directory might contain files that have different quota information. Re-execute the command with the same specification when the command executed with this option specified has stopped.

### *limit-options*

Specify these options if you want to set the soft and hard limits for the specified directory. You can specify a combination of the following options:

`-b` *block-soft-limit*

Specify the soft limit for block usage (in megabytes). Specify a valid value within the range 0 to 2,097,151. Make sure that the soft limit value does not exceed the hard limit value.

The initial value is `0` (no soft limit). If you omit this argument, the current setting applies.

`-B` *block-hard-limit*

Specify the hard limit for block usage (in megabytes). Specify a valid value within the range 0 to 2,097,151.

The initial value is `0` (no hard limit). If you omit this argument, the current setting applies.

`-i` *i-node-soft-limit*

Specify the soft limit for i-node usage. Specify a valid value within the range 0 to 2,147,483,647. Make sure that the soft limit value does not exceed the hard limit value.

The initial value is `0` (no soft limit). If you omit this argument, the current setting applies.

`-I` *i-node-hard-limit*

Specify the hard limit for i-node usage. Specify a valid value within the range 0 to 2,147,483,647.

The initial value is `0` (no hard limit). If you omit this argument, the current setting applies.

### *grace-period-options*

Specify these options to set grace periods. You can specify either or both of the following options:

`-b` *block-grace-period*

Specify the grace period (number of days) until files can no longer be created or updated after block usage exceeds the soft limit. Specify a value from 1 to 9,999. The value cannot begin with 0.

The initial setting is 7 days. If you omit this argument, the current setting applies.

`-i` *i-node-grace-period*

Specify the grace period (number of days) until files can no longer be created or updated after i-node usage exceeds the soft limit. Specify a value from 1 to 9,999. The value cannot begin with 0.

The initial setting is 7 days. If you omit this argument, the current setting applies.

### *file-system-name/directory-name*

Specify the directory for which you want to set a quota. Specify the directory name (immediately under the mount point directory) after the file system name with a forward slash (/) placed between them. For example, to set a quota for the `/mnt/FS1/dir01` directory, specify `FS1/dir01`.

### *user...*

When you set a user quota, specify the name or ID of the user.

You can specify any of the following users by the user name:

- Users registered by NAS Manager (user IDs: 97 and 104 to 2,147,483,147)
- Users registered in the NIS server or LDAP server for user authentication (other than groups whose group ID is 0)
- Users registered by user mapping

When you specify a user ID, specify a valid value within the range 0 to 2,147,483,147.

When specifying multiple user names or user IDs, separate them with space. Multiple user names and user IDs can coexist.

### *group...*

When you set a group quota, specify the name or ID of the group.

You can specify any of the following groups by group name:

- Groups registered by NAS Manager (group IDs: 97 and 104 to 2,147,483,147)
- Groups registered in the NIS server or LDAP server for user authentication (other than groups whose group ID is 0)
- Groups registered by user mapping

When you specify a group ID, specify a valid value within the range 0 to 2,147,483,147.

When specifying multiple group names or group IDs, separate them with space. Multiple group names and group IDs can coexist.

### *grace-period*

Specify the number of days for the grace period to be applied to both the block usage and i-node usage. Specify a value from 1 to 9,999.

The initial setting is 7 days. If you omit this argument, the current setting applies.

## Return values

| | |
|---|---|
| 0 | Completed successfully. |
| 1 | ▪ A character other than a numerical value is entered. Enter a numerical value, and then retry the operation.<br>▪ The operation cannot be performed because the block soft (or hard) limit value exceeds the maximum. Enter a value no greater than the maximum (2,097,151) setting for a block limit value, and then retry the operation.<br>▪ The operation cannot be performed because the i-node soft (or hard) limit value exceeds the maximum. Enter a value no greater than the maximum (2,147,483,647) setting for an i-node value, and then retry the operation.<br>▪ A value outside the valid range (1-9,999) has been specified for the grace period. Specify a value of 1-9,999 for the grace period, and then retry the operation.<br>▪ A soft limit value that is larger than the hard limit value cannot be specified. Enter a soft limit value no greater than the hard limit value.<br>▪ The specified directory does not exist. Make sure the path of the target directory is correct, and then retry the operation. |
| 10 | ▪ The specified path is not a directory. Specify a directory, and then retry the operation.<br>▪ The operation cannot be performed because the target file system is mounted with the quota setting disabled. Enable the quota setting, mount the target file system, and then retry the operation.<br>▪ A quota is not set for the specified directory. Specify a directory for which a quota is set.<br>▪ The specified user does not exist. Make sure the user name is correct, and then retry the operation.<br>▪ The specified group does not exist. Make sure the group name is correct, and then retry the operation.<br>▪ A new quota cannot be set because the number of directories for which a quota has been set has reached the maximum. Please check how many directories for which a quota has been set exist in the file system. Also, if there is an unnecessary quota set for a directory, cancel that quota setting.<br>▪ The specified file system is not mounted. If the file system is not mounted, mount it or specify a correct file system name, and then try again.<br>▪ An attempt to specify the settings failed because the file system is full. Reduce the capacity used by the file system, and then try again.<br>▪ An attempt to specify the settings failed because the file system is mounted with read-only permissions. Remount the file system with read/write permissions, and then try again. |
| 99 | ▪ An attempt to acquire mount information has failed. There might be a problem in the processing for either the NAS OS LU or the acquisition of mount information. Check the NAS OS LU settings and whether an error exists on the NAS OS LU. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel.<br>▪ The specified file system is not in a normal state. Check whether an error occurred in the specified file system. If there is no problem, acquire all of the kernel logs, and then contact maintenance personnel. |

## Examples

### To set a quota for the `/mnt/FS1/dir01` directory under the following conditions:

- Set the soft limit of block usage to 10 GB and the hard limit to 12 GB.
- Set the soft limit of i-node usage to 30,000 and the hard limit to 35,000.

```
$ sudo stquotaset -b 10240 -B 12288 -i 30000 -I 35000 FS1/dir01
```

**To set user quotas for the `/mnt/FS1/dir01` directory under the following conditions:**

- The target users are `user1` and `user2`.
- Set the soft limit of block usage to 800 MB and the hard limit to 1 GB.
- Set the soft limit of i-node usage to 3,000 and the hard limit to 3,500.

```
$ sudo stquotaset -b 800 -B 1024 -i 3000 -I 3500 FS1/dir01 user1
user2
```

**To set the default quota for the `/mnt/FS1/dir01` directory under the following conditions:**

- Set the soft limit of block usage to 1 GB and the hard limit to 1.5 GB.
- Set the soft limit of i-node usage to 3,000 and the hard limit to 3,500.

```
$ sudo stquotaset -d -b 1024 -B 1536 -i 3000 -I 3500 FS1/dir01
```

**To set the quota grace periods for the `/mnt/FS1/dir01` directory under the following conditions:**

- Set the grace period for directory.
- Set the grace period for block usage to 10 days.
- Set the grace period for i-node usage to 3 weeks.

```
$ sudo stquotaset -t -b 10 -i 21 FS1/dir01
```

**The following shows a sample command execution in which quotas were applied to the existing `/mnt/FS1/dir02` directory (when there are 100,000 files):**

```
$ sudo stquotaset -x FS1/dir02
FS1/dir02: Wait ............. Success
```

# Chapter 7 Performing End User Operations

This chapter describes the NAS Manager operations that end users of a NAS Modular system perform to check the access status of a file system.

Note that only the end users registered by NAS Manager, the NIS server, or the LDAP user-authentication server can perform the operations described in this chapter.

- Overview of Operations (see section 7.1)
- Logging In and Logging Out (see section 7.2)
- Window Transitions (see section 7.3)
- Basic GUI Operations (see section 7.4)
- Viewing a List of NFS File Shares (see section 7.5)
- Viewing Quota Information (see section 7.6)
- Changing Your Password (see section 7.7)
- Editing Your User Comment (see section 7.8)

## 7.1 Overview of Operations

You can check the accessibility of data in file systems by using the NAS Manager to perform the following tasks:

- **View a list of file shares**.

  You can check which shared directories you are allowed to access.

- **View quota information**.

  You can check your own quota information and quota information for the groups to which you belong. For details, see section 7.6.

- **Change your password**.

  You can change your **Login** password. Regularly changing your password improves data security. If you are a CIFS user, the changes will also take effect for the password for CIFS user authentication. For details, see section 7.7.

- **Edit a comment**.

  You can edit the comment in your own user information. For details, see section 7.8.

***Note:*** Only users whose password is encrypted using either the DES or MD5 algorithm can perform these tasks.

## 7.2 Logging In and Logging Out

By logging in to NAS Manager from a Web browser, you can access the NAS Manager file systems. The end user quits NAS Manager by logging out of NAS Manager.

This section describes the method for logging in to and logging out from NAS Manager.

### 7.2.1 Logging In

You will use the **Login** (end user) window to log into NAS Manager.

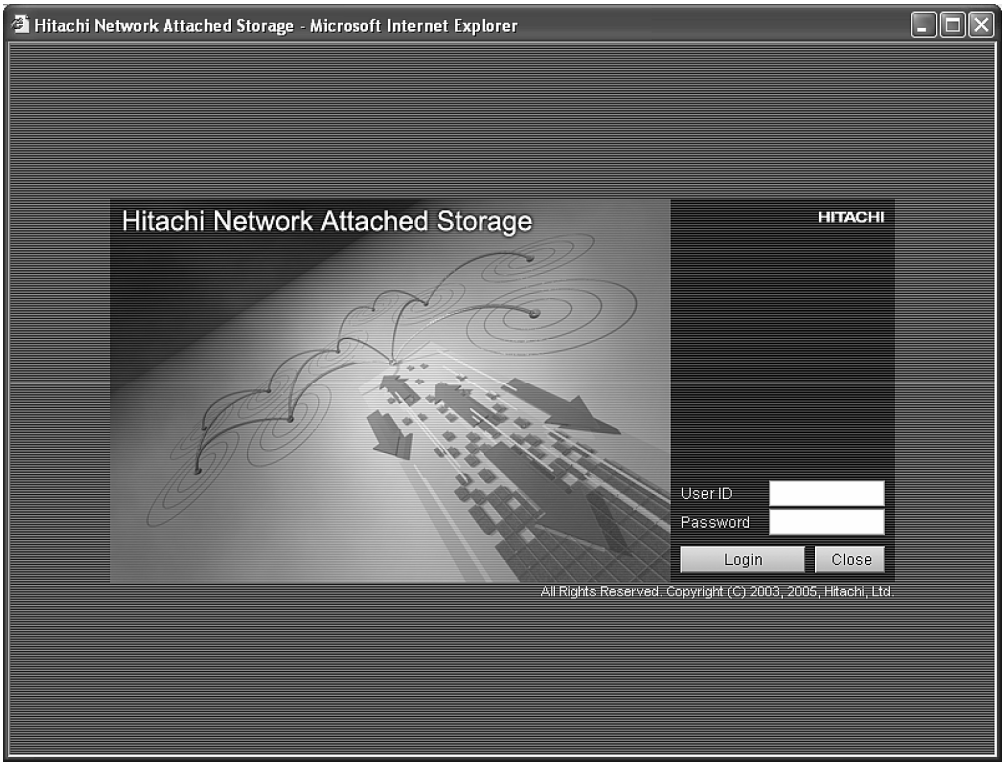



**Figure 7.1 Login (End User) Window**

To log in to NAS Manager:

1. Start your Web browser, and type the URL of the **Login** (end user) window:

   `https://`*`service-IP-address-of-the-NAS-Unit-for-connection`*`/index.cgi`

   The **Login** (end user) window displays.

2. Enter the required information as described below, and then click the **Login** button:
   - **User ID** Enter the user name of the NAS Modular system end user.
   - **Password** Enter the password of the end user.

   The **List of File Shares** (List of NFS File Shares) (end user) window displays. For details on the **List of File Shares** (List of NFS File Shares) (end user) window, see section 7.5.

### 7.2.2 Logging Out

At the end of your NAS Manager session, be sure to log out before quitting your Web browser. The logout operations will not be performed when you directly quit your Web browser.

To log out of NAS Manager, click **Close** in the menu area. Afterward, quit your Web browser.

## 7.3 Window Transitions

You can use the NAS Manager to check file system accessibility. When you log in as an end user from your Web browser to a NAS Unit configured in a cluster, the **List of File Shares** (List of NFS File Shares) (end user) window appears and you can view information about file shares.

By selecting **List of CIFS file shares** from the drop-down list, you can switch to the **List of File Shares** (List of CIFS File Shares) (end user) window instead. End users of the NAS Modular system can perform user operations such as viewing quota information, changing passwords, or editing comments from both of these windows. For details on displaying the **List of File Shares** (List of NFS File Shares) (end user) window, see section 7.5. Figure 7.2 shows the window transitions.

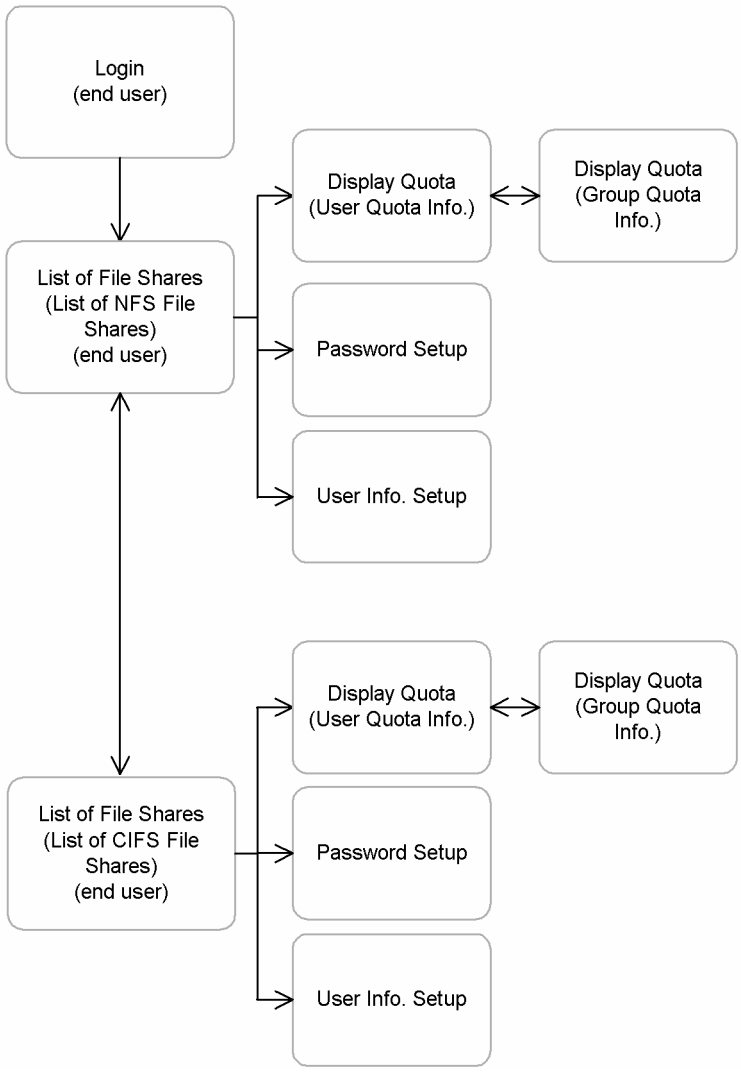



**Figure 7.2 Window Transitions for End Users**

## 7.4 Basic GUI Operations

You can use the NAS Manager to check the usage of a file system. This section describes the basic operations of the NAS Manager GUI.

***Note:*** When using a wheel mouse, do not rotate the wheel while pressing the **Shift** key. Doing so might cause the displayed window to change to another, and processing might not continue. If such an error has occurred, you must log out by clicking **Close** in the menu area, and then log in again.

If the window displayed when the error has occurred does not contain a **Close** button in the menu area, close the window by using the control menu of the web browser, and then log in again.

When using a wheel mouse, do not rotate the wheel while pressing the **Shift** key. This operation might cause the window to change to another and the running operation to end abnormally. If an error occurs when using the wheel mouse and the **Shift** key, you must log out by clicking **Close** in the menu area, and then log in again.

If **Close** is not displayed in the menu area, click the button (on the title bar) that closes the window, and then log in again.

### 7.4.1 Window Layout

Figure 7.3 provides the window layout of the NAS Manager.

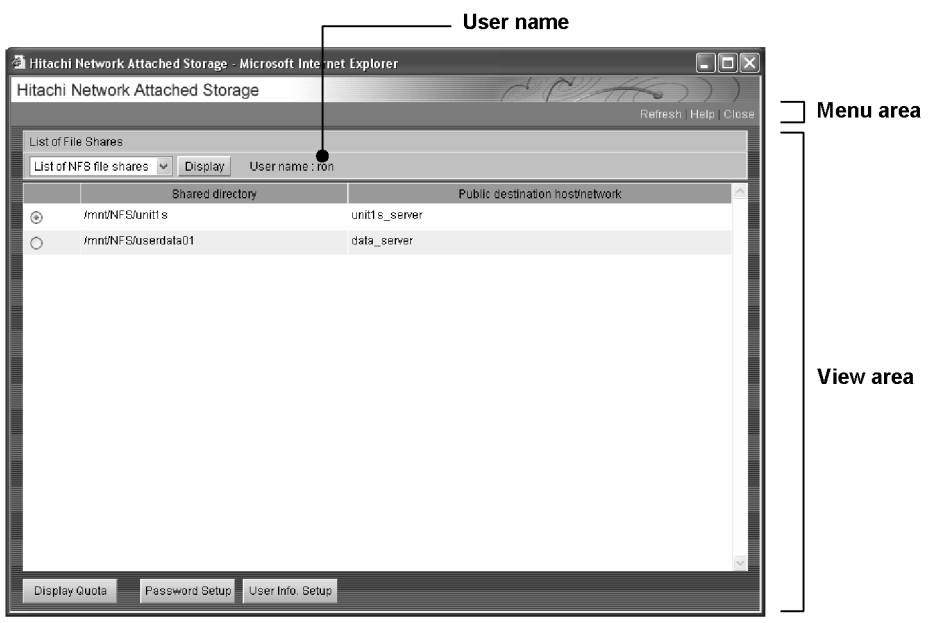



**Figure 7.3 GUI Window Layout**

The NAS Manager for end users consists of a menu area and view area. The menu area is common to all windows accessed by end users, except for message dialog boxes and the **Login** (end user) window. Table 7.1 explains how to use the components displayed in the menu area.

**Table 7.1 NAS Manager Components for End Users (Menu Area)**

| Component | Details |
|---|---|
| Refresh | Click this button to refresh the information displayed in a window used to view a list or status. Although this **Refresh** button also appears in windows used for purposes other than viewing information, clicking the button in such windows does not refresh any information. |
| Help | Click to display the HTML manual. |
| Close | Click to close the current window. |

| | |
|---|---|
| User name | Name of the logged-in user. |
| ▪ **List of File Shares** (List of NFS File Shares) (end user) window<br>▪ **List of File Shares** (List of CIFS File Shares) (end user) window | The **List of File Shares** (List of NFS File Shares) (end user) window is displayed at login. When you select **List of CIFS file shares** from the drop-down list, the **List of File Shares** (List of CIFS File Shares) (end user) window appears.<br>In these windows, you can view a list of NFS or CIFS shares. Also, from each window, an end user can display a window for viewing the end user's quota information, a window for changing the end user's own password, and a window for editing the end user's own comment. |
| ▪ **Display Quota** (User Quota Info.) window<br>▪ **Display Quota** (Group Quota Info.) window | The **Display Quota** (User Quota Info.) window opens first when you select a shared directory or a name of file share, then click the **Display Quota** button in the **List of File Shares** (List of NFS File Shares) (end user) window or in the **List of File Shares** (List of CIFS File Shares) (end user) window. When you select **Group quota info.** from the drop-down list, the **Display Quota** (Group Quota Info.) window appears.<br>In these windows, you can check the user or group quota information set for a file system. |
| **Password Setup** window | This window opens when you click the **Password Setup** button in the **List of File Shares** (List of NFS File Shares) (end user) window or **List of File Shares** (List of CIFS File Shares) (end user) window. This window allows you to change your password. |
| **User Info. Setup** window | This window opens when you click the **User Info. Setup** button in the **List of File Shares** (List of NFS File Shares) (end user) window or **List of File Shares** (List of CIFS File Shares) (end user) window. This window allows you to edit your comment. |

The following list describes the basic NAS Manager operations that you can perform:

- Refreshing information in a window used to view a list or status:

  Click **Refresh** in the menu area to refresh the information displayed in a window used to view a list or status. Although this **Refresh** button also appears in other windows, clicking the button in such windows does not refresh any information.

- Displaying the HTML manual:

  Click **Help** in the menu area to display the HTML manual.

- Logging out from NAS Manager:

  Click **Close** in the menu area to log out of NAS Manager.

### 7.4.2 Reviewing Program Usage Notes

Note the following points when you use the NAS Manager:

- To end your NAS Manager session, always log out by clicking Close in the menu area. The logout operations will not be performed if you directly quit your Web browser.
- You will be forced to log out if you do not access the program for 30 minutes or more during your **Login** session.
- If failover occurred in the NAS Unit where you are logging in, you will be forced to log out.

## 7.5 Viewing a List of NFS File Shares

In the **List of File Shares** (List of NFS File Shares) (end user) window, you can view a list of NFS file shares. Figure 7.4 shows the **List of File Shares** (List of NFS File Shares) (end user) window.

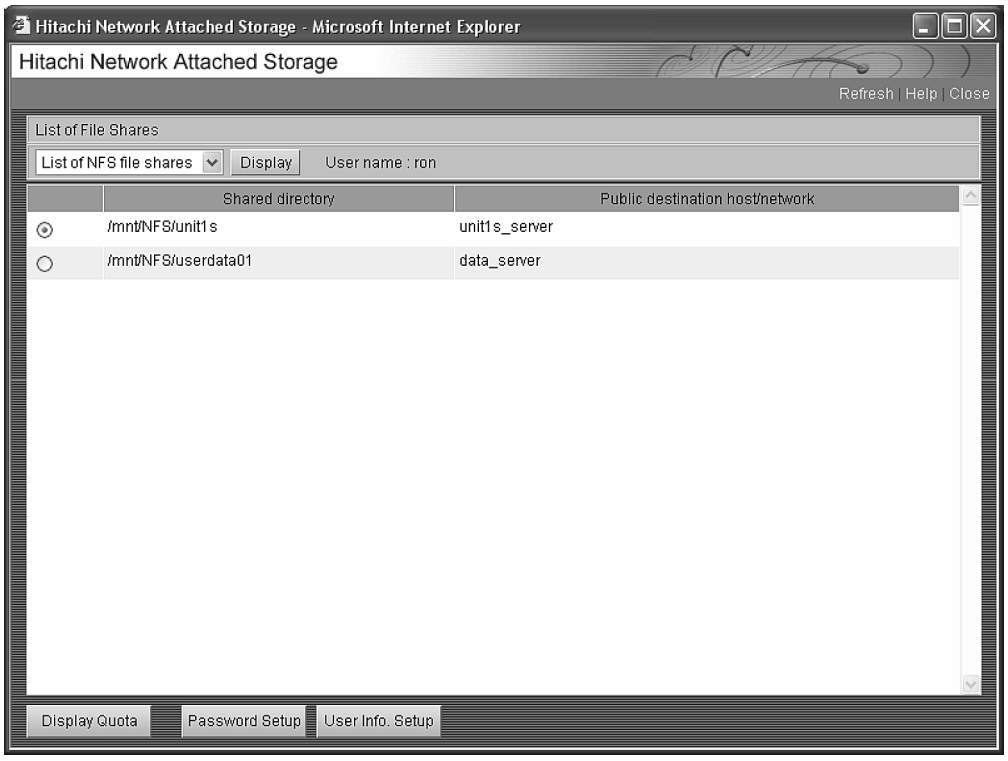



**Figure 7.4 List of File Shares (List of NFS File Shares, end user) Window**

To view a list of NFS file shares:

1. Open the **List of File Shares** window and select **List of NFS file shares** in the drop-down list.
2. Click the **Display** button. The **List of File Shares** (List of NFS File Shares) (end user) window displays.

### 7.5.1 Viewing a List of CIFS File Shares

In the **List of File Shares** (List of CIFS File Shares) (end user) window, you can view a list of CIFS file shares. Figure 7.5 shows the **List of File Shares** (List of CIFS File Shares) (end user) window.

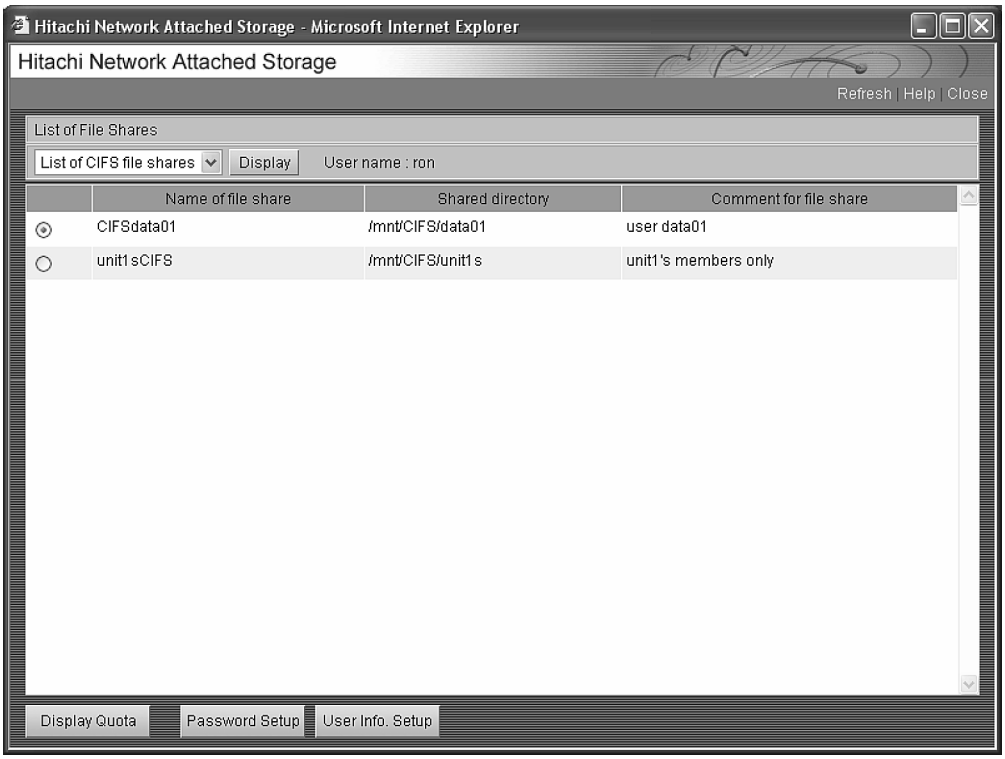



**Figure 7.5 List of File Shares (List of CIFS File Shares, end user) Window**

To view a list of CIFS file shares:

1. In the **List of File Shares** window, select **List of CIFS file shares** in the drop-down list.
2. Click the **Display** button.

   The **List of File Shares** (List of CIFS File Shares) (end user) window displays.

## 7.6 Viewing Quota Information set for file systems (end user)

Quota information includes the maximum amount of disk space available to individual users and groups, and the grace time until files can no longer be created or updated. Such information is set to prevent system disks from filling up with data.

As an end user, you can view the quota information set for a file system. When you view quota information, you can check your own quota settings and the quota information set for the groups to which you belong, as well as check the current block usage and i-node usage.

Note that the system administrator might be managing quotas for each directory immediately under the mount point (subtree quotas). For details on the quota information set for the directories, contact the system administrator.

### 7.6.1 Viewing User Quota Information (end user)

In the **Display Quota** (User Quota Info.) window, end users can view their own quota information set for a file system. Figure 7.6 shows the **Display Quota** (User Quota Info.) window.

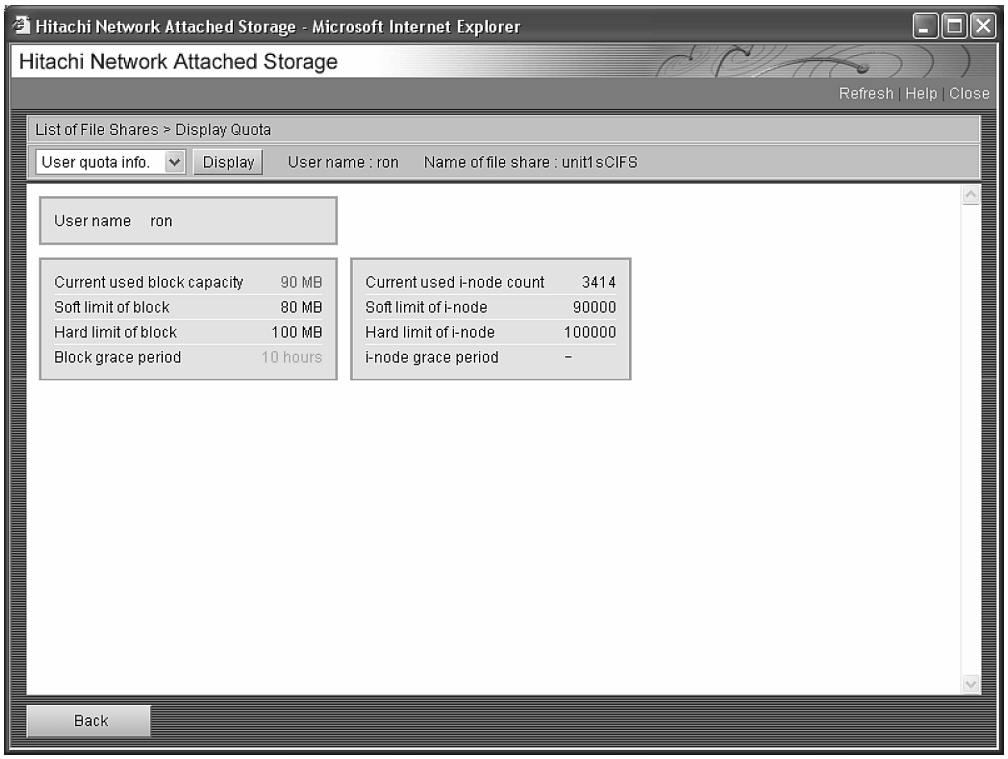



**Figure 7.6 Display Quota (User Quota Info.) Window**

Table 7.2 lists the user quota information displayed in the **Display Quota** (User Quota Info.) window.

**Table 7.2 Contents of Display Quota (User Quota Info.) Window**

| Item | Description |
|---|---|
| Name of file share or Shared directory | For a CIFS share, **Name of file share** displays the name of the CIFS share whose quota information is being viewed.<br>For an NFS share, **Shared directory** displays the name of the shared directory whose quota information is being viewed. |
| User name | Name of the logged-in user. |
| Current used block capacity | Amount of block space being used by each user (unit: MB).<br>Shown in red if the amount exceeds the value set as the soft limit or reaches the hard limit. |

| | |
|---|---|
| | If there is less than 1 MB left before the amount reaches the **Hard limit of block**, it may not be possible to create a new file. |
| Soft limit of block | Soft limit (warning value) for block usage (unit: MB). |
| Hard limit of block | Hard limit (upper bound) for block usage (unit: MB). |
| Block grace period | Remaining grace time until files can no longer be created or updated after the block usage exceeds the soft limit. Displayed in one of the following formats:<br>*n* `days`<br>The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.<br>*n* `hours`<br>The remaining grace time is less than 24 hours. The value is shown in orange. For example, `0 hours` appears if less than 1 hour remains.<br>`Over`<br>The grace time has elapsed. Shown in red.<br>`-`<br>The block usage is less than the soft limit. |
| Current used i-node count | Usage of i-node for each user.<br>Shown in red if it exceeds the value set as the soft limit or reaches the hard limit. |
| Soft limit of i-node | Soft limit (warning value) for i-node usage. |
| Hard limit of i-node | Hard limit (upper bound) for i-node usage. |
| i-node grace period | Remaining grace time until files can no longer be created after the i-node usage exceeds the soft limit. Displayed in one of the following formats:<br>*n* `days`<br>The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.<br>*n* `hours`<br>The remaining grace time is less than 24 hours. The value is shown in orange. For example, `0 hours` appears if less than 1 hour remains.<br>`Over`<br>The grace time has elapsed. Shown in red.<br>`-`<br>The user's i-node usage is less than the soft limit. |

To view user quota information set for a file system:

1. In the **List of File Shares** window, select **List of NFS file shares** or **List of CIFS file shares** from the drop-down list, and then click the **Display** button.

   The **List of File Shares** (List of NFS File Shares) (end user) window or **List of File Shares** (List of CIFS File Shares) (end user) window displays. For details on the **List of File Shares** (List of NFS File Shares) (end user) window, see section 7.5. For details on the **List of File Shares** (List of CIFS File Shares) (end user) window, see section 7.5.1.

2. Select a shared directory or share name to view quota information, then click the **Display Quota** button.

   The **Display Quota** (User Quota Info.) window displays.

### 7.6.2 Viewing Group Quota Information (end user)

In the **Display Quota** (Group Quota Info.) window, end users can view the quota information set for a file system for the group to which the end user belongs. Figure 7.7 shows the **Display Quota** (Group Quota Info.) window.

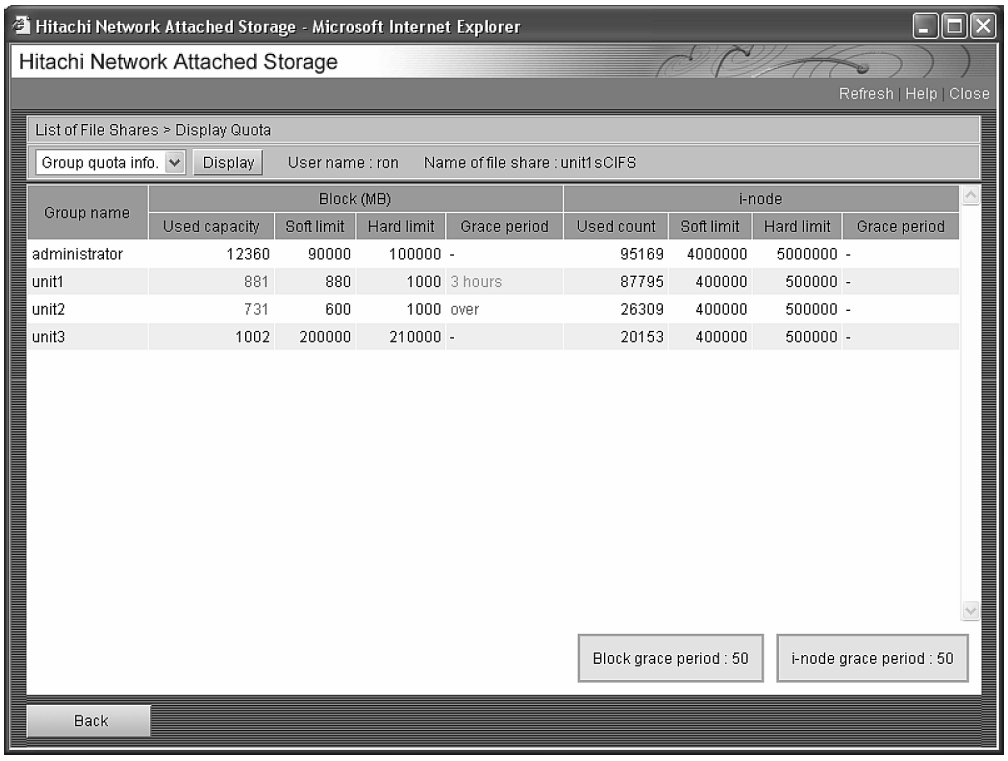



**Figure 7.7 Display Quota (Group Quota Info.) Window**

Table 7.3 lists the group quota information displayed in the **Display Quota** (Group Quota Info.) window.

**Table 7.3 Contents of Display Quota (Group Quota Info.) Window**

| Item | Description |
|---|---|
| Name of file share or Shared directory | For a CIFS share, **Name of file share** displays the name of the CIFS share whose quota information is being viewed.<br>For an NFS share, **Shared directory** displays the name of the shared directory whose quota information is being viewed. |
| Group name | Name of a group to which the logged-in user belongs |

| Item | Description |
|---|---|
| Block (MB) | Availability of the block for each group:<br>**Used capacity**<br>Amount of block space being used (unit: MB).<br>Shown in red if the amount exceeds the value set as the soft limit or reaches the hard limit.<br>If there is less than 1 MB left before the amount reaches the **Hard limit**, it may not be possible to create a new file.<br>**Soft limit**<br>Soft limit (warning value) for block usage (unit: MB).<br>**Hard limit**<br>Hard limit (upper bound) for block usage (unit: MB).<br>**Grace period**<br>Remaining grace time until files can no longer be created or updated after the block usage exceeds the soft limit. Displayed in one of the following forms:<br>*n* days<br>The remaining grace time is 24 hours or longer. For example, 1 days appears if there are 24 hours or more, but less than 48 hours remaining.<br>*n* hours<br>The remaining grace time is less than 24 hours. The value is shown in orange. For example, 0 hours appears if less than 1 hour remains.<br>Over<br>The grace time has elapsed. Shown in red.<br>-<br>The block usage is less than the soft limit. |
| i-node | Availability of i-nodes for each group:<br>**Used count**<br>Usage of i-node<br>Shown in red if it exceeds the value set as the soft limit or reaches the hard limit.<br>**Soft limit**<br>Soft limit (warning value) for i-node usage by the group.<br>**Hard limit**<br>Hard limit (upper bound) for i-node usage by the group.<br>**Grace period**<br>Remaining grace time until files can no longer be created after the i-node usage exceeds the soft limit. Displayed in one of the following forms:<br>*n* days<br>The remaining grace time is 24 hours or longer. For example, 1 days appears if there are 24 hours or more, but less than 48 hours remaining.<br>*n* hours<br>The remaining grace time is less than 24 hours. The value is shown in orange. For example, 0 hours appears if less than 1 hour remains.<br>Over<br>The grace time has elapsed. Shown in red.<br>-<br>The block usage is less than the soft limit. |
| Block grace period | Block grace period set for the file system to which the shared directory belongs. |
| i-node grace period | i-node grace period set for the file system to which the shared directory belongs. |

To view group quota information set for the file system:

1. In the **List of File Shares** window, select **List of NFS file shares** or **List of CIFS file shares** from the drop-down list, and then click the **Display** button.

   The **List of File Shares** (List of NFS File Shares) (end user) window or **List of File Shares** (List of CIFS File Shares) (end user) window displays. For details on the **List of File Shares** (List of NFS File Shares) (end user) window, see section 7.5. For details on the **List of File Shares** (List of CIFS File Shares) (end user) window, see section 7.5.1.

2. Select a shared directory or share name to view quota information, and then click the **Display Quota** button.

   The **Display Quota** (User Quota Info.) window displays. For window details, see section 7.6.1.

3. Select **Group Quota Info.** from the drop-down list, and then click the **Display** button.

   The **Display Quota** (Group Quota Info.) window displays.

## 7.7 Changing Your Password

In the **Password Setup** window, an end user who is registered by NAS Manager can change his or her **Login** password. For increased security, end users should change their passwords regularly.

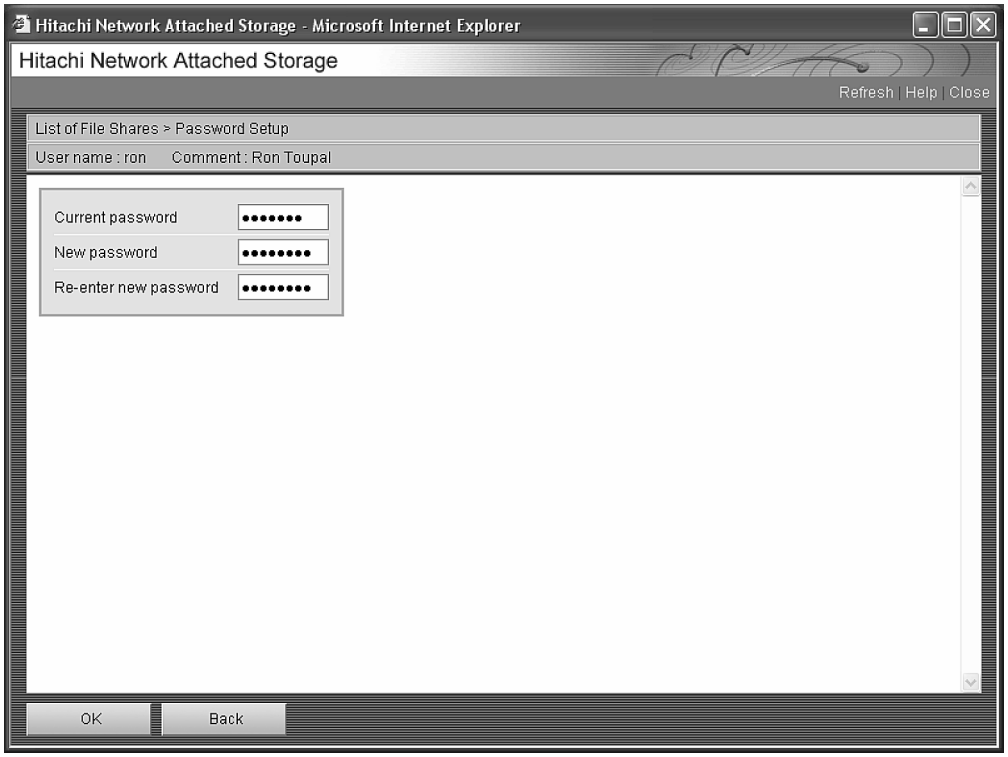



**Figure 7.8 Password Setup Window**

To change your password:

1. In the **List of File Shares** window, select **List of NFS file shares** or **List of CIFS file shares** from the drop-down list, and then click the **Display** button.

   The **List of File Shares** (List of NFS File Shares) (end user) window or **List of File Shares** (List of CIFS File Shares) (end user) window displays. For details on the **List of File Shares** (List of NFS File Shares) (end user) window, see section 7.5. For details on the **List of File Shares** (List of CIFS File Shares) (end user) window, see section 7.5.1.

2. Click the **Password Setup** button.

   The **Password Setup** window displays.

3. Enter the required information as described below, and then click the **OK** button:

   - **Current password**

     Enter your current password.

   - **New password**

     Enter your new password. Specify from 6 to 8 (inclusive) characters.

   - You can use any alphanumeric character, exclamation mark (!), quote ("), number sign (#), dollar sign ($), percent sign (%), ampersand (&), apostrophe ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,) hyphen (-), period (.), forward slash (/), colon (:), semicolon (;), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left bracket ([), backslash (\), right bracket (]), circumflex (^), underscore (_), grave accent (`), left brace ({), vertical bar (|), right brace (}), and tilde (~).

   - **Re-enter new password**

     Re-enter the password that you specified in New password.

   Your password changes and the **List of File Shares** (List of NFS File Shares) (end user) window or **List of File Shares** (List of CIFS File Shares) (end user) window re-displays. At this time, if user information has been registered in the CIFS environment, the password for CIFS user authentication is also applied automatically.

## 7.8 Editing Your User Comment

In the **User Info. Setup** window, a logged-in end user who is registered by NAS Manager can edit the comment in his or her user information.

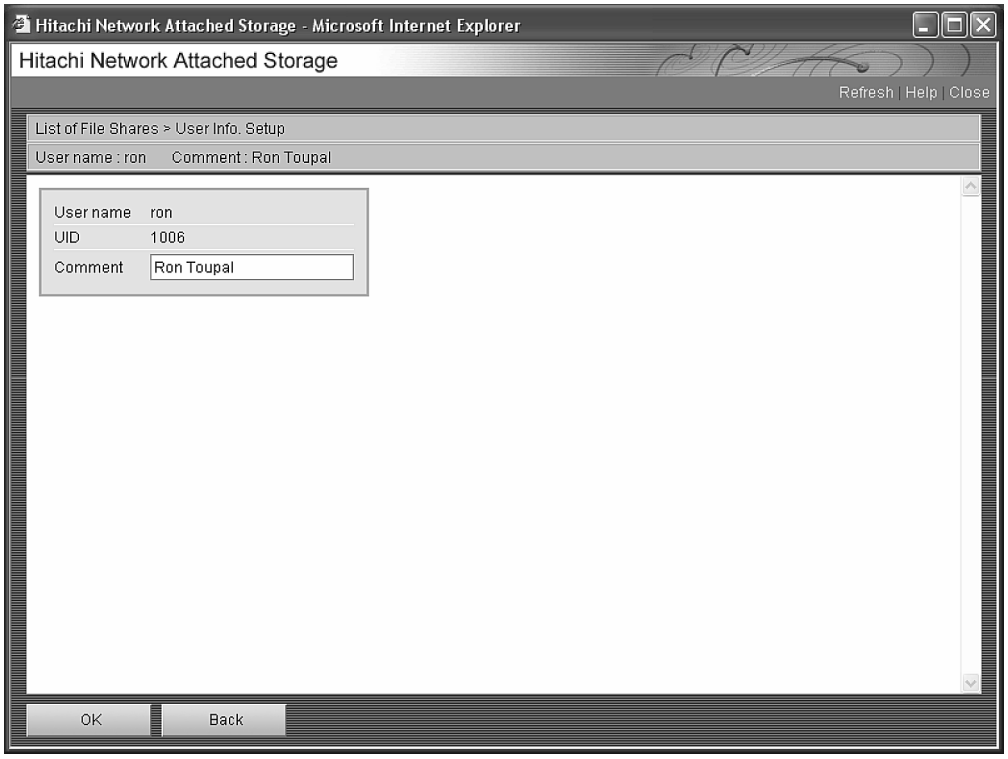



**Figure 7.9 User Info. Setup Window**

To edit your user comment:

1. In the **List of File Shares** window, select **List of NFS file shares** or **List of CIFS file shares** from the drop-down list, and then click the **Display** button.

   The **List of File Shares** (List of NFS File Shares) (end user) window or **List of File Shares** (List of CIFS File Shares) (end user) window displays. For details on the **List of NFS File Shares** (end user) window, see section 7.5. For details on the List of CIFS File Shares (end user) window, see section 7.5.1.

2. Click the **User Info. Setup** button. The **User Info. Setup** window displays.

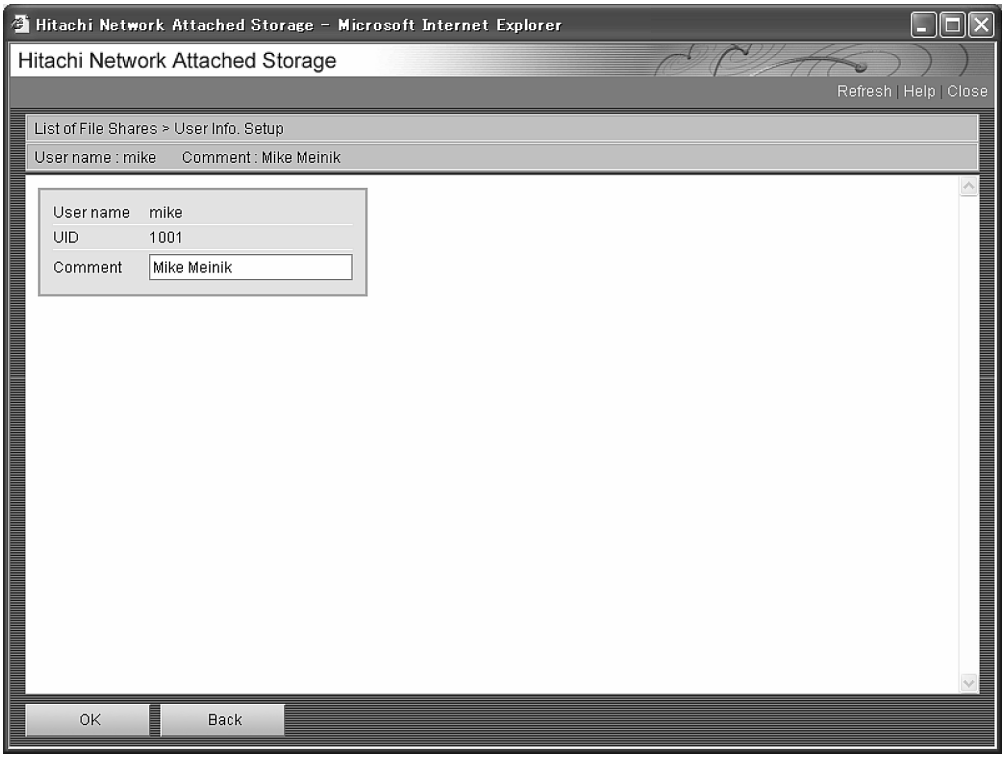



**Figure 7.10 User Info Setup Window**

3. Enter the required information in **Comment**. Enter a maximum of 32 characters.

   You can use any alphanumeric character, number sign (#), percent sign (%), ampersand (&), apostrophe ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), hyphen (-), period (.), forward slash (/), semicolon (;), left angle bracket (<), right angle bracket (>), question mark (?), at mark (@), left bracket ([), right bracket (]), circumflex (^), underscore (_), left brace ({), vertical bar (|), right brace (}), and tilde (~). Although you can optionally specify spaces, they cannot be specified at the beginning or at the end of the character string.

4. Click the **OK** button.

   The comment is set and the **List of File Shares** (List of NFS File Shares) (end user) window or **List of File Shares** (List of CIFS File Shares) (end user) window re-displays.

# Chapter 8 Performing Maintenance Tasks

This chapter describes the tasks performed by a system administrator when NAS Modular system maintenance is required; for example, periodically replacing hardware or software, or when changing the configuration. Complete these tasks as instructed by your HDS representative.

- Maintaining the Hardware (see section 8.1)
- Maintaining the Software (see section 8.2)

## 8.1 Maintaining the Hardware

Of the hardware-related maintenance tasks for the TagmaStore AMS/WMS Series, a system administrator must perform the following tasks:

- Replacement of the management LAN port cable
- Replacement of the data LAN port cables

A system administrator must save user data or must perform a failover or failback for a resource group with which a service is running, as instructed by your HDS representative. While your HDS representative is performing maintenance, follow his or her instructions.

This section describes the tasks that the system administrator performs when replacing hardware periodically, or adding or removing disks.

### 8.1.1 Tasks for replacing hardware periodically

This subsection describes the tasks that the system administrator performs when replacing hardware.

#### 8.1.1.1 Replacing a data LAN cable periodically (when trunking is not used)

The following describes the procedure that the system administrator uses to replace a data LAN port cable periodically when trunking is not used.

To replace a data LAN port cable when trunking is not used:

4. Manually fail over the resource group that is operating on the NAS Unit whose LAN cable is to be removed.

Replace the LAN cable.

Check the switch status.

For details on how to check the switch status, see the documentation for the switch being used.

Fail back the resource groups.

Confirm that a connection to the new LAN cable has been established.

Make the following checks:

- Check the status of the LED beside the LAN port.

  For the exact location of the LED, see the documentation for the disk array.

- Check the contents of the `log_ifconfig` file.

  Use the **List of RAS Information** (Batch-download) window to download the files of the network information log group. Then, check the contents of the `log_ifconfig` file, which is one of the downloaded files. For details on the contents of the `log_ifconfig` file, see *D.2 Output content of the log_ifconfig file*.

#### 8.1.1.2 Replacing a data LAN cable periodically (when trunking is used)

The following describes the procedure that the system administrator uses to replace a data LAN port cable periodically when trunking is used.

Note that if a data LAN cable is replaced while trunking is used, error information will be reported to the maintenance personnel. In this case, the system administrator must tell the maintenance personnel that the LAN cable replacement was required, and then ask the maintenance personnel to delete the error information.

Note

If all the LAN cables are linked down at once while trunking is used, a failover will occur. For each cable, perform the following step1 to 3.

To replace a data LAN port cable when trunking is used:

5. Replace the LAN cable.

Check the switch status.

For details on how to check the switch status, see the documentation for the switch being used.

Confirm that a connection to the new LAN cable has been established.

Make the following checks:

- Check the status of the LED beside the LAN port.

  For the exact location of the LED, see the documentation for the disk array.

- Check the contents of the `log_ifconfig` file.

  Use the **List of RAS Information** (Batch-download) window to download the files of the network information log group. Then, check the contents of the `log_ifconfig` file, which is one of the downloaded files. For details on the contents of the `log_ifconfig` file, see *D.2 Output content of the log_ifconfig file*.

#### 8.1.1.3 Replacing management LAN cables periodically

The following describes the procedure that the system administrator uses to replace a management LAN port cable periodically.

To replace a management LAN port cable:

6. Replace the LAN cable.

Check the switch status.

For details on how to check the switch status, see the documentation for the switch being used.

Confirm that a connection to the new LAN cable has been established.

Make the following checks:

- Check the status of the LED beside the LAN port.

  For the exact location of the LED, see the documentation for the disk array.

- Check the contents of the `log_ifconfig` file.

  Use the **List of RAS Information** (Batch-download) window to download the files of the network information log group. Then, check the contents of the `log_ifconfig` file, which is one of the downloaded files. For details on the contents of the `log_ifconfig` file, see *D.2 Output content of the log_ifconfig file*.

#### 8.1.1.4 Tasks for replacing hardware other than LAN cables

The system administrator need not perform any special tasks when hardware other than cables for LAN ports is replaced.

### 8.1.2 Tasks for adding or removing disks

This subsection describes the tasks that the system administrator performs when adding or removing disks.

While a disk is being formatted, I/O performance for the RAID group that contains the disk is degraded. As a result, file system operations, NAS Modular system operations, and starting and restarting of the NAS OS may slow down.

If you format a disk, do so while accesses to the file system and the NAS Modular system are at a minimum. In addition, do not start or restart the NAS OS while formatting a disk.

### 8.1.3 Adding a Disk to Add a New File System

To add a disk in order to add a new file system, complete the following steps:

1. Request your HDS representative to add a new disk.
2. Create the file system when your HDS representative notify you that the extra disk space has been added.

   For details on creating a file system, see section 4.10.5.
3. Create the file shares.

   For details on creating file shares, see section 4.11.2 or section 4.11.8.

### 8.1.4 Deleting a File System to Remove Disks

To delete a file system in order to remove disks, complete the following steps:

1. Identify the device files and their constituent file systems on the disk that is to be removed.
2. Delete all file shares relating to the file systems on the disk to be removed.

   For details on deleting file shares, see section 4.11.5 or section 4.11.12.
3. Unmount all file systems on the disk to be removed.

   For details on how to unmount a file system, see section 4.10.7.
4. Delete the file systems on the disk to be removed.

   For details on deleting a file system, see section 4.10.9.
5. From the Storage Navigator, identify the logical device numbers of the LDEV that make up each device file.

   For details on how to identify the logical unit number of a device file from the Storage Navigator, see the manual for Storage Navigator Modular.
6. Report the logical device numbers to your HDS representative and ask them to remove the disk.

#### 8.1.4.1 Adding a disk to Expand File System capacity (When using a volume manager)

To add a disk in order to expand file capacity when using a volume manager, you (the system administrator) carry out the following steps:

1. Request the maintenance personnel to add a disk.
2. From Storage Navigator Modular, identify the logical unit numbers for the frame of the LUs that make up each device file.

   For details on how to identify the logical unit number of a device file from Storage Navigator Modular, see the manual for Storage Navigator Modular.
3. Expand the capacity of the file system in the **Expand File System** window.

### 8.1.5 Expanding File System Capacity (When not using a volume manager)

When another disk is required to expand the capacity of a file system, perform the following tasks.

1. Request clients to stop using the file system to be expanded.
2. Back up the file system.

   For details on backing up a file system, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.
3. Delete all file shares for the file system.

   For details on deleting file shares, see section 4.11.5 or section 4.11.12.
4. Unmount all file systems from the disk to be expanded.

   For details on how to unmount a file system, see section 4.10.7.
5. Delete the file system to be expanded.

   For details on deleting a file system, see section 4.10.9.
6. Advise your HDS representative that the file system has been deleted and ask them to add another disk.
7. Re-create the file system when your HDS representative notify you that the extra disk has been added.

   For details on creating a file system, see section 4.10.5.
8. Restore the file system from backup.

   For details on restoring a file system, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.
9. Re-create the file shares.

   For details on creating file shares, see section 4.11.2 or section 4.11.8.

### 8.1.6 Removing a Disk to Reduce File System Capacity

To remove a disk in order to reduce file system capacity, complete the following steps:

1. Request clients to stop using the file systems on the disk to be removed.
2. Back up the file systems.

   For details on backing up a file system, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.
3. Delete all file shares for the file systems on the disk to be removed.

   For details on deleting file shares, see section 4.11.5 or section 4.11.12.
4. Unmount all file systems from the disk to be removed.

   For details on how to unmount a file system, see section 4.10.7.
5. Delete the file systems on the disk to be removed.

   For details on deleting a file system, see section 4.10.9.

6. Advise your HDS representative that the file systems have been deleted and ask them to remove the disk.
7. Re-create the file systems when your HDS representative notify you that the disk has been removed.

   For details on creating a file system, see section 4.10.5.
8. Restore the file systems from backup.

   For details on restoring a file system, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.
9. Re-create the file shares.

   For details on creating file shares, see section 4.11.2 or section 4.11.8.

## 8.2 Software Maintenance

This section is for system administrators who are responsible for program management and describes how to install the NAS Manager program.

The NAS OS is installed by your HDS representative. According to the instructions of your HDS representative, you should stop and start the node in which the resource group is running, or to perform failover and failback to the resource group. For details on performing failover and failback for a resource group, see section 4.5.11. For details on stopping and starting a node, see section 4.5.5.

In some cases, a system administrator can install patches (programs individually provided) for the NAS OS from the NAS Manager GUI. To determine whether or not patches can be installed from the NAS Manager GUI, see the documentation provided by the program developers.

### 8.2.1 Installing NAS Manager

To install NAS Manager, complete the following steps:

1. Obtain a patch version, corrected version, or regular version of the program from the developer.

   Proceed as detailed in the documentation accompanying the program.
2. Install the regular version of the program into all NAS Units in the cluster.

   Make sure that installation was successful. For details on the installation procedure, see section 4.15.2.
3. If requested by an instruction in the documentation attached to the program obtained in step 1, reboot the NAS OS.

   For details on rebooting the NAS OS, see section 4.5.12.

### 8.2.2 Installing an optional program

To install an optional program of NAS Manager, the system administrator carries out the following steps:

1. Obtain a regular (official) version of the program from the program developers.

   Proceed as detailed in the documentation accompanying the program.

2. Install the regular version of the program into all NAS Units in the cluster.

3. If requested by an instruction in the documentation attached to the program obtained in step 1, reboot the NAS OS.

### 8.2.3 Installing a NAS OS Patch Version

To install a NAS OS patch version, complete the following steps:

1. Receive the NAS OS patch version from the developer.

   Proceed as detailed in the documentation accompanying the program. If you are instructed to stop a node or cluster, do it before installing the program.

2. Install the program on all NAS Units in the cluster.

   Make sure that installation was successful. For details on the installation procedure, see section 4.15.2.

3. If requested by an instruction in the documentation attached to the program obtained in step 1, reboot the NAS OS.

   For details on rebooting the NAS OS, see section 4.5.12.

# Chapter 9 Troubleshooting

This chapter describes the procedures to be performed by a system administrator for errors that might occur in a NAS Modular system. Always contact your HDS representative if you cannot identify the cause of an error or solve the problem.

- General Troubleshooting Procedures (see section 9.1)
- Identifying the Error (see section 9.2)
- Recovering from an Error (see section 9.3)
- Collecting Data and Contacting your HDS representative (see section 9.4)

## 9.1 General Troubleshooting Procedures

This section describes the general procedure for solving errors that occur during operation of a NAS Modular system. Figure 9.1 illustrates the general troubleshooting procedure.

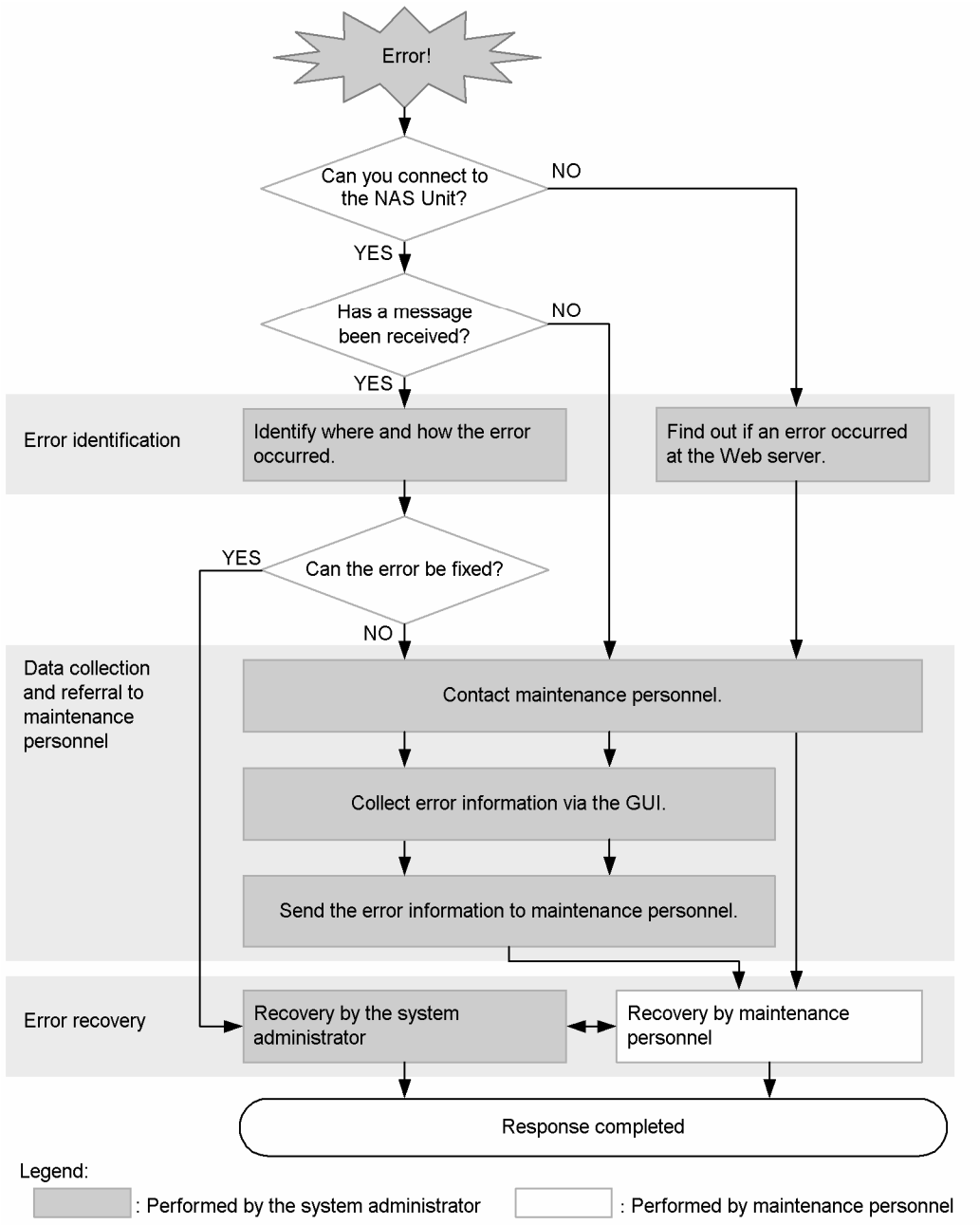



**Figure 9.1 General Troubleshooting Procedure**

### 9.1.1 Detecting Errors

A system administrator can detect errors in a NAS Modular system from the following sources:

- Notification of the stop of a service from an end user

  Before a system administrator detects an error, an end user of a NAS Modular system may notify the system administrator that a file share service has stopped.

- SNMP notification

When SNMP is set, the SNMP manager can notify a system administrator of an error in NAS Manager or the disk array. For details on the SNMP settings in NAS Manager, see section 4.7.13. For details on the SNMP settings in the disk array, see the manual for SNMP Agent Support Function.

- E-mail notification

  If an error has occurred in the disk array, an e-mail can be used to notify a system administrator of the error. For details on the settings for e-mail notification and messages to be reported, see the *Storage Navigator Modular User's Guide*.

- Status check with the error monitoring function of Storage Navigator Modular

  When NAS Units are registered as disk array components in Storage Navigator Modular and set so that errors can be monitored, the status of the NAS Units can be checked from the Storage Navigator Modular GUI. For details on registering NAS Units as disk array components, monitoring errors, and checking the status of NAS Units, see the *Storage Navigator Modular User's Guide*.

- Warning LED on a NAS Unit

  If an error occurs on a NAS Unit, the warning LED on the NAS Unit is turned on.

- Buzzer of the disk array

  If an error that stops the NAS Modular system occurs, the disk array beeps. For details on setting the volume of the buzzer, see the documentation for the disk array

- Web flasher

  When a NAS Unit has been registered as a component in a Web flasher, if an error that stops the NAS Modular system operation occurs, the flasher is activated.

### 9.1.2 Troubleshooting

If you confirm that an error has occurred in the NAS Modular system, you must discover the cause of the error and take corrective measures.

- **Identifying the error**

  Investigate the error information detected by NAS Manager to find out why the problem occurred. If a failover resulted from the error, contact your HDS representative immediately. For details on discovering the cause of an error, see section 9.2.

- **Collecting data and contacting your HDS representative**

  In the event of a problem that you cannot fix or identify a cause, collect the error information and contact your HDS representative. For details on collecting error information, see section 9.4.

- **Recovering from an error**

  When you know what caused the error, take the recovery action indicated by the error message or by your HDS representative. Depending on the type of error, you may need to restore the system in consultation with your HDS representative. Carry out the necessary operations as instructed. For details on restoring the system after an error, see section 9.3.

## 9.2 Identifying the Error

If an error occurs in the NAS Modular system, complete the following steps to identify the cause of the error:

1. Check the error message displayed in the processing results window in the NAS Manager.
2. Check the system messages displayed in the **List of RAS Information** (List of Messages) window in NAS Manager.
3. Check the error information displayed in the **Browse Cluster Status** window in NAS Manager.
4. Check the error status of the file system and device files in the **List of File Systems** window in NAS Manager.
5. Check the error information using SNMP notification.
6. Check whether an error has occurred on the Web server.
7. Check the connection between the NAS Units and the following servers:
   - DNS server
   - NIS server
   - NTP server
   - LDAP server
   - CIFS client authentication server
8. Check the error message received by email.
9. Check error information by using Storage Navigator Modular.

   For details on checking error information by using Storage Navigator Modular, see the manual *Storage Navigator Modular User's Guide*.

An end user may notify a system administrator that services of the NAS Modular system are unavailable before the system administrator detects the error. For details on how to identify the cause of the error in this situation, see section 9.2.1 if an end user cannot use services of a NAS Modular system.

If a failover has occurred, contact your HDS representative.

### 9.2.1 Verifying the Source of Error without using a NAS Modular System

This subsection describes how a system administrator can discover the cause of an error if an end user cannot mount a volume to a file system or cannot use other NAS Modular system services.

#### 9.2.1.1 Verifying the Source of Error

To verify the error location and the error cause when a user notifies you that a service has stopped, take the following steps:

1. Receive a report from the user that the file share service has stopped. You must check whether the file share used by the user is an NFS share or a CIFS share:
   - If an NFS share is stopped:

     The system administrator must check the service IP address and shared directory name for the stopped service with the end user, to determine the cluster, node, resource group, file system, or directory.
   - If a CIFS share is stopped:

     The system administrator must check the shared path name for the stopped service (*NNC-name**CIFS-share-name**directory-path-used*) with the end user, to determine the cluster, node, resource group, file system, or folder.

     If you are using user mapping, review the mapping information to make sure that user IDs and group IDs have been assigned correctly to those users who cannot use the service. For details, see 9.2.9.
2. Check the access suppression status for the file system.

   Access from end users to the file system is temporarily suppressed during the following operations:
   - Creating a differential-data snapshot (NAS Sync Image functionality)
   - Expanding a differential-data storage device (NAS Sync Image functionality)
   - Performing online backup (NAS Backup Restore functionality)

   If the Remote Copy function of NAS Backup Restore is being used, the system administrator might have intentionally suppressed access from clients by using the horc_pvol_freeze command.

   The system administrator must use the enas_fsctl command to check the access suppression status for the file system that was being used by end users. For details on the syntax of the enas_fsctl command, see enas_fsctl (Manage an active file system) in Chapter 6.

   If access suppression has not been disabled because of an error or a mistake by the system administrator, use the horc_pvol_unfreeze command of NAS Backup Restore to disable access suppression. For details on the syntax of the horc_pvol_unfreeze command, see the *NAS Backup Restore Modular User's Guide*.
3. In the **Browser Cluster Status** window, check the error information.

   See the **Browse Cluster Status** window of the NAS Manager of the cluster determined in the previous step, and confirm that no error has occurred with the failover function. For details about how to check the status of the failover function, see section 5.5.8.

   CIFS share service stoppage due to resource group migration.

   When a resource group is migrated due to failover or failback, even if the failover or failback succeeds, services for the CIFS share using the migrated resource group will be forced to terminate. For details, see section 2.8.2.

4. In the **List of Services** window, check the operation status of the service.

   If you are unable to confirm that an error has occurred with the failover function, the service may have stopped. In the **Browse Cluster Status** (Resource Group Status) window, see the **Running node** to check the node allocated to the resource group used by the user. Then, check that node in the **List of Services** window in the NAS Manager to confirm the operating status of the service used by the user. For details about how to view the **List of Services** window, see section 4.6.1.

5. Check the error information in the **List of File Systems** window.

   If you are unable to confirm whether an error has occurred in the operation of the service used by the user, the error may lie with the file system. In the **List of File Systems** window of the NAS Manager, check the status of the file system determined in step 1. For details about checking the status of a file system, see section 4.10.4.

6. In the **List of File Shares** window, check the file share settings:

   – If you are unable to confirm whether an error has occurred in the correctly-mounted file system, in the **List of File Shares** window of the NAS Manager, check the file share used by the user. For details about viewing the **List of File Shares** window, see section 4.11.1 or section 4.11.7.

     If the set file share that was specified by using either the host name or the netgroup name is not displayed, there might be an error in one of the following servers:

     – NIS server
     – DNS server
     – WINS server

     For details on how to check the connection to the servers, see 9.2.10. You also check the settings of the DNS server and NIS server in the **DNS, NIS, LDAP Setup** window.

7. Check the operating environment for the network and clients.

   If the file share is displayed but you are unable to confirm that an error occurred, check whether the operating environment for the network and clients has an error.

   Check the configuration and operating status of the network connecting the NAS Unit and client. Check the connection between the NAS Units and the following servers:

   - DNS server
   - NIS server
   - NTP server
   - LDAP server for user authentication
   - LDAP server for user mapping
   - CIFS client authentication server

   – If the set file share is not displayed:

     If the file share, set by specifying either the host name or netgroup name, is not displayed, the error may lie in the NIS server, DNS server, or WINS server. In the **NIS and DNS Setup** window of the NAS Manager, check the NIS server or DNS server that is being used on the NAS Modular system. For details on viewing the **NIS and DNS Setup** window, see section 4.7.5.

8. Check the network connection status.
9. Investigate any error causes outside the disk system.

   If you are unable to confirm whether an error has occurred in the displayed file share, confirm that the cause of the error lies within the disk system:

   - The operating environment for the network:

     Check the configuration and operating status of the network connecting the NAS Unit and client. For details about the network configuration for a NAS Modular system, see section 2.2.

   - The operating environment for the client:

     If the operating environment of the client does not meet the usage conditions for the file system provided by the NAS Modular system, file share services may become unusable when failover or failback occurs. For details about the operating conditions for file systems provided by the NAS Modular system, see section 2.7.1.

If you are not using SNMP notification and an error that disables the NAS Manager occurs, you will not be able to examine the error information. We therefore recommend that you use NAS Manager in conjunction with SNMP notification.

This section describes how to check error information and identify errors.

#### 9.2.1.2 Verifying the Source of Error When Unable to Verify the Error has Occurred

Error information, such as NAS Modular system messages and error messages, is not always output even when an end user cannot use services of the NAS Modular system. If no error information is output, the system administrator is unable to confirm that an error has occurred. This situation tends to occur if a network failure occurs or network settings are incorrectly specified.

The following procedure shows how you can discover the cause of an error if you are unable to confirm that the error has occurred.

To discover the cause of an error you are unable to find:

1. Receive a report from the end user that the file share service has stopped.

   Check whether an error has occurred.

2. Check whether the NAS Unit, network hub, and disk array are turned on.

   If they are turned off, turn them on, and then check whether the end user can use services of the NAS Modular system.

3. From the client machine of the end user who cannot use services, use the ping command to check the connection status for the fixed IP address of the NAS Unit.

   - If the NAS Unit responds:

From the client machine of the end user who cannot use the desired services, use the `ping` command to check the connection status for the service IP address of the NAS Unit. If the NAS Unit responds, the error may pertain to the NAS OS. Collect the NAS dump and restart the NAS OS, regardless of whether the NAS Unit responds. If the maintenance personnel ask to have the error information collected, collect the NAS Dump. For details, see the documentation for the disk array.

If the maintenance personnel ask to have the error information collected, collect the NAS Dump. For details, see the documentation for the disk array.

– If the NAS Unit does not respond:

A network error may exist on the route between the client machine of the end user who cannot use services and the NAS Unit. Check whether the IP address settings are correct, and contact the network administrator. If no network error in the network, contact your HDS represetative.

### 9.2.2 Checking Error Messages in the Processing Results Window

If an error results from an incorrect GUI operation, an error message appears in the processing results window. For a detailed explanation of displayed error messages, see the *NAS Modular Error Codes*. You can use the message ID to locate the relevant message, and check the message particulars.

An error listed in the processing results window is typically caused by:

- An incorrect specification of a server, network, or other connection target.
- An error that occurred in the connection target server or in the network device.
- Incorrect GUI operations and input values due to an incorrect procedure or setting.
- An unexpected update of a setting value due to multiple logins by system administrators.
- Insufficient NAS OS LU free capacity.
- A temporary loss of function due to a software error.
- A hardware error occurred in the NAS Modular system.

Check the displayed error message to identify the cause of the problem.

### 9.2.3 Checking System Messages

Important messages that affect the NAS Modular system as a whole are output to the system messages log. Such messages may be about hardware or software errors, or incorrect GUI operations, for example.

In the event of an error, check the system messages in the **List of RAS Information** (List of Messages) window in NAS Manager to find out where and why the error occurred. For details on checking system messages, see section 4.13.1.

Error information, including system messages, can be reported by SNMP notification. For more information, see section 9.2.6.

From the system message ID, you can identify the program in which the error occurred. From the message text, you can see what caused the error.

If you cannot identify the cause of the error from the system messages, or if a message advises you to contact your HDS representative, download the error information and forward it to your HDS representative.

System messages consist of a message ID and message text.

The message ID format is as follows:

KA*XXYYYYY-Z*

*$X^1X^2$*

Characters representing the program that produced the message. The meanings are as follows:

QB: NAS Backup Restore

QG: NAS File Sharing

QK: NAS Data Control

QM: NAS Manager

QS: NAS Sync Image

QV: NAS Anti Virus Agent

*$Y^1Y^2Y^3Y^4Y^5$*

A number representing the message type

*Z*

A symbol representing the message level. The meaning is as follows:

E: Error level

I: Information level

W: Warning level

Q: Query level

Message IDs KAQG70000 to KAQG799 indicate a message related to the failover.

Even if the system outputs a message reporting that failover was successful, you must still recover from the error that triggered the failover. Check the system messages to identify the error cause.

If the system outputs a message reporting that failover was unsuccessful, as well as recovering from the error that triggered the failover, you must also identify what caused the unsuccessful failover and the recover from the problem. For details on identifying the cause of a failover error, see section 9.2.4.

### 9.2.4 Checking Error Information in the Browse Cluster Status Window

In the event of an error in the failover, you can check the status of the cluster, nodes, and resource groups in the **Browse Cluster Status** window. For details, see section 4.5.3.

For details on recovering from an identified error in a cluster, node, or resource group, see section 9.3.4.

You can identify the error cause by checking the system messages displayed before or after the time when the error occurred, and by checking the error status displayed in the **Browse Cluster Status** window. The table below lists the cluster statuses displayed in this window and the causes that generate each status.

**Table 9.1 Cluster Statuses and Causes for Display**

| Cluster Status | Description | Causes for Status Display | | | |
|---|---|---|---|---|---|
| | | Normal | Hardware Error | Software Error | User Error |
| ACTIVE | Running normally | Yes | Not Applicable | Not Applicable | Not Applicable |
| INACTIVE | Stopped | Yes | Not Applicable | Not Applicable | Yes |
| UNKNOWN | Status unknown | Not Applicable | Yes | Yes | Yes |

You can view the status of a node in **Node status** in the **Browse Cluster Status** (Cluster / Node Status) window. The table below lists the node statuses displayed in this window and the causes that generate each status.

**Table 9.2 Node Statuses and Causes for Display**

| Node Status | Description | Causes for Status Display | | | |
|---|---|---|---|---|---|
| | | Normal | Hardware Error | Software Error | User Error |
| UP | Running normally | Yes | Not Applicable | Not Applicable | Not Applicable |
| INACTIVE | Stopped | Yes | Not Applicable | Not Applicable | Not Applicable |
| DOWN | Stopped abnormally | Not Applicable | Yes | Yes | Not Applicable |
| UNKNOWN | Status unknown | Not Applicable | Yes | Yes | Yes |

You can view the status of a resource group in **Resource Group Status** in the **Browse Cluster Status** (Resource Group Status) window. The resource group status and error information are displayed in the following form:

*resource-group-status*/*error-information*

The table below lists the resource group statuses displayed in this window and the causes that generate each status.

**Table 9.3 Resource Group Statuses and Causes for Display**

| Resource Group Status | Description | Causes for Status Display | | | |
|---|---|---|---|---|---|
| | | Normal | Hardware Error | Software Error | User Error |
| Online | Running normally. | The displayed message corresponds to the resource group error data. | | | |
| Online Maintenance | Automatic failover is not possible because monitoring is disabled. | | | | |
| Online Pending | Starting. | Yes | Not Applicable | Not Applicable | Not Applicable |
| Online - Ready | The resource group cannot start because the cluster is inactive, or the service is not running normally because an error occurred while the cluster was stopping. | Yes | Not Applicable | Yes | Yes |
| Offline | Stopped. | The displayed message corresponds to the resource group error data. | | | |
| Offline Pending | Stopping. | Yes | Not Applicable | Not Applicable | Not Applicable |
| Discovery (exclusivity) | Starting. | Yes | Not Applicable | Not Applicable | Not Applicable |
| Initializing | Starting. | Yes | Not Applicable | Not Applicable | Not Applicable |
| Internal Error | Internal error detected. Contact your HDS representative. | Not Applicable | Yes | Yes | Not Applicable |

The following table lists the resource group error information displayed in the **Browse Cluster Status** (Resource Group Status) window and the causes for the error information.

**Table 9.4 Resource Group Error Information and Reasons for Display**

| Error Information | Description | Causes for Error Information Display | | | |
|---|---|---|---|---|---|
| | | Normal | Hardware Error | Software Error | User Error |
| No error | No error occurred. | Yes | Not Applicable | Not Applicable | Not Applicable |
| Internal error - not recoverable | An unrecoverable internal error was detected. | Not Applicable | Yes | Yes | Not Applicable |
| Monitor activity unknown | An error occurred in processing during monitoring or outside the monitoring scope | Not Applicable | Not Applicable | Yes | Not Applicable |
| No available nodes or No available nodes in | An error occurred but a failover could not be performed because it is already in a failover | Yes | Not Applicable | Not Applicable | Yes |

| | | | | | |
|---|---|---|---|---|---|
| failure domain after monitor failure | status. | | | | |
| Node unknown | The resource group cannot start because the **Node status** of the node is UNKNOWN. | Not Applicable | Yes | Yes | Yes |
| Split resource group (exclusivity) | The duplicate resource group is active within the cluster. Perform a forced stop for the cluster, and then ask the maintenance personnel to restart the NAS OS on both NAS Units. For details on how to restart the NAS OS, see the manual *Storage Navigator Modular User's Guide*. | Not Applicable | Not Applicable | Yes | Yes |
| srmd executable error | An error occurred during start or stop processing. | Not Applicable | Yes | Yes | Not Applicable |

Errors in the failover can be classified as follows:

- Errors at NAS OS startup
- Errors at cluster operation
- Errors triggering a failover
- Errors at unsuccessful failover
- Other types of errors

The steps you should take to identify what caused the error depend on the particular situation, as described below.

### 9.2.4.1 Identifying Errors at NAS OS Startup

An error at NAS OS startup may cause a communication failure between the nodes in the cluster. In this case, the status of the cluster and nodes is shown as UNKNOWN in the **Browse Cluster Status** (Cluster/Node Status) window, and the services fail to start. Your HDS representative must perform startup and shutdown of the NAS OS. Perform any error recovery operation that includes startup or shutdown of the NAS OS as instructed by your HDS representative.

The main situations in which you may need to start or restart the NAS OS are:

- Starting after the NAS OS is stopped by a planned shutdown for maintenance
- Starting after replacing a NAS Unit
- Starting after changing an NNC name

- Starting after performing a planned stop of a disk array of the TagmaStore AMS/WMS series

All the file systems are mounted when the NAS OS is activated and the services start. If there are a large number of file systems, the activation process of the NAS OS and the startup process for the services can take a long time. By making a note of the standard time taken for services to start after you boot the NAS OS, you will be able to quickly discover any problems that may occur.

If services have not started within the standard time after NAS OS startup, check the status of the cluster and nodes in the **Browse Cluster Status** (Cluster / Node Status) window to identify the problem.

If you have performed a planned shutdown of the whole NAS Modular system by shutting down the power of a disk array of the TagmaStore AMS/WMS series, when the power is restored the services will start automatically. However, if you perform any one of the procedures below before shutting down the power of disk array, services will not start automatically. Also note that, after a NAS OS shutdown, services will usually not start automatically regardless of operations performed before the NAS OS shutdown.

- Stopping a cluster when shutting down the NAS OS.
- Stopping a cluster or node when shutting down the power of the disk array.

Normally services do not start automatically regardless of operations performed before the NAS OS shutdown.

#### 9.2.4.2 Identifying Errors at Cluster Operation

If a cluster operation fails due to an error, error information is displayed for the affected cluster, nodes, or resource group in the **Browse Cluster Status** window.

The main types of cluster operations you may need to perform are:

- Operating on the status of a cluster, node, or resource group in the **Browse Cluster Status** window
- Adding or deleting capacity to a file system
- Adding or deleting a file system
- Adding or deleting a file share
- Changing a node name or cluster name
- Adding, changing, or deleting a service IP address

In the NAS Modular system, services are stopped and failover is not performed if the same error is likely to recur and disrupt services after failover. In this case, any attempt to move the resource group to the other node in the cluster without first fixing the error will fail. Also, if you attempt to mount a file system that was not created by the NAS Modular system or the file system creation is unsuccessful, any cluster operations will fail.

If services stop when you attempt a cluster operation, check the status of the cluster, nodes, and resource groups in the **Browse Cluster Status** windows and identify the cause of the error.

#### 9.2.4.3 Identifying Errors Triggering a Failover

If the system is allowed to continue running in a degenerated state after a successful failover, access performance will decline and any subsequent errors may cause services to stop. When an error triggers a failover, it is essential to fix the problem and to return to normal operation as soon as possible.

Check the system messages on both nodes using the **List of RAS Information** window of NAS Manager, and identify the cause of the error that caused the failover. For details on checking system messages, see section 9.2.3.

#### 9.2.4.4 Identifying Errors at an Unsuccessful Failover

If an error occurs in the failover, failover will be unsuccessful and the provided services will stop. Before recovering from the failover error, you must first recover from the original problem that triggered the failover and restart the services. For details on identifying errors that trigger a failover, see section 9.2.3.

After you have restarted services, collect the error information and contact your HDS representative to identify the cause of unsuccessful failover.

#### 9.2.4.5 Identifying Other Types of Errors

The daemons that constitute the failover restart automatically if anything causes them to stop. Each daemon may output core files and stop.

If an error has disabled services, open the **List of RAS Information** (List of Core Files) window and check whether a recurring error has produced a succession of core files. For details on displaying this window, see section 4.14.1.

If an error occurred in the system, the status of clusters and nodes may not be displayed in the **Browse Cluster Status** window. Collect the error information and contact your HDS representative.

### 9.2.5 Checking Error Statuses in the List of File Systems Window

If an error occurs with a file system or device file, you must the error status of the file system or device file in the **List of File Systems** window, and work with your HDS representative to recover from the error. For more information, see section 4.10.4.

The system administrator also needs to determine the cause of the error by checking the system messages displayed in the **List of RAS Information** (List of Messages) window around the time that the error occurred.

If the cause of the error lies in the file system operated by NAS Manager, take action according to the procedure described in 9.3.29.

If the cause of the error lies in a file system used by the NAS Sync Image differential-data snapshot function, or in the differential-data snapshot itself, take action according to the procedure described in the manual *NAS Sync Image Modular User's Guide*.

### 9.2.6 Checking Error Information by using SNMP Notification

When using SNMP notification, SNMP traps can be issued to an SNMP manager program that was set up in advance. This allows you to identify the location and cause of any errors.

***Note:*** To use SNMP error notification, you must first prepare an SNMP manager and complete SNMP setup. For details, see section 4.7.13.

If an error at the Error level occurs, an SNMP trap is issued to the predefined SNMP manager to report the error information. You can identify the cause of the error from the message ID in the received notification. For message ID categories, see section 9.2.3. For the data formats of the error information reported by SNMP traps, see Appendix A.2, *List of MIB Objects*.

### 9.2.7 Checking for a Web Server Error

Failure to connect to a specified NAS Unit may be due to an error at the Web server, or a problem in the network connection. If a user cannot connect to a specified NAS Unit, use the `ping` command to check the connection status. The network may not be physically connected. For example:

- A LAN cable may be disconnected
- A NAS Unit may be incorrectly mounted
- The power may be disconnected

If the specified NAS Unit is still unreachable and the network is connected, it is possible that an error occurred on the Web server running on the NAS OS. In this case, if SNMP error notification is implemented in your system, an SNMP trap will be issued. You can then verify the Web server error in the error information. The file system services do not stop if there is a Web server error.

The Web server restarts automatically after an error. If the error is temporary, the Web server will recover from the error at automatic restart.

If connection to the NAS Unit still fails after the Web server restarts automatically, or if the system issues SNMP traps relating to the Web server, notify your HDS representative that you suspect a Web server failure.

### 9.2.8 Checking Error Information Sent by E-mail

The e-mail notification function of Storage Navigator Modular can notify the system administrator of an error that occurred in the disk array. For more information, see the manual *Storage Navigator Modular Graphical User Interface (GUI) User's Guide*.

### 9.2.9 Checking user mapping information

If an end user is unable to use the CIFS service in an environment where user mapping is enabled, user IDs and group IDs might not have been assigned correctly. In this case, the system administrator needs to check that:

- CIFS service configuration definitions are the same on both nodes

  In the **CIFS Service Maintenance** window, check whether the CIFS service configuration definitions have been applied the same on both nodes. For details on how to check the CIFS service configuration definitions, see 4.6.4.1.

- The CIFS service is operating correctly

  In the **List of Services** window, make sure the **Status** of the CIFS service is **Running**.

- The NAS Units are connected to the domain controller

  In the **CIFS Service Maintenance** window, make sure the **DC server connection status** is **Connectable**. For details about the **CIFS Service Maintenance** window, see 4.6.4.1.

- A trust has been established between the domains

  Verify whether a trust has been established between the registered domains. For example, if you use Windows 2000 Server or Windows Server 2003 as the domain controller, you can check for a trust relationship by using Windows administrative tools.

- The latest user information has been applied

  If an end user accesses a CIFS share immediately after the user or the group information managed by a domain controller is changed, old user mapping information that has been cached may be applied.

  If a system administrator makes a change to the user or the group information managed by a domain controller (such as re-creating a user), the system administrator must restart the CIFS service or inform end users that the CIFS share must not be accessed for five minutes, to refresh the information.

If no particular problems are found, the system administrator must perform either of the following tasks:

- Delete the cached user mapping information

- Inform end users that the CIFS share must not be accessed for five minutes

Depending on the user mapping method you are using, also check the following requirements.

#### 9.2.9.1 User mapping using RIDs

Check the following requirements when user mapping uses RIDs:

- The domains to which users of the CIFS service belong have been set in NAS Manager.

  Users who belong to a domain that is in a direct trust relationship with the domain that the NAS Unit belongs to, but is not set up in NAS Manager, will be unable to use the CIFS service provided by the NAS Modular system.

  Make sure that the domain has been set up under **User mapping information** in the **CIFS Service Maintenance** window.

- The IDs of the users and groups who will use the CIFS service fall within the range of valid user IDs and group IDs that you set for each domain.

  Users whose user ID or group ID falls outside the range specified under **User mapping setup** in the **CIFS Service Management** window will be unable to use the CIFS service.

  When using NAS Manager commands, check that the user or group name can be converted to an ID mapped using RIDs. For details on checking the IDs and names of users and groups mapped using RIDs, see 5.7.4.

#### 9.2.9.2 User mapping using LDAP

Check the following requirements when user mapping uses LDAP:

- The LDAP server is operating correctly.

  Check whether the LDAP server set in the **CIFS Service Management** window is operating correctly.

- The highest value of the assigned user IDs and group IDs is within the specified range of the user ID or group ID.

  From the **List of RAS Information** (Batch-download) window, download a group of user mapping information logs in a **Batch Operation**, and then check whether a user ID or group ID is assigned to an end user that cannot use the CIFS service. If there are no IDs that are assigned to end users that cannot use the CIFS service, in the **CIFS Service Maintenance** window, make sure that the values displayed in **Largest currently used UID** and **Largest currently used GID** are not the same as the largest values of IDs displayed in **Range of UIDs** and **Range of GIDs**.

  For details on the **CIFS Service Maintenance** window, see 4.6.4.1.

### 9.2.10 Checking for a possible server connection problem

To find out whether there is a problem in the network connection to the NAS Units, check the status and network configuration of the following servers used by the NAS Modular system:

- DNS server
- NIS server
- NTP server

- LDAP server
- CIFS client authentication server

The system administrator should download the network information logs in a **Batch Operation** from the **List of RAS Information** (Batch-download) window.

You should then view the `log_interfaces_check` file in the downloaded log files to check the connection between each server and the NAS Units. For details on the information output to the `log_interfaces_check` file and the appropriate action to take, see *D.3 Output content of the log_interfaces_check file*.

## 9.3 Collecting data and contacting the maintenance personnel

If you cannot identify the cause or location of an error, or if you cannot fix the problem, you must collect the required information, as indicated in the error message. Download the error information from the **List of RAS Information** window in NAS Manager, and then forward the information to the maintenance personnel.

If you find in the course of investigation that a failover has occurred, you must contact the maintenance personnel.

This section describes how to collect error information.

### 9.3.1 Downloading error information

A system administrator can use the NAS Manager GUI to download error information. Follow the instructions provided by the message or by maintenance personnel, and download all of the log data (**All log data**) from the **List of RAS Information** window or other logs instructed by the message or by maintenance personnel, and then submit all collected data to maintenance personnel.

Recovering from an Error

When an error occurs, you will identify its cause from the error message and system messages, and take recovery action as indicated in the message text or as instructed by your HDS representative.

Error recovery operations must be based on liaison between the HDS representative and the system administrator. If you (the system administrator) cannot fix the error, perform failover and failback operations as instructed by your HDS representative. Your HDS representative must perform startup and shutdown of the NAS OS. Be sure to contact your HDS representative when you need to start or shut down the NAS OS during the error recovery operations.

During error recovery, you must complete the following tasks:

- Check any erroneous GUI operations and run them again.
- Check the system messages and take appropriate action.

- View the error information in the **Browse Cluster Status** window and take recovery action.
- Perform manual failover and failback.
- Request your HDS representative to restart the NAS OS.
- Replace the NAS Manager (if the system administrator is responsible for program management).
- Check error information about the file system and device file in the **List of File Systems** window.
- Check the error information in the **List of Interfaces** window to recover from errors.
- Check the error information on data LAN port errors in the **List of Data Ports** window to recover from errors.
- Replace cables connected to the data LAN port and management LAN port.

This section describes each of these error recovery methods.

### 9.3.2 Checking and Re-Running Erroneous GUI Operations

If the error was due to an erroneous GUI operation, such as a wrong setting or operational mistake, perform the operation again, as indicated by the error message displayed in the processing results window. To check the information in an error message, see the *Hitachi AMS/WMS Error Codes*. You can use the message ID to locate the relevant message, and check the message particulars.

### 9.3.3 Checking System Messages

From the system message ID, you can identify the program in which the error occurred. From the message text, you can see what caused the error. For details on the appropriate action in response to a particular system message, see the NAS Manager Error Codes. You can use the message ID to locate the relevant message, and find out how to recover from the error.

### 9.3.4 Viewing Error Data in the Browse Cluster Status Window

In the event of an error in the failover, check the error status of the affected cluster, nodes, and resource groups in the **Browse Cluster Status** window and perform the necessary recovery action with your HDS representative. For more information on viewing the status of a cluster, node, or resource group, see section 4.5.7.

To identify the error in the failover, you must confirm the recovery method indicated in Table 9.5 to Table 9.7, according to the status of the cluster, nodes, and resource groups that were checked in the **Browse Cluster Status** window. Also, confirm the instructions of your HDS representative, then specify the recovery procedure from Table 9.5 to Table 9.7.

To view the status of a cluster, see **Cluster status** in the **Browse Cluster Status** (Cluster / Node Status) window. The table below summarizes the error recovery procedure for each of the cluster statuses displayed in this window.

**Table 9.5 Error Recovery Procedures for Cluster Statuses**

| Cluster Status | Recovery Procedure | See |
|---|---|---|
| ACTIVE | Running normally. No recovery action is required. | — |
| INACTIVE | Start the stopped cluster. | — |
| UNKNOWN | Fix the problem that occurred at NAS OS startup.<br>Stop both nodes and fix the problem.<br>Stop both nodes and replace the program. | 9.3.5 |
| | Restart the NAS OS on both NAS units in the cluster. | 9.3.6 |
| | Restart the NAS OS on bothNAS units in the cluster, while degenerated operation is in progress following the failover. | 9.3.6 |

***Note:*** After stopping a node or performing a forced stop of a node, if the **Browse Cluster Status** (Cluster / Node Status) window is displayed while the stopped node is being logged in to, then UNKNOWN is displayed for the status of the cluster and the other node. In such a case, you cannot check the status of the cluster and the other node. To check the status of the cluster and the other node, log in to the running node (the other node), and then check the **Browse Cluster Status** (Cluster / Node Status) window.

To view the status of a node, see **Node status** in the **Browse Cluster Status** (Cluster / Node Status) window. The table below summarizes the error recovery procedure for each of the node statuses displayed in this window.

**Table 9.6 Error Recovery Procedures for Node Statuses**

| Node Status | Recovery Procedure | See |
|---|---|---|
| UP | Running normally. No recovery action is required. | — |
| INACTIVE | Start the stopped node. | — |
| DOWN | Restart the NAS OS on the NAS Unit for the failed node, while continuing degenerated operation following the failover. | 9.3.8 |
| | Replace the program without stopping services, while continuing degenerated operation following the failover. | 9.3.9 |
| | Stop both nodes and replace the program. | 9.3.10 |
| UNKNOWN | Stop both nodes and fix the problem. | 9.3.10 |
| | Stop and recover the node where the error occurred, while continuing degenerated operation following the failover. | 9.3.7 |
| | Restart the NAS OS on the NAS Unit for the failed node, while continuing degenerated operation following the failover. | 9.3.8 |
| | Fix the hardware or software error that occurred on both nodes at NAS OS startup.<br>Stop both nodes and replace the program. | 9.3.10 |

| | | |
|---|---|---|
| | Fix the hardware or software error that occurred on either node at NAS OS startup. | 9.3.11 |
| | Restart the NAS OS on both NAS Units in the cluster. | 9.3.12 |

To view the status of a resource group, see **Resource group status** in the **Browse Cluster Status** (Resource Group Status) window. The resource group status and error information are displayed in the following form:

*resource-group-status*/*error-information*

The table below summarizes the error recovery procedure for each of the displayed resource group statuses.

**Table 9.7 Error Recovery Procedures for Resource Group Statuses**

| Resource Group Status | Recovery Procedure | See |
|---|---|---|
| Online | See the resource group error information. | Table 9.8 |
| Online Maintenance | See the resource group error information. | Table 9.8 |
| Online Pending | The resource group is starting. No recovery action is required. | — |
| Online Ready | Stop both nodes and replace the program. | 9.3.10 |
| | The cluster was stopped at NAS OS shutdown. Fix the error at the next session. | 9.3.13 |
| | The node was stopped when the turning the power of NAS Modular system. Fix the error at the next session.<br>Restart the failover only at the node where the error occurred. | 9.3.14 |
| | Restart only the node where the error occurred. | 9.3.15 |
| | Start the resource group when the cluster is running normally. | 9.3.26 |
| Offline | See the resource group error information. | Table 9.8 |
| Offline Pending | The resource group is stopping. No recovery action is required. | — |
| Discovery (exclusivity) | Online processing is being performed for the resource group before operations begin. No recovery action is required. | — |
| Initializing | The resource group is initializing. No recovery action is required. | — |
| Internal Error | See the resource group error information. | Table 9.8 |

The table below summarizes the error recovery procedures for the displayed resource group error information.

**Table 9.8 Error Recovery Procedures for Resource Group Errors**

| Error Information | Recovery Procedure | See |
|---|---|---|
| No error | Running normally. No recovery action is required. | — |
| Internal error - not recoverable | Fix the error on the node that failed to start at NAS OS startup in the cluster. | 9.3.16 |
| | Your HDS representative must replace the hardware. | 9.3.17 |
| | Restart the resource group where the error occurred. | 9.3.18 |
| | Restart the NAS OS on the NAS Unit running the resource group in which the error occurred. | 9.3.19 |
| | Restart the NAS OS on the node running the resource group in which the error occurred. | 9.3.20 |
| | Stop only the node where the error occurred and replace the program. | 9.3.21 |
| | Stop both nodes and replace the program. | 9.3.22 |
| Monitor activity unknown | Stop both nodes and replace the program. | 9.3.22 |
| | Take action to restore services as soon as possible, and replace the program at a later date. | 9.3.24 |
| No available nodes or No available nodes in failure domain after monitor failure | If the error occurred in a resource group that was failed over to the alternate node in a cluster, and the original resource group is still active on that node, fix the error and then restart services on the original node. | 9.3.17 |
| | If the error occurred in a resource group that was failed over to the alternate node in a cluster, and the original resource group on that node has been switched to the other node, fix the error and then restart the services of the failed resource group. | 9.3.25 |
| Node unknown | Restart the node running the resource group in which the error occurred. | 9.3.19 |
| | Restart the NAS OS on the NAS Unit running the resource group in which the error occurred. | 9.3.20 |
| | Stop only the node where the error occurred and replace the program. | 9.3.21 |
| | Stop both nodes and replace the program.<br>Stop both nodes and fix the problem.<br>Fix the hardware error that occurred on both nodes at NAS OS startup.<br>Stop the node where the error occurred at NAS OS startup and replace the program on the node. | 9.3.22 |
| Split resource group (exclusivity) | Fix the error that occurred at NAS OS startup.<br>Take action to restore the services provided by the resource group as soon as possible, and replace the program at a later date. | 9.3.23 |
| | Stop both nodes and replace the program. | 9.3.22 |

| Error Information | Recovery Procedure | See |
|---|---|---|
| `srmd executable error` | Stop both nodes and fix the problem. | 9.3.5 |
| `srmd executable error` | Restart the NAS OS on the node where the error occurred, while continuing degenerated operation following the failover. | 9.3.8 |
| | Restart the NAS OS on the NAS Unit for the failed node, while continuing degenerated operation following the failover. | 9.3.10 |
| | Fix the hardware or software error that occurred on either node at NAS OS startup. | 9.3.11 |
| | Restart the NAS OS on both NAS Units in the cluster. | 9.3.12 |

The recovery procedure for each of these errors is described below.

### 9.3.5 Recovery Procedure 1

1. Perform a forced stop for the cluster. For details, see section 4.5.6.
2. Request your HDS representative to restart the NAS OS on both NAS Units in the cluster.

   Consult with your HDS representative for details on error recovery operations, then ask them to restart the NAS OS after the maintenance is complete. If an error occurs in the switch (if the switch is not turned on), you do not have to ask your HDS representative to restart the NAS OS.
3. Start the cluster. For details, see section 4.5.4.

### 9.3.6 Recovery Procedure 2

1. Perform a forced stop for the cluster. For details, see section 4.5.6.
2. Restart the NAS OS on both NAS Units in the cluster.

   Use Storage Navigator Modular to restart the NAS OS. See the manual *Storage Navigator Modular User's Guide*.
3. Start the cluster. See section 4.5.4.

### 9.3.7 Recovery Procedure 3

1. Request your HDS representative to start the NAS OS on the repaired NAS Unit.

   Consult with your HDS representative for details on error recovery operations, then ask them to restart the NAS OS after the maintenance is complete.
2. Fail back the resource group to the original node. For details, see section 4.5.11.

### 9.3.8 Recovery Procedure 4

1. Restart the NAS OS on the NAS Unit where the error occurred.

   Use Storage Navigator Modular to restart the NAS OS. See the manual *Storage Navigator Modular User's Guide*.

2. Fail back the resource group to the original node. See section 4.5.11.

### 9.3.9 Recovery Procedure 5

1. Request your HDS representative to start the NAS OS on the repaired NAS Unit.

   Consult with your HDS representative for details on error recovery operations, then request them to restart the NAS OS after the maintenance is complete.

2. Change the execution node of both resource groups. For details, see section 4.5.11.

3. Ask your HDS representative to restart the NAS OS on the other NAS Unit in the cluster.

   Consult with your HDS representative for details on error recovery operations, then ask them to restart the NAS OS after the maintenance is complete.

4. Fail back the resource group to the original node. For details, see section 4.5.11.

### 9.3.10 Recovery Procedure 6

1. Perform a forced stop for the cluster. For details, see section 4.5.6.

2. Ask your HDS representative to restart the NAS OS on the NAS Unit from the active node.

   Consult with your HDS representative for details on error recovery operations, then ask them to restart the NAS OS after the maintenance is complete.

3. Start the cluster. For details, see section 4.5.4.

### 9.3.11 Recovery Procedure 7

1. Perform a forced stop for the node where the error occurred. For details, see section 4.5.6.

2. Ask your HDS representative to restart the NAS OS on the NAS Unit where the error occurred.

   Consult with your HDS representative for details on error recovery operations, then ask them to restart the NAS OS after the maintenance is complete.

3. Start the repaired node. For details, see section 4.5.5.

### 9.3.12 Recovery Procedure 8

1. Perform a forced stop for the cluster. For details, see section 4.5.6.
2. Shut down the NAS OS on the NAS Unit from the active node.

   Use Storage Navigator Modular to shut down the NAS OS. See the manual *Storage Navigator Modular User's Guide*.
3. Start the NAS OS on both NAS Units in the cluster.
4. Start the cluster if it is in `INACTIVE` status. For details, see section 4.5.4.

   The system administrator can use Storage Navigator Modular to restart the NAS OS. For details on how to do this, see the manual *Storage Navigator Modular User's Guide*.
5. Start the cluster if it is in `INACTIVE` status. For details, see section 4.5.4.

### 9.3.13 Recovery Procedure 9

Start the cluster. For details, see section 4.5.4.

### 9.3.14 Recovery Procedure 10

Start the node. For details, see section 4.5.5.

### 9.3.15 Recovery Procedure 11

Restart the NAS OS on the NAS Unit where the error occurred.

Use Storage Navigator Modular to restart the NAS OS. See the manual *Storage Navigator Modular User's Guide*.

### 9.3.16 Recovery Procedure 12

1. Perform a forced stop for the resource group where the error occurred. For details, see section 4.5.9.
2. Stop the node where the error occurred. For details, see section 4.5.5.
3. Start the resource group that was running on the node where the error occurred. For details, see section 4.5.8.
4. Ask your HDS representative to start the NAS OS on the repaired NAS Unit.

   Consult with your HDS representative for details on error recovery operations, then ask them to restart the NAS OS after the maintenance is complete.
5. Start the repaired node. For details, see section 4.5.5.
6. Fail back the resource group to the original node. For details, see section 4.5.11.

### 9.3.17 Recovery Procedure 13

1. Perform a forced stop for the resource group that was running on the node where the error occurred. For details, see section 4.5.9.
2. Restart the NAS OS on the NAS Unit where the error occurred.

   Use Storage Navigator Modular to restart the NAS OS. See the manual *Storage Navigator Modular User's Guide*.
3. Start the resource group. For details, see section 4.5.8.

### 9.3.18 Recovery Procedure 14

1. Perform a forced stop for the resource group where the error occurred. For details, see section 4.5.9.
2. Start the resource group. For details, see section 4.5.8.

### 9.3.19 Recovery Procedure 15

1. Perform a forced stop for the resource group where the error occurred. For details, see section 4.5.9.
2. Stop the node. For details, see section 4.5.5.
3. Start the node. For details, see section 4.5.5.
4. Start the resource group. For details, see section 4.5.8.

### 9.3.20 Recovery Procedure 16

1. Perform a forced stop for the resource group where the error occurred. For details, see section 4.5.9.
2. Stop the node. For details, see section 4.5.5.
3. Restart the NAS OS on the NAS Unit for the stopped node.

   Use Storage Navigator Modular to restart the NAS OS. See the manual *Storage Navigator Modular User's Guide*.
4. Start the node. See section 4.5.5.
5. Start the resource group. See section 4.5.8.

### 9.3.21 Recovery Procedure 17

1. Perform a forced stop for the resource group where the error occurred. For details, see section 4.5.9.
2. Stop the node on which the error occurred. For details, see section 4.5.5.
3. Request your HDS representative to restart the NAS OS on the node.

Consult with your HDS representative for details on error recovery operations, then ask them to restart the NAS OS after the maintenance is complete.

4. Start the node. For details, see section 4.5.5.
5. Start the resource group. For details, see section 4.5.8.
6. Fail over the resource group on the other node in the cluster. For details, see section 4.5.11.
7. Stop the other node mentioned in Step 6. For details, see section 4.5.5.
8. Ask your HDS representative to restart the NAS OS on the other NAS Unit in the cluster.

   Your HDS representative must start the NAS OS after the maintenance is complete.
9. Start this node. For details, see section 4.5.5.
10. Fail back the resource group to the original node. For details, see section 4.5.11.

### 9.3.22 Recovery Procedure 18

1. Perform a forced stop for the resource group where the error occurred. For details, see section 4.5.9.
2. Stop the other resource group in the cluster. For details, see section 4.5.8.
3. Stop the cluster. For details, see section 4.5.4.
4. Ask your HDS representatiave to restart the NAS OS on both NAS Units in the cluster.

   Use Storage Navigator Modular to restart the NAS OS. See the *Storage Navigator Modular User's Guide*.
5. Start the cluster. See section 4.5.4.
6. Start both resource groups. See section 4.5.8.

### 9.3.23 Recovery Procedure 19

1. Perform a forced stop for the resource group where the error occurred. For details, see section 4.5.9.
2. Stop the other resource group in the cluster. For details, see section 4.5.8.
3. Stop the cluster. For details, see section 4.5.4.
4. Restart the NAS OS on both NAS Units in the cluster. The system administrator can use Storage Navigator Modular to restart the NAS OS. For details, see the manual for Storage Navigator Modular.
5. Start the cluster. For details, see section 4.5.4.
6. Start the resource groups on both nodes. For details, see section 4.5.8.

### 9.3.24 Recovery Procedure 20

1. Monitor the resource group. For details, see section 4.5.10.
2. Disable resource group monitoring. For details, see section 4.5.10.
3. Repeat steps 1 and 2.

### 9.3.25 Recovery Procedure 21

1. Perform a forced stop for the resource group where the error occurred. For details, see section 4.5.9.
2. Stop the failover node to which the resource group was relocated. For details, see section 4.5.5.
3. Ask your HDS representative to restart the NAS OS on the repaired NAS Unit (failover source) for the stopped node.

   Consult with your HDS representative for details on error recovery operations, then ask them to restart the NAS OS after maintenance is complete.
4. Start the repaired failover node. For details, see section 4.5.5.
5. Change the execution node on which the active resource group runs. For details, see section 4.5.11.
6. Stop the original node from which the resource group was relocated.
7. Ask your HDS representative to restart the NAS OS on the repaired NAS Unit (failover target) for the stopped node.
8. Start the original node.
9. Start the resource group on the original node. For details, see section 4.5.8.

### 9.3.26 Recovery Procedure 22

Start the resource group. For details, see section 4.5.8.

### 9.3.27 Manual Failover and Failback

When maintenance or error recovery of a NAS Unit is required, you must perform a failover and failback manually from the **Browse Cluster Status** (Resource Group Status) window as instructed by your HDS representative. On receiving instructions to proceed, fail over the resource group in which services are active. After verifying that maintenance performed by your HDS representative has finished, fail back the resource group to the original node. For details on manual failover and failback to recover from error, see section 9.3.4:

- **Manual failover** involves relocating one resource group to the other node when resource groups are running on separate nodes in the cluster. The purpose of this operation is to ensure that the services provided by the resource group remain continuously available when maintenance or error recovery is required at a node.

- **Manual failback** means migrating a failed-over resource group from the node where both resource groups are running to the original node. The purpose of this operation is to restore the failed-over resource group on its original node after error recovery has finished.

If an unrecoverable error occurs during manual failover or failback, see section 9.3.4.

### 9.3.28 Replacing NAS Manager

If you are responsible for program management, replace the failed NAS Manager. For details on replacement procedures, see section 8.2.

### 9.3.29 Recovering from File System Errors

This subsection describes the actions that you need to take to recover from errors in a file system operated by NAS Manager.

For details about the appropriate action to take when an error occurs in a file system used by the NAS Sync Image differential-data snapshot function, or in the differential-data snapshot itself, see the manual *NAS Sync Image Modular User's Guide*.

If an error occurs in a file system operated by NAS Manager, the recovery procedure differs depending on the cause of the error.

When **Device status** is `Normal` and **Mount status** is `Fatal error`:

The file system is blocked due to an error in the NAS OS.

Check whether automatic failover in the event of file system blockage has been enabled.

- When the automatic failover functionality is enabled:
- When the automatic failover functionality is not enabled:

  Take action according to the procedure described in 9.3.29.2.

When **Device status** is `Error` and **Mount status** is `Fatal error`:

The file system is blocked due to an error in a device file (multiple errors on a drive).

Confirm that the automatic failover functionality for file system blockage has been enabled.

- When the automatic failover functionality is enabled:

  Take action according to the procedure described in 9.3.29.3
- When the automatic failover functionality is not enabled:

  Take action according to the procedure described in 9.3.29.4.

If the cause of the error cannot be determined, follow the instructions provided by the maintenance personnel.

We recommend that you regularly back up data for the NAS Modular system in case of failure. The following describes how to restore a file system, assuming that there is backup data available (stored in a medium other than the NAS Modular subsystem).

### 9.3.29.1 When the file system is blocked due to an error in the NAS OS

When the file system is blocked due to an error in the NAS OS if the automatic failover functionality has been enabled. The following describes how to restore a file system that is blocked due to an error in the NAS OS.

To restore the file system by working with maintenance personnel:

1. Record the setting information for the file share and file system at the failover target node.

   If a file share has been created in the blocked file system, record the file share setting information displayed in the **List of File Shares** window so that the file share can be re-created after the file system is restored.

   ***Note:*** You might not be able to view setting information for the NFS shares when a file system cannot be mounted at the failover target.

   Also, record the file system setting information displayed in the **List of File Systems** window in order to reconfigure the file system after the NAS OS is restarted.

2. Perform a failback for the resource group to the original node.

3. Check the status of the resource group to which the blocked file system belongs.

   You can check the status of the resource group in the **Browse Cluster Status** (Resource group status) window.

   - If the status of the resource group is `Online / No error`:

     Go to step 4.

   - If the status of the resource group is `Offline / No error`:

     Go to step 8.

   - If the status of the resource group is neither `Online / No error` nor `Offline / No error`:

     Perform a forced stop for the resource group, and then go to step 8.

4. Notify the end users that the file share service will stop.

5. Check whether the blocked file system is mounted.

   In the **List of File Systems** window, check whether the blocked file system is mounted.

6. Delete the file share.

   In the **List of File Shares** window, delete the file shares on the blocked file system.

   If the file system in step 5 was mounted:

   Delete the NFS and CIFS shares, and then go to step 7.

   If the file system in step 5 was not mounted:

   Delete the CIFS share, and then go to step 8.

7. Unmount the file system.

   In the **List of File Systems** window, unmount the blocked file system..

8. Delete the file system.

In the **List of File Systems** window, delete the blocked file system.

9. Perform a manual failover of the resource group on the node.
10. Stop the node.
11. Ask the maintenance personnel to restart the NAS OS on the NAS Unit for the stopped node.
12. Start the stopped node.
13. Perform a failback for the resource group to the original node.
14. For the other node in the cluster, perform step 9 to step 13.
15. Re-create the file system.
16. Using the file system settings information recorded in step 1, re-create the file system. Remount the file system.
17. Restore the backup data to the re-created file system.
18. Re-create the NFS share and CIFS share as required.

    You must select **Do not create / change** for **Directory creation / change** in each of the file share creation windows because the file system is restored by using the backup data.

#### 9.3.29.2 When the file system is blocked due to an error in the NAS OS (When the automatic failover functionality has not been enabled)

The following describes how to restore a file system that is blocked due to an error in the NAS OS.

To restore the file system by working with maintenance personnel:

1. Record the setting information for the file share and file system.

   If a file share has been created in the blocked file system, record the file share setting information so that the file share can be re-created after the file system is restored.

   Also, record the file system setting information in order to reconfigure the file system after the NAS OS is restarted.
2. Ask the maintenance personnel to collect the error information.

   A failover of the resource group starts along with the collection of the error information.
3. Perform a failback for the resource group to the original node.
4. Check the status of the resource group to which the blocked file system belongs.

   You can check the status of the resource group in the **Browse Cluster Status** (Resource group status) window.

   - If the status of the resource group is `Online / No error`:

     Go to step 5.
   - If the status of the resource group is `Offline / No error`:

     Go to step 9.

- If the status of the resource group is neither `Online / No error` nor `Offline / No error`:

  Perform a forced stop for the resource group, and then go to step 9.

5. Notify the end users that the file share service will stop.
6. Check whether the blocked file system is mounted.

   In the **List of File Systems** window, check whether the blocked file system is mounted.
7. Delete the file share.

   In the **List of File Shares** window, delete the file shares on the blocked file system.

   If the file system in step 6 was mounted:

   Delete the NFS and CIFS shares, and then go to step 8.

   If the file system in step 6 was not mounted:

   Delete the CIFS share, and then go to step 9.
8. Unmount the file system.

   In the **List of File Systems** window, unmount the blocked file system. Delete the file system.

   In the **List of File Systems** window, delete the blocked file system.
9. Perform a manual failover of the resource group on the node.
10. Stop the node.
11. Ask the maintenance personnel to restart the NAS OS on the NAS Unit for the stopped node.
12. Start the stopped node.
13. Perform a failback for the resource group to the original node.
14. For the other node in the cluster, perform step 10 to step 14.
15. Re-create the file system.

    Using the file system settings information recorded in step 1, re-create the file system. Remount the file system.
16. Restore the backup data to the re-created file system.
17. Re-create the NFS share and CIFS share as required.

    You must select **Do not create / change** for **Directory creation / change** in each of the file share creation windows because the file system is restored by using the backup data.

#### 9.3.29.3 When the File System is Blocked due to an error in a Device File (When the automatic Failover Functionality has been Enabled)

The following describes how to restore a file system that is blocked due to an error in a device file when the automatic failover functionality has been enabled:

1. Identify the device file and file system in which the error has occurred.

2. In the **List of File Systems** window, from **Device files** and **File system (used by)**, identify the device file and file system in which the error has occurred. Perform a failback for the resource group, which failed over automatically when the file system was blocked, to the original node.
3. Check the status of the resource group to which the blocked file system belongs.

   You can check the status of the resource group in the **Browse Cluster Status** (Resource group status) window.

   - If the status of the resource group is `Online / No error`:

     Go to step 4.
   - If the status of the resource group is `Offline / No error`:

     Go to step 7.
   - If the status of the resource group is neither `Online / No error` nor `Offline / No error`:

     Perform a forced stop for the resource group, and then go to step 7.
4. Notify the end users that the file share service will stop.
5. Record the file share settings information.

   If a file share has been created on the blocked file system, record the file share settings information. This information will be used when the file share is re-created after the device file has been replaced.

   ***Note:*** You might not be able to view setting information for the NFS shares when a file system cannot be mounted on the original node.
6. Delete the file shares.

   In the **List of File Shares** window, delete the CIFS share on the blocked file system. For details on how to delete a CIFS share, see 4.11.2.7. For details on how to delete an NFS share, see 4.11.1.6.
7. Record the file system settings information.

   Since you will need to re-create the blocked file system after the device file has been replaced, record the file system settings information.
8. Delete the file system.

   In the **List of File Systems** window, delete the blocked file system.
9. Perform a manual failover of the resource group.

   When requested to do so by maintenance personnel, perform a manual failover of the resource group that was using the failed device file.
10. Stop the cluster.
11. Ask maintenance personnel to stop the NAS OS on the NAS Units in the cluster.
12. Ask maintenance personnel to replace the device file.
13. Ask maintenance personnel to start the NAS OS on the NAS Units in the cluster.
14. Start the cluster. For details on starting the cluster, see 4.5.4.

15. Re-create the file system.

    Using the file system settings information recorded in step 5, re-create the file system. Remount the file system.

16. Restore the backup data to the re-created file system.

17. Re-create the file share.

    You must select **Do not create/change** for **Directory creation/change** in each of the file share creation windows because the file system is restored by using the backup data.

#### 9.3.29.4 When the File System is Blocked due to an error in a Device File (when the automatic failover functionality has not been enabled)

The following describes how to restore a file system that is blocked due to an error in a device file when the automatic failover functionality has been disabled:

1. Identify the device file and file system in which the error has occurred.

   In the **List of File Systems** window, from **Device files** and **File system (used by)**, identify the device file and file system in which the error has occurred.

2. Check the status of the resource group to which the blocked file system belongs.

   You can check the status of the resource group in the **Browse Cluster Status** (Resource group status) window.

   - If the status of the resource group is `Online / No error`:

     Go to step 3.

   - If the status of the resource group is `Offline / No error`:

     Go to step 6.

   - If the status of the resource group is neither `Online / No error` nor `Offline / No error`:

3. Notify the end users that all services will stop.

4. Record the file share settings information.

   If a file share has been created on the blocked file system, record the file share settings information. This information is used when the file share is re-created after the device file has been replaced.

5. Delete the file share.

   In the **List of File Shares** window, delete the file share on the blocked file system.

6. Record the file system settings information.

   Since you will need to re-create the blocked file system after the device file has been replaced, record the file system settings information.

7. Unmount the file system.

   In the **List of File Systems** window, unmount the blocked file system.

8. Delete the file system.

In the **List of File Systems** window, delete the blocked file system. For details on deleting a file system, see 4.10.7.

9. Stop the cluster. For details on stopping the cluster, see 4.5.4.
10. Ask maintenance personnel to stop the NAS OS on the NAS Units in the cluster.
11. Ask maintenance personnel to replace the device file.
12. Ask maintenance personnel to start the NAS OS on the NAS Units in the cluster.
13. Start the cluster. For details on starting the cluster, see 4.5.4.
14. Re-create the file system.

    Using the file system settings information recorded in step 6, re-create the file system. For details on creating a file system, see 4.10.3.
15. Remount the file system. For details on mounting a file system, see 4.10.4.
16. Restore the backup data to the re-created file system.
17. Re-create the file share.

    You must select **Do not create/change** for **Directory creation/change** in each of the file share creation windows because the file system is restored by using the backup data.

### 9.3.30 Checking Error Information in the List of File Systems Window

If an error occurs with a file system or device file, you need to check the error status of the file system or device file in the **List of File Systems** window, and work with your HDS representative to recover from the error.

By checking the system messages around the time that the error occurred, and viewing the **Mount status** and **Device status** items in the **List of File Systems** window to check the error status of the file system and device file, you can determine the cause of the error.

- When **Device status** is normal and Mount status is fatal error:

  The file system is blocked due to an error in the NAS OS.
- When **Device status** is error and Mount status is fatal error:

  The file system is blocked due to an error in a device file.

Check the error status of the file system or device file, and then take action according to the cause of the error.

When the file system is blocked due to an error in the NAS OS:

Take action according to the procedure described in section 9.3.7.

If you are using NAS Backup Restore snapshot, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

When the file system is blocked due to an error in a device file:

Contact your HDS representative to check whether a hardware error has occurred. If multiple errors have occurred on a drive, take action according to the procedure described in 9.3.7.

If you are using NAS Backup Restore, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*. If you are using NAS Sync Image, see the *Hitachi AMS/WMS NAS Sync Image User's Guide*

If the cause of the error is not multiple errors on a drive, follow the instructions provided by your HDS representative.

The following describes how to restore the file system, assuming that the file system data has been backed up to a tape device:

**When the File System is Blocked Due to a NAS OS Error**

The following describes how to restore a file system that is blocked due to an error in the NAS OS:

To restore the file system by working with your HDS representative:

1. Save the setting information on the file share and file system.

   If a file share has been created in the file system where an error occurred, save the file share setting information displayed in the **List of File Systems** window so that the file share can be re-created after the file system is restored.

   Also, save the file system setting information displayed in the **List of File Systems** window in order to reconfigure the file system after the NAS OS is restarted.

2. Collect the NAS dump. A failover of the resource group is usually accompanied by the collection of the NAS dump.

   Use Web to collect a NAS dump. For more information, see the documentation for the disk array.

3. Perform a failback for the resource group to the original node.

   For details about performing failback of a resource group, see section 4.5.11.

4. Check whether the blocked file system is mounted.

   In the **List of File Systems** window, check whether the blocked file system is mounted.

5. Delete the file share.

   In the **List of File Shares** window, delete the file share on the failed file system.

   If the file system in step 4 was mounted:

   Delete the NFS and CIFS shares, and then go to step 6.

   If the file system in step 4 was not mounted:

   Delete the CIFS share, and then go to step 7.

   For details about how to delete file shares, see section 4.11.1.

6. Unmount the file system.

   In the **List of File Systems** window, unmount the failed file system. For details about how to unmount file systems, see section 4.10.5.

For details about how to unmount a file system or snapshot used with the NAS Backup Restore snapshot function, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

For details about how to unmount a file system or differential-data snapshot used in NAS Sync Image, see the *Hitachi AMS/WMS NAS Sync Image User's Guide*.

7. Delete the file system.

   In the **List of File Systems** window, delete the failed file system.

   For details about how to delete file systems, see section 4.10.9.

8. Perform a manual failover of the resource group on the node.
9. Stop the node.

   For details on stopping a node, see section 4.5.5.

10. Restart the NAS OS on the stopped node.

    Use Storage Navigator Modular to restart the NAS OS. For more information, see the *Storage Navigator Modular User's Guide*.

11. Start the stopped node.

    For details on starting a node, see section 4.5.5.

12. Perform a failback for the resource group to the original node.

    Perform a failback for the resource group to the original node. For details about performing failback of a resource group, see section 4.5.11.

13. For the other node in the cluster, perform step 8 to step 12.
14. Recreate the file system.

    Using the file system settings information recorded in step 1, re-create the file system.

    For details about how to create a file system, see section 4.10.4.

    For details about how to create a file system or snapshot used with the NAS Backup Restore snapshot function, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

    For details about how to create a file system or differential-data snapshot used in NAS Sync Image, see the *Hitachi AMS/WMS NAS Sync Image User's Guide*.

15. Remount the file system.

    For details on how to mount a file system, see section 4.10.6.

16. Restore the backup data for the re-created file system.
17. Recreate the NFS share and CIFS share as required.

    For details about how to create a file share, see section 4.10.5.2.

    You must select **Do not create / change for Directory creation / change** in each of the file share creation windows because the file system is restored by using the backup data.

**When the File System is Blocked Due to a Device File Error**

The following procedure shows how to correct a file system that is blocked due to an error in a device file.

To restore a file system that is blocked due to an error in a device file:

1. Check the status of the resource group of the node to which the blocked file system belongs.

   You can check the status of the resource group in the **Browse Cluster Status** (Resource group status) window.

   - If the status of the resource group is Online / No error:

     Go to step 2.

   - If the status of the resource group is Offline / No error:

     Go to step 5.

   - If the status of the resource group is neither Online / No error nor Offline / No error:

     Perform a forced stop for the resource group, and then go to step 5. For details on performing a forced stop for a resource group, see section 4.5.9.

2. Notify end users that the file share service will stop.

   Check the file system for which the file share is created in the **List of File Shares** window, and notify the end users using the NAS Modular system that the file share service will stop. For details about how to view the **List of File Shares** window, see section 4.11.1.

3. Record the file share settings information.

   If a file share has been created on the blocked file system, record the file share settings information displayed in the **List of File Shares** window. This information will be used when the file share is re-created after the disk is replaced.

4. Delete the file share.

   In the **List of File Shares** window, delete the file share on the blocked file system. For details about how to delete file shares, see section 4.11.1.

5. Record the file system settings information.

   Since you will need to re-create the failed file system after the device file has been replaced, record the file system settings information displayed in the **List of File Systems** screen.

   If the status of the resource group is not Online / No error in step 1, go to step 7.

6. Unmount the file system.

   In the **List of File Systems** window, unmount the failed file system. For details about how to unmount file systems, see section 4.10.5.

   For details about how to unmount a file system or snapshot used with the NAS Backup Restore snapshot function, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

   For details about how to unmount a file system or differential-data snapshot used in NAS Sync Image, see the *Hitachi AMS/WMS NAS Sync Image User's Guide*.

7. Delete the file system.

   In the **List of File Systems** window, delete the failed file system.

   If the status of the resource group is not Online / No error in step 1, delete the file system and go to step 7.

   For details about how to delete file systems, see section 4.10.7.

For details about how to delete a file system or snapshot used with the NAS Backup Restore snapshot function, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

For details about how to delete a file system or differential-data snapshot used in NAS Sync Image, see the *Hitachi AMS/WMS NAS Sync Image User's Guide*.

8. Perform a manual failover of the resource group.

   When indicated to do so by your HDS representative, perform a manual failover of the resource group that was using the device file to be replaced.

9. Stop the node that was using the device file where the error occurred.

   For details about how to stop a node, see section 4.5.5.

10. Ask your HDS representative to Restart the NAS OS on the stopped node.

    For details on how to restart the NAS OS, see section 4.5.12.

11. Start the node for which the NAS OS was restarted.

    For details about how to start a node, see section 4.5.5.

12. Perform a failback for the resource group to the original node or start the resource group on the original node.

    - If the status of the resource group is Online / No error in step 1:

      Perform a failback for the resource group to the original node.

    - If the status of the resource group is not Online / No error in step 1:

      Start the resource group on the original node. For details on starting a resource group, see section 4.5.8.

      Also, if a CIFS share has been created in the failed file system, delete that CIFS share. For details on deleting a CIFS share, see section 4.11.12.

13. Identify and replace the disk where the error occurred.

    For details on how to identify and replace the disk where an error occurred, see the *Hitachi AMS/WMS Storage Navigator Modular Graphical User Interface (GUI) User's Guide* (MK-95DF711).

14. Recreate the file system.

    Using the file system settings information recorded in step 5, re-create the file system.

    For details about how to create a file system, see section 4.10.5.

    For details about how to create a file system or snapshot used with the NAS Backup Restore snapshot function, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

    For details about how to create a file system or differential-data snapshot used in NAS Sync Image, see the *Hitachi AMS/WMS NAS Sync Image User's Guide*.

15. Remount the file system.

    For details on how to mount a file system, see section 4.10.6.

16. Restore the backup data for the recreated file system.

17. Recreate the file share.

    For details about how to create a file share, see section 4.11.

You must select **Do not create / change for Directory creation / change** in each of the file share creation windows because the file system is restored by using the backup data.

### 9.3.31 Checking Error Information (List of Interfaces Window)

If an error occurs in the interface or network, a system administrator checks the status of the error in the **List of Interfaces** window and recovers the error by working with your HDS representative as necessary.

#### 9.3.31.1 Recovering from an 'Unknown' Error

This section describes the actions to take when, among the nodes configuring a cluster, Unknown is displayed in the display item for a node to which a user is not currently logged on (in the **List of Interfaces** window).

- **Check whether the NAS OS is running**

  Among the nodes in the cluster, check whether the NAS OS is running on any NAS Unit to which you are not currently logged on. If the NAS OS is not running, start it. Use Storage Navigator Modular to start the NAS OS. For more information, see the manual *Storage Navigator Modular User's Guide*.

  After starting the NAS OS, recheck the interface and network information in the **List of Interfaces** window.

- **Check the MTU value for the management LAN Port (mng1)**

  Check whether the MTU value for eth1 is specified correctly. If the specified value is incorrect, specify the correct value. For details on checking and specifying an MTU value, see the manual for Storage Navigator Modular.

  After specifying the correct value for the MTU value, recheck the interface and network information in the **List of Interfaces** window.

- **Check the IP address for the management LAN (mng1)**

  Check whether the fixed IP address and netmask for eth1 are specified correctly. If the specified values are incorrect, specify the correct values. For details on checking and specifying a fixed IP address, see the manual for Storage Navigator Modular.

  After specifying the correct values for the fixed IP address and netmask, recheck the interface and network information in the **List of Interfaces** window.

- **Check communication devices, such as hubs**

  Make sure that there are no problems with communication devices such as hubs. If a problem exists in a communication device such as a hub, remove the problem and recheck the interface and network information in the **List of Interfaces** window.

If Unknown is still displayed in the **List of Interfaces** window, contact your HDS representative.

### 9.3.31.2 Recovering from an 'Invalid' Error (mng1)

This section describes the actions to take when, among the nodes configuring a cluster, `Invalid` is displayed in the display item for mng1 on the node to which a user is not currently logged on (in the **List of Interfaces** window).

- **Check whether the MTU values are the same for both nodes**

  If Invalid is displayed in the display item for the MTU value, log on to the node for which Invalid is displayed, display the **List of Interfaces** window, and then check whether the MTU values are the same for both nodes. If the MTU values are different, specify the same value for both nodes. For details on specifying the MTU value, see the manual *Storage Navigator Modular User's Guide*.

- **Check the settings for IP addresses**

  If `Invalid` is displayed in the display items for the fixed IP address, or netmask, make sure the settings for the fixed IP address, and netmask are correct. If the specified value is incorrect, specify the correct value. For details on checking and specifying a fixed IP address, see the manual *Storage Navigator Modular User's Guide*.

If `Invalid` is still displayed in the **List of Interfaces** window, contact your HDS representative.

### 9.3.31.3 Recovering from an 'Invalid' Error (other than mng1)

When, among the nodes configuring a cluster, `Invalid` is displayed (in the **List of Interfaces** window) in the display item for the data LAN (other than mng1) on the node to which a user is not currently logged on, delete all interfaces for which `Invalid` is displayed. Then specify the correct value and add a new interface.

For details on:

- Adding an interface, see section 4.7.4.3.
- Deleting an interface, see section 4.7.4.5.

If `Invalid` is still displayed in the **List of Interfaces** window, contact your HDS representative.

### 9.3.32 Checking Error Information on Trunking

If an error occurs in the trunking settings, a system administrator checks the status of the error in the **List of Trunking Configurations** window, and then recovers the error.

**When Down is Displayed in the Link Status**

If Down is displayed in Link status in the **List of Trunking Configurations** window, the link might have been disconnected. The following describes actions to take when the link is disconnected:

- Check whether a cable is connected to the port in use.

Check whether a cable is connected to the port in use. If not, connect the cable correctly.

- Check the cable.

  If the link remains disconnected even when the cable is connected correctly, there might be a problem with the cable. Replace the cable.

- Check the switch.

  If there is no problem with the cable, there might be a problem with the switch. In such a case, resolve the problem with the switch.

If there is no problem with the cable or switch, there might be a problem with the NAS Modular system hardware. Contact your HDS representative to resolve the problem.

**When Not aggregated is Displayed in Aggregate of LACP**

If `Not aggregated` is displayed in Aggregate of LACP in the **List of Trunking Configurations** window, wait for 10 minutes or more, and then click Refresh to update the information displayed in the window. If `Not aggregated` is still displayed even after clicking Refresh several times, the port might not have joined link aggregation.

The following describes actions to take when the port cannot join link aggregation.

When Up is displayed in Link status:

- Make sure that the switch supports IEEE802.3ad (Dynamic LACP).
- The cable might be inserted in the wrong place. Check the places to which the cable between the NAS Modular system and the switch is connected.
- There might be a problem in the switch settings. Make sure that the link aggregation settings for the switch are the same as those for the NAS Modular system. If not, specify the correct settings for the switch.
- Depending on the switch type, there are limitations on the port combination that can perform link aggregation. Check the switch specifications.

When Down is displayed in Link status:

The link might have been disconnected. Take action according to the procedure described in section 9.3.9.

**When Standby is Displayed in Status of Active Port for the Port Normally in Use**

When Link Alternation is set, if Standby is displayed in Status for Active port of the port normally in use (the port selected in Default active port in the **Link Alternation Setup** window), an error might have occurred on the port. The following describes actions to take when an error occurs on the port normally in use.

When Up is displayed in Link status:

Select the Link Alternation port (rdn0 or rdn1) in the **List of Trunking Configurations** window, and then click the **Change Active Port Status** button. Active is displayed in Status for Active port, and normal operation begins. If Status for Active port does not change to Active, contact your HDS representative to resolve the error.

When Down is displayed in Link status:

The link might have been disconnected. Take action according to the procedure described in section 9.3.9.

### 9.3.33 Checking Error Information on Data LAN Port

If an error occurs with the data LAN port in the **List of Data Ports** window, a system administrator checks the transmission status of the data LAN port, and then recovers the error.

#### 9.3.33.1 When Down is Displayed in Link status

If `Down` is displayed in **Link status** in the **List of Data Ports** window, the link might have been disconnected. Take the following actions if the link has been disconnected:

- Check whether a cable is connected to the port in use

  Check whether a cable is connected to the port in use. If not, connect the cable correctly.

- Check the cable

  If the link remains disconnected even though the cable is connected correctly, there might be a problem with the cable. Replace the cable.

- Check the cable setting

  Check whether the setting of the negotiation mode for the switch is the same as that for the NAS Modular system.

- Check the switch

  If there is no problem with the cable, there might be a problem with the switch. In such a case, resolve the switch problem.

If there is no problem with the cable or switch, there might be a problem with the NAS Modular system hardware. Contact your HDS representative to resolve the problem.

#### 9.3.33.2 When 10Base is Displayed for Speed in Connected status

If `10Base` is displayed for **Speed** in **Connected status**, the setting for the switch might be wrong. Check whether the setting of the negotiation mode for the switch is the same as that for the NAS Modular system. If not, correct the setting for the switch.

## 9.4 Collecting Data and Contacting Your HDS Representative

If you cannot identify the cause or location of an error, or if you cannot fix the problem, collect the required information, as indicated in the error message. Use the NAS Manager to download the error information and forward the information to your HDS representative.

If a failover has occurred, contact your HDS representative immediately.

**Downloading Error Information**

A system administrator can use the NAS Manager to download error information. Follow the instructions provided by the error message or by your HDS representative, and download all of the log data (**All log data**) from the **List of RAS Information** window or other logs instructed by the message or by your HDS representative, and then submit all collected data to your HDS representative. For details on downloading error information, see section 4.13.

## 9.5 Calling the Hitachi Data Systems Support Center

If you call the Hitachi Data Systems Support Center, make sure to provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure
- The exact content of any error messages displayed on the host system(s).

The worldwide Hitachi Data Systems Support Centers are:

- Hitachi Data Systems North America/Latin America
  San Diego, California, USA
  1-800-446-0744
- Hitachi Data Systems Europe
  Contact Hitachi Data Systems Local Support
- Hitachi Data Systems Asia Pacific
  North Ryde, Australia
  61-2-9325-33

# Appendix A List of Reserved Words

This section shows the words reserved in NAS Modular systems. Reserved words cannot be used to specify the names of:

- Clusters
- Nodes
- NNCs

**Table A.1 List of Reserved Words in NAS Modular systems**

| Initial Letter | Reserved Words |
|---|---|
| A | add, admin |
| C | CLU_partition, cluster |
| D | define, delete |
| F | Failover_policy, Filesystem, for, force |
| H | ha_parameter, ha_services, hostname |
| I | in, IP_address |
| L | log_group, LVM_volume |
| M | maintenance_off, maintenance_on, modify, move |
| N | NFS, NFS_admin, node |
| O | offline, online |
| R | remove, resource, resource_group, resource_type |
| S | set, show, start, status, stop |
| T | To |
| Symbol | One period ( . ), two periods ( . . ) |

# Appendix B List of MIB Objects

The system administrator can use SNMP to report information about exceeded quotas, system information and error information. This section describes the structure of Hitachi's proprietary Management Information Base (MIB) objects, as well as that of the standard MIB objects used in the NAS Modular system. The following figures describe these structures.

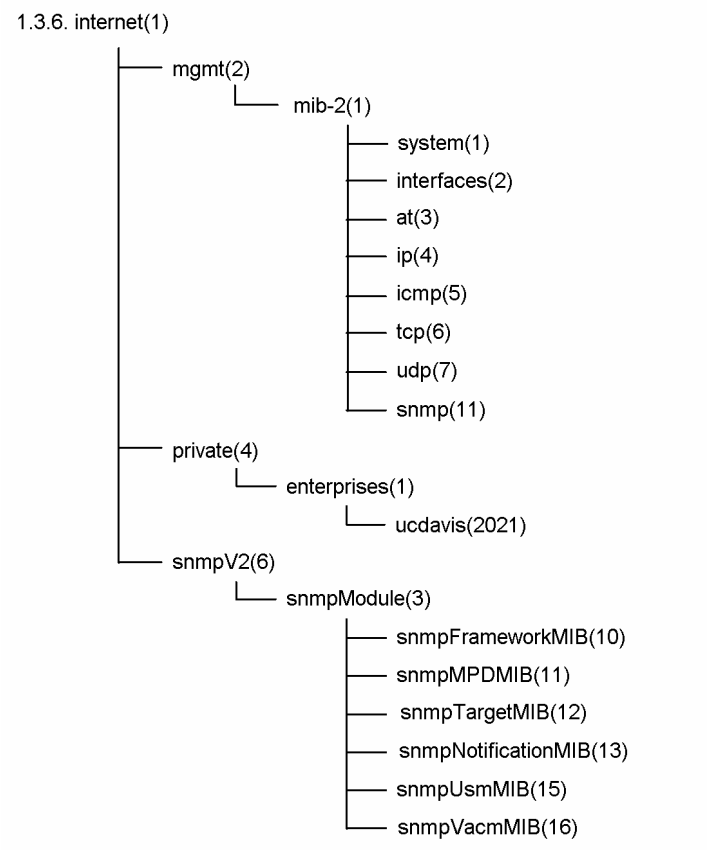



**Figure B.1 Structure for Standard MIB Objects**

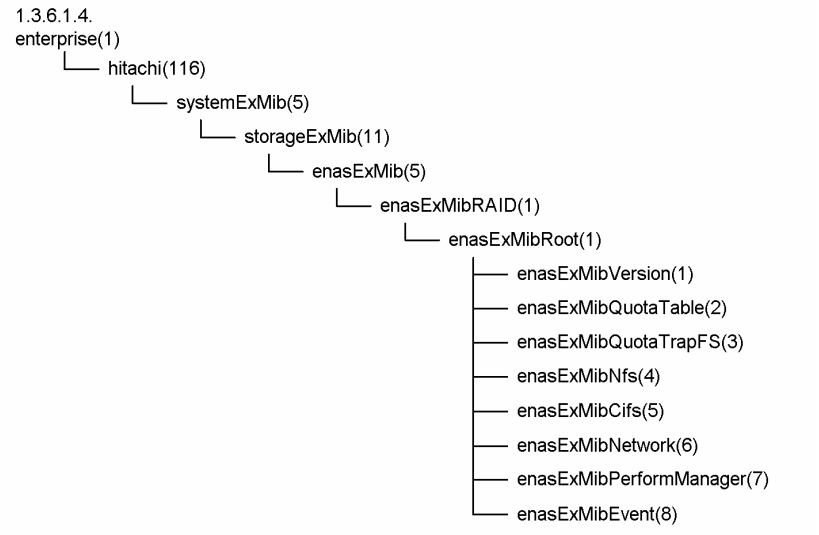



**Figure B.2 Responding to SNMP Get Requests - Tables Referenced (Stnd MIB Objects)**

## B.1 MIB Objects for Responding to SNMP Get Requests

The following table lists the groups of MIB objects in the NAS Modular system used for responding to SNMP `get` requests and the tables to be referenced for each group:

**Table B.1 MIB Objects for Responding to SNMP Get Requests (standard MIB objects)**

| Group Name | | Description | Table |
|---|---|---|---|
| 1.3.6.1.2.mib-2(1) | system(1) | This group is for `system` information. | Table B. |
| | interfaces(2) | This group is for `interfaces` information. | Table B. |
| | at(3) | This group is for `at` information. | |
| | ip(4) | This group is for `ip` information. | Table B. |
| | icmp(5) | This group is for `icmp` information. | Table B.7 |
| | tcp(6) | This group is for `tcp` information. | Table B. |
| | udp(7) | This group is for `udp` information. | Table B. |
| | snmp(11) | This group is for `snmp` information. | Table B. |
| 1.3.6.1.4.enterprises(1) | ucdavis(2021) | This group is for `ucdavis` information. | Table B.11 |
| 1.3.6.1.6.snmpModule(3) | snmpFrameworkMIB(10) | This group is for `snmp` management structures. | Table B.12 |
| | snmpMPDMIB(11) | This group is for message processing. | Table B.13 |
| | snmpTargetMIB(12) | This group is for parameter formation, for message creation. | Table B.14 |

| | | | |
|---|---|---|---|
| | snmpNotificationMIB(13) | This group is for parameter formation, for notification. | Table B.15 |
| | snmpUsmMIB(15) | This group is for security information definition. | Table B.16 |
| | snmpVacmMIB(16) | This group is for access/control information definition. | Table B.17 |

**Table B.2 MIB Objects for Responding to SNMP Get Requests (Hitachi MIB objects)**

| Group Name | Description | Tables |
|---|---|---|
| enasExMibVersion(1) | This group is for version information. | — |
| enasExMibQuotaTable(2) | This group is for quota set for file systems. | Table B.18 |
| enasExMibNfs(4) | This group is for NFS. | Table B.19 |
| enasExMibCifs(5) | This group is for CIFS. | Table B.20 |
| enasExMibNetwork(6) | This group is for the network. | Table B.21 |
| enasExMibPerformManager(7) | This group is for performance management. | Table B.22 |

Table B.3 through Table B.22 summarize the groups of MIB objects used in responding to SNMP `get` requests.

**Table B.3 System(1) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | sysDescr(1) | Names or version numbers for the hardware, OS, and network OS. |
| 2 | sysObjectID(2) | Vendor authentication ID for the network management system. |
| 3 | sysUpTime(3) | Time elapsed since system startup. |
| 4 | sysContact(4) | Contact information for the management node. |
| 5 | sysName(5) | The name and domain name of the management node. |
| 6 | sysLocation(6) | Location in which the management node is set up. |
| 7 | sysServices(7) | A value indicating services. |
| 8 | sysORLastChange(8) | The latest value for sysUpTime. |
| 9 | sysORTable(9) | For each MIB module, lists the functions of the local SNMPv2 entity acting as an agent. |
| 9.1 | sysOREntry(1) | Contains sysORTable entries. |
| 9.1.1 | sysORIndex(1) | A support variable used to identify instances of sysORTable columns and objects. |
| 9.1.2 | sysORID(2) | Proper identifiers for each MIB module.<br>MIB modules are supported based on the local SNMPv2 entity acting as an agent. |
| 9.1.3 | sysORDescr(3) | Defines a text description of the function identified by the corresponding sysORID. |

| | | |
|---|---|---|
| 9.1.4 | sysORUpTime(4) | Value of sysUpTime at the time this overview row was last instantiated. |

**Table B.4 Interfaces(2) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | ifNumber(1) | The number of network interfaces provided by the system. |
| 2 | ifTable(2) | The interface entity table. |
| 2.1 | ifEntry(1) | A list of interface information belonging to the sub-network layer. |
| 2.1.1 | ifIndex(1) | A number identifying this interface (values are sequential, from 1 to `ifNumber`). |
| 2.1.2 | ifDescr(2) | Information about the interface. |
| 2.1.3 | ifType(3) | The interface type. |
| 2.1.4 | ifMtu(4) | The maximum size of datagrams that can be transmitted with this interface. |
| 2.1.5 | ifSpeed(5) | An estimate of the current line speed for this interface. |
| 2.1.6 | ifPhysAddress(6) | The physical address immediately below the network layer of this interface. |
| 2.1.7 | ifAdminStatus(7) | The desired status for this interface. |
| 2.1.8 | ifOperStatus(8) | The current status of this interface. |
| 2.1.9 | ifLastChange(9) | The value of `sysUpTime` at the time at which `ifOperStatus` was last changed for this interface. |
| 2.1.10 | ifInOctets(10) | The number of octets received with this interface. |
| 2.1.11 | ifInUcastPkts(11) | The number of unicast packets for which the upper protocol has been notified. |
| 2.1.12 | ifInNUcastPkts(12) | The number of non-unicast packets (broadcast or multicast packets) for which the upper protocol has been notified. |
| 2.1.13 | ifInDiscards(13) | The number of packets for which no errors occurred, but nevertheless could not be passed to the upper protocol (the number of incoming packets that were discarded, with no buffer, etc.). |
| 2.1.14 | ifInErrors(14) | The number of packets that could not be received because an error occurred within the packet. |
| 2.1.15 | ifInUnknownProtos(15) | The number of packets discarded, due to having been received with an unsupported protocol. |
| 2.1.16 | ifOutOctets(16) | The number of octets from packets transmitted with this interface. |
| 2.1.17 | ifOutUcastPkts(17) | The number of unicast packets sent by the upper layer. |
| 2.1.18 | ifOutNUcastPkts(18) | The number of non-unicast packets sent by the upper layer. |
| 2.1.19 | ifOutDiscards(19) | The number of packets with no errors, but that were discarded during transmission processing (for which the transmission buffer was insufficient, etc.). |
| 2.1.20 | ifOutErrors(20) | The number of packets that could not be sent due to an error. |
| 2.1.21 | ifOutQLen(21) | The size of the queue for transmission packets. |
| 2.1.22 | ifSpecific(22) | A reference to a MIB defining properties of the interface media.<br>The object ID of a MIB is dependent on `ifType`. |

**Table B.5 at(3) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | atTable(1) | The table for `NetworkAddress`, for the corresponding value of the physical address. |
| 1.1 | atEntry(1) | A list related to one `NetworkAddress` for the corresponding value of the physical address for each entry. |
| 1.1.1 | atIfIndex(1) | The value of `ifIndex` for the corresponding interface. |
| 1.1.2 | atPhysAddress(2) | The physical address. |
| 1.1.3 | atNetAddress(3) | The IP address corresponding to `atPhysAddress`, depending on the media. |

**Table B.6 ip(4) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | ipForwarding(1) | Availability of IP relay function (whether or not operation is performed by gateway). |
| 2 | ipDefaultTTL(2) | The default TTL setting in IP headers. |
| 3 | ipInReceives(3) | The total number of IP datagrams received from all interfaces. |
| 4 | ipInHdrErrors(4) | The number of datagrams received and then discarded due to IP header errors. |
| 5 | ipInAddrErrors(5) | The number of packets discarded due to an invalid destination address in the IP header. |
| 6 | ipForwDatagrams(6) | The number of packets for which relay was deemed necessary. |
| 7 | ipInUnknownProtos(7) | The number of IP data programs discarded due to the following:<br>▪ The protocol cannot be confirmed for incoming IP packets.<br>▪ The protocol is unsupported. |
| 8 | ipInDiscards(8) | The total number of IP datagrams discarded during transmission for reasons other than errors. |
| 9 | ipInDelivers(9) | The number of IP datagrams reported to the upper layer. |
| 10 | ipOutRequests(10) | The total number of IP datagrams requested by the upper layer, for IP packet transmission. |
| 11 | ipOutDiscards(11) | The number of IP datagrams discarded for reasons other than errors. |
| 12 | ipOutNoRoutes(12) | The number of IP datagrams discarded because no transmission route was specified. |
| 13 | ipReasmTimeout(13) | The maximum number of seconds to hold fragment packets waiting for re-assembly. |
| 14 | ipReasmReqds(14) | The number of incoming IP datagrams for which re-assembly is necessary. |
| 15 | ipReasmOKs(15) | The number of incoming IP datagrams for which re-assembly was successful. |
| 16 | ipReasmFails(16) | The number of incoming IP datagrams for which re-assembly failed. |
| 17 | ipFragOKs(17) | The number of IP datagrams for which fragmentation was successful. |
| 18 | ipFragFails(18) | The number of IP datagrams for which fragmentation failed. |

| ID | Object Name | Meaning |
|---|---|---|
| 19 | ipFragCreates(19) | The number of IP datagram fragments created as a result of fragmentation. |
| 20 | ipAddrTable(20) | A table for addressing information related to the IP address of this entity (a table of address information, by IP address). |
| 20.1 | ipAddrEntry(1) | A list of addressing information for one of the IP addresses of this entity. |
| 20.1.1 | ipAdEntAddr(1) | IP address. |
| 20.1.2 | ipAdEntIfIndex(2) | The index value for the interface used by this entry. |
| 20.1.3 | ipAdEntNetMask(3) | The subnet mask for the IP address of this entry. |
| 20.1.4 | ipAdEntBcastAddr(4) | The value of the lowest bit of the address during IP broadcast transmission. |
| 20.1.5 | ipAdEntReasmMaxSize(5) | The maximum IP packet size that can be re-assembled from input IP datagrams that were divided into IP fragments received by the interface. |
| 21 | ipRouteTable(21) | The IP routing table for this entity. |
| 21.1 | ipRouteEntry(1) | Routing information for a specified destination. |
| 21.1.1 | ipRouteDest(1) | The destination IP address of this route. |
| 21.1.2 | ipRouteIfIndex(2) | The index value of the interface existing on the first hop of this route. |
| 21.1.3 | ipRouteMetric1(3) | The primary routing metric of this route. |
| 21.1.4 | ipRouteMetric2(4) | The alternate routing metric of this route. |
| 21.1.5 | ipRouteMetric3(5) | The alternate routing metric of this route. |
| 21.1.6 | ipRouteMetric4(6) | The alternate routing metric of this route. |
| 21.1.7 | ipRouteNextHop(7) | The IP address of the next hop of this route. |
| 21.1.8 | ipRouteType(8) | The route type. |
| 21.1.9 | ipRouteProto(9) | The routing structure that learned the route. |
| 21.1.10 | ipRouteAge(10) | The amount of time elapsed since the route was updated. |
| 21.1.11 | ipRouteMask(11) | The subnet mask value for `ipRouteDest.` |
| 21.1.12 | ipRouteMetric5(12) | The alternate routing metric of this route. |
| 21.1.13 | ipRouteInfo(13) | A reference to the MIB object defining the specific routing protocol that can be trusted on this route. |
| 22 | ipNetToMediaTable(22) | The IP address conversion table used to map a physical address from IP addresses. |
| 22.1 | ipNetToMediaEntry(1) | A list of individual IP addresses that correspond to the physical address. |
| 22.1.1 | ipNetToMediaIfIndex(1) | The ID number of the active interface. |
| 22.1.2 | ipNetToMediaPhysAddress(2) | The media-dependent physical address. |
| 22.1.3 | ipNetToMediaNetAddress(3) | The IP address corresponding to the media-dependent physical address. |
| 22.1.4 | ipNetToMediaType(4) | The mapping type. |
| 23 | ipRoutingDiscards(23) | The number of routing entries selected for rejection despite being active, such as those rejected due to an insufficient buffer for the routing table. |

**Table B.7 icmp(5) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | icmpInMsgs(1) | The total number of ICMP messages received by this entity. |
| 2 | icmpInErrors(2) | The number of ICMP error messages received (such as those for checksum errors and frame length errors). |
| 3 | icmpInDestUnreachs(3) | The number of ICMP Destination Unreachable messages received. |
| 4 | icmpInTimeExcds(4) | The number of ICMP Time Exceed messages received. |
| 5 | icmpInParmProbs(5) | The number of ICMP Parameter Problem messages received. |
| 6 | icmpInSrcQuenchs(6) | The number of ICMP Source Quench messages received. |
| 7 | icmpInRedirects(7) | The number of ICMP Network Redirect messages received. |
| 8 | icmpInEchos(8) | The number of ICMP Echo request messages received. |
| 9 | icmpInEchoReps(9) | The number of ICMP Echo response messages received. |
| 10 | icmpInTimestamps(10) | The number of ICMP TimeStamp request messages received. |
| 11 | icmpInTimestampReps(11) | The number of ICMP TimeStamp response messages received. |
| 12 | icmpInAddrMasks(12) | The number of ICMP Address Mask request messages received. |
| 13 | icmpInAddrMaskReps(13) | The number of incoming ICMP Address Mask response messages. |
| 14 | icmpOutMsgs(14) | The total number of ICMP send attempts (including those for which errors occurred). |
| 15 | icmpOutErrors(15) | The number of ICMP messages that were not sent due to an error. |
| 16 | icmpOutDestUnreachs(16) | The number of ICMP Destination Unreachable messages sent. |
| 17 | icmpOutTimeExcds(17) | The number of ICMP Time Exceeded messages sent. |
| 18 | icmpOutParmProbs(18) | The number of ICMP Parameter Problem messages sent. |
| 19 | icmpOutSrcQuenchs(19) | The number of ICMP Source Quench messages sent. |
| 20 | icmpOutRedirects(20) | The number of ICMP Redirect messages sent. |
| 21 | icmpOutEchos(21) | The number of ICMP Echo request messages sent. |
| 22 | icmpOutEchoReps(22) | The number of ICMP Echo response messages sent. |
| 23 | icmpOutTimestamps(23) | The number of ICMP Timestamp request messages sent. |
| 24 | icmpOutTimestampReps(24) | The number of ICMP Timestamp response messages sent. |
| 25 | icmpOutAddrMasks(25) | The number of ICMP Address Mask request messages sent. |
| 26 | icmpOutAddrMaskReps(26) | The number of ICMP Address Mask response messages sent. |

**Table B.8 tcp(6) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | tcpRtoAlgorithm(1) | The algorithm to decide the timeout time used for retransmission. |
| 2 | tcpRtoMin(2) | The minimum value for the retransmission timeout time. |
| 3 | tcpRtoMax(3) | The maximum value for the retransmission timeout time. |
| 4 | tcpMaxConn(4) | The total number of supportable TCP connections. -1 is returned when this number is dynamic. |
| 5 | tcpActiveOpens(5) | The number of times that TCP connections were moved from the CLOSE status to the SYN-SENT status. |
| 6 | tcpPassiveOpens(6) | The number of times that TCP connections were moved from the LISTEN status to the SYN-RCVD status. |
| 7 | tcpAttemptFails(7) | The number of times TCP connections were moved from the SYN-SENT or SYN-RCVD statuses to the CLOSE status, added to the number of times TCP connections were moved from the SYN-RCVD status to the LISTEN status. |
| 8 | tcpEstabResets(8) | The number of times TCP connections were moved from the ESTABLISHD or CLOSE-WAIT statuses to the CLOSE status. |
| 9 | tcpCurrEstab(9) | The total number of TCP connections in the ESTABLISHD or CLOSE-WAIT status. |
| 10 | tcpInSegs(10) | The total number of incoming segments, including error segments. |
| 11 | tcpOutSegs(11) | The total number of segments sent. |
| 12 | tcpRetransSegs(12) | The total number of re-sent segments. |
| 13 | tcpConnTable(13) | A table of information specific to TCP connections. |
| 13.1 | tcpConnEntry(1) | Entry information about a particular TCP connection. |
| 13.1.1 | tcpConnState(1) | The TCP connection status. |
| 13.1.2 | tcpConnLocalAddress(2) | The local IP address of this TCP connection. |
| 13.1.3 | tcpConnLocalPort(3) | The local port number of this TCP connection. |
| 13.1.4 | tcpConnRemAddress(4) | The remote IP address of this TCP connection. |
| 13.1.5 | tcpConnRemPort(5) | The remote port number of this TCP connection. |
| 14 | tcpInErrs(14) | The total number of error segments received. |
| 15 | tcpOutRsts(15) | The number of segments sent that have the RST flag. |

**Table B.9 udp(7) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | udpInDatagrams(1) | The number of UDP datagrams reported to the upper layer. |
| 2 | udpNoPorts(2) | The total number of incoming UDP packets for which no parent application exists in the address port. |
| 3 | udpInErrors(3) | The number of UDP datagrams unable to be reported to the application due to reasons other than `udpNoPorts.` |
| 4 | udpOutDatagrams(4) | The total number of UDP datagrams sent by the parent application. |
| 5 | udpTable(5) | A table for UDP listener information. |
| 5.1 | udpEntry(1) | The number of entries for a particular UDP listener. |
| 5.1.1 | udpLocalAddress(1) | The local IP address of this UDP listener. |
| 5.1.2 | udpLocalPort(2) | The local port number of this UDP listener. |

**Table B.10 >snmp(11) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | snmpInPkts(1) | The total number of incoming SNMP messages. |
| 2 | snmpOutPkts(2) | The total number of outgoing SNMP messages. |
| 3 | snmpInBadVersions(3) | The total number of incoming messages of unsupported versions. |
| 4 | snmpInBadCommunityNames(4) | The total number of incoming SNMP messages for unused communities. |
| 5 | snmpInBadCommunityUses(5) | The total number of incoming messages indicating operations not allowed by the community. |
| 6 | snmpInASNParseErrs(6) | The total number of incoming `ASN.1` error messages. |
| 8 | snmpInTooBigs(8) | The total number of incoming PDUs for which the error status is `tooBig.` |
| 9 | snmpInNoSuchNames(9) | The total number of incoming PDUs for which the error status is `noSuchName.` |
| 10 | snmpInBadValues(10) | The total number of incoming PDUs for which the error status is `badValue.` |
| 11 | snmpInReadOnlys(11) | The total number of incoming PDUs for which the error status is `readOnly.` |
| 12 | snmpInGenErrs(12) | The total number of incoming PDUs for which the error status is `genErr.` |
| 13 | snmpInTotalReqVars(13) | The total number of MIB objects for which MIB collection was successful. |
| 14 | snmpInTotalSetVars(14) | The total number of MIB objects for which MIB setup was successful. |
| 15 | snmpInGetRequests(15) | The total number of `GetRequestPDU`s received. |
| 16 | snmpInGetNexts(16) | The total number of `GetNextRequestPDU`s received. |
| 17 | snmpInSetRequests(17) | The total number of `SetRequestPDU`s received. |
| 18 | snmpInGetResponses(18) | The total number of `GetReresponsePDU`s received. |

| ID | Object Name | Meaning |
|---|---|---|
| 19 | snmpInTraps(19) | The total number of TrapPDUs received. |
| 20 | snmpOutTooBigs(20) | The total number of outgoing PDUs for which the error status is tooBig. |
| 21 | snmpOutNoSuchNames(21) | The total number of outgoing PDUs for which the error status is noSuchName. |
| 22 | snmpOutBadValues(22) | The total number of outgoing PDUs for which the error status is badValue. |
| 24 | snmpOutGenErrs(24) | The total number of outgoing PDUs for which the error status is genErr. |
| 25 | snmpOutGetRequests(25) | The total number of GetRequestPDUs sent. |
| 26 | snmpOutGetNexts(26) | The total number of GetNextRequestPDUs sent. |
| 27 | snmpOutSetRequests(27) | The total number of SetRequestPDUs sent. |
| 28 | snmpOutGetResponses(28) | The total number of GetResponsePDUs sent. |
| 29 | snmpOutTraps(29) | The total number of TrapPDUs sent. |
| 30 | snmpEnableAuthenTraps(30) | Whether or not an authentication-failureTrap was issued. |
| 31 | snmpSilentDrops(31) | The total number, sent to the SNMP entity, of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs.<br>(If the size of a response containing an alternate Response-PDU with a blank variable binding field is larger than the local limit, or the maximum message size on the side from which the request originated, the snmpSilentDrops object will be discarded without being reported.) |
| 32 | snmpProxyDrops(32) | The total number, sent to the SNMP entity, of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs.<br>(If the transmission of messages (which are probably converted) to the proxy target fails without a Response-PDU being returned (aside from timeouts), the snmpProxyDrops object will be discarded without being reported.) |

**Table B.11 ucdavis(2021) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 2 | prTable(2) | Contains the process status. |
| 2.1 | prEntry(1) | A hierarchical tree comprising a table that contains a list of process information. |
| 2.1.1 | prIndex(1) | An index number allocated to this process information. |
| 2.1.2 | prNames(2) | The process names specified in that of the `proc` line. |
| 2.1.3 | prMin(3) | The minimum value set for the `proc` line. |
| 2.1.4 | prMax(4) | The maximum value set for the `proc` line. |
| 2.1.5 | prCount(5) | The number of processes specified in `prNames` that are currently running. |
| 2.1.100 | prErrorFlag(100) | In the case of an error, this is `1`. Otherwise, it is `0`. |
| 2.1.101 | prErrMessage(101) | This contains an error message, when `prErrorFlag` is `1`. |
| 2.1.102 | prErrFix(102) | When the administrator sets this object to `1`, the command already specified on the `procfix` line of the `snmpd.conf` file is used. |
| 2.1.103 | prErrFixCmd(103) | The name of the command used when `prErrFix` is set to `1`. |
| 4 | memory(4) | Contains the memory status. |
| 4.1 | memIndex(1) | A dummy index number (always `0`). |
| 4.2 | memErrorName(2) | A dummy name (always `swap`). |
| 4.3 | memTotalSwap(3) | The amount of space reserved for the swap file. |
| 4.4 | memAvailSwap(4) | The amount of unused swap file space. |
| 4.5 | memTotalReal(5) | The amount of real memory installed. |
| 4.6 | memAvailReal(6) | The amount of real memory available.<br>***Note:*** NAS Units use most of the memory as an I/O buffer cache to enable cached I/O data to be reused. For this reason, the amount of memory that is used increases periodically, and the variations in the amount of available memory become smaller. |
| 4.7 | memTotalSwapTXT(7) | The swap file reserved area that is used for text. |
| 4.8 | memAvailSwapTXT(8) | The amount of swap file space for text that is unused. |
| 4.9 | memTotalRealTXT(9) | The total real memory used for text. |
| 4.10 | memAvailRealTXT(10) | The amount of available memory used for text. |
| 4.11 | memTotalFree(11) | The total available memory. |
| 4.12 | memMinimumSwap(12) | The available size of the swap file during an error. |
| 4.13 | memShared(13) | The total amount of shared memory. |
| 4.14 | memBuffer(14) | The total amount of buffer memory. |
| 4.15 | memCached(15) | The total amount of cache memory. |
| 4.100 | memSwapError(100) | The swap error flag. |
| 4.101 | memSwapErrorMsg(101) | The error message when `memSwapError` is `1`. |

| ID | Object Name | Meaning |
|---|---|---|
| 8 | extTable(8) | Uses the commands already specified on the system, and contains the results. |
| 8.1 | extEntry(1) | A hierarchical tree that holds a table containing data from execution results. |
| 8.1.1 | extIndex(1) | An index number. |
| 8.1.2 | extNames(2) | The name specified for the set name in the `exec` line. |
| 8.1.3 | extCommand(3) | The full path name and arguments of the execution file specified in the `exec` line. |
| 8.1.100 | extResult(100) | The error code returned when the execution file specified in `extCommand` is used. |
| 8.1.101 | extOutput(101) | The execution results of the execution file specified in `extCommand`. |
| 8.1.102 | extErrFix(102) | When the administrator sets this object to `1`, the command already specified in the `execfix` line of the `snmpd.conf` file is used. |
| 8.1.103 | extErrFixCmd(103) | The name of the command used when `extErrFix` is set to `1`. |
| 9 | dskTable(9) | Contains the disk status. |
| 9.1 | dskEntry(1) | A hierarchical tree to hold disk information. |
| 9.1.1 | dskIndex(1) | An index number. |
| 9.1.2 | dskPath(2) | The path name of the inspection target.<br>The value specified for the path name to be inspected, in the `disk` line. |
| 9.1.3 | dskDevice(3) | The device name contained in `dskPath`. |
| 9.1.4 | dskMinimum(4) | The minimum amount for error handling specified in the `disk` line (`-1` when a percentage is specified). |
| 9.1.5 | dskMinPercent(5) | The minimum percentage amount for error handling specified in the `disk` line (`-1` when units are specified in KB). |
| 9.1.6 | dskTotal(6) | The maximum amount that can be stored on the device specified in `dskDevice`. |
| 9.1.7 | dskAvail(7) | The amount of space currently available on the device specified in `dskDevice`. |
| 9.1.8 | dskUsed(8) | The current usage rate of the device specified in `dskDevice`. |
| 9.1.9 | dskPercent(9) | The current usage rate of the device specified in `dskDevice`, expressed as a percentage. |
| 9.1.10 | dskPercentNode(10) | The current i-node usage rate of the device specified in `dskDevice`, expressed as a percentage. |
| 9.1.100 | dskErrorFlag(100) | An error flag that indicates whether or not the available space is less than that specified on the `disk` line:<br>`1`: less than or equal to the specified space<br>`0`: greater than or equal to the specified space |
| 9.1.101 | dskErrorMsg(101) | The error message when `dskErrorFlag` is `1`. |
| 10 | laTable(10) | Contains load average information for the system. |
| 10.1 | laEntry(1) | A hierarchical directory that contains load average information. |

| ID | Object Name | Meaning |
|---|---|---|
| 10.1.1 | laIndex(1) | An index number.<br>This value is 1 for one-minute average value information, 2 for five-minute average value information, and 3 for fifteen-minute average value information. |
| 10.1.2 | laNames(2) | The monitoring name.<br>This value is Load-1 for one-minute average value information, Load-5 for five-minute average value information, and Load-15 for fifteen-minute average value information. |
| 10.1.3 | laLoad(3) | The load average value, expressed as a string.<br>laLoad-1 stores the accumulated value for the last minute. laLoad-2 stores the accumulated value for the last 5 minutes. laLoad-3 stores the accumulated value for the last 15 minutes.<br>In NAS Manager, the load average value is always at least 1 even when the system is not loaded. |
| 10.1.4 | laConfig(4) | The average value set in the load line for error handling. |
| 10.1.5 | laLoadInt(5) | laLoad, expressed as a percentage. |
| F10.1.6 | laLoadFloat(6) | laLoad, expressed as a floating-point decimal. |
| 10.1.100 | laErrorFlag(100) | An error flag.<br>This value is 1 when the set average value of the load average is exceeded, and 0 otherwise. |
| 10.1.101 | laErrMessage(101) | The error message when laLoadErrorFlag is 1. |
| 11 | systemStats(11) | Contains the system status. |
| 11.1 | ssIndex(1) | A dummy index number (always 1). |
| 11.2 | ssErrorName(2) | The systemStats name (always systemStats). |
| 11.3 | ssSwapIn(3) | The time required for swap-in. |
| 11.4 | ssSwapOut(4) | The time required for swap-out. |
| 11.5 | ssIOSent(5) | The time required for transmission to the block device. |
| 11.6 | ssIOReceive(6) | The time required for reception from the block device. |
| 11.7 | ssSysInterrupts(7) | The number of interruptions for one second, including clock interruptions. |
| 11.8 | ssSysContext(8) | The number of context switches switched for one second. |
| 11.9 | ssCpuUser(9) | The ratio of CPU capacity used by the user. |
| 11.10 | ssCpuSystem(10) | The ratio of CPU capacity used by the system. |
| 11.11 | ssCpuIdle(11) | The ratio of CPU capacity that is idle. |
| 11.50 | ssCpuRawUser(50) | The time for which the user is using the CPU. |
| 11.51 | ssCpuRawNice(51) | The value of the nice process. |
| 11.52 | ssCpuRawSystem(52) | The time for which the user is using the CPU. |
| 11.53 | ssCpuRawIdle(53) | The time for which the CPU is idle. |
| 13 | ucdExperimental(13) | An experimental MIB. |

| ID | Object Name | Meaning |
|---|---|---|
| 13.14 | ucdDlmodMIB(14) | The dynamic load module MIB<br>Function for loading a predefined MIB definition file during snmpd operation. |
| 13.14.1 | dlmodNextIndex(1) | The index of the next-loaded MIB. |
| 100 | version(100) | Contains the `snmpd` version information. |
| 100.1 | versionIndex(1) | The index to MIB. |
| 100.2 | versionTag(2) | The CVS tag keyword. |
| 100.3 | versionDate(3) | The date from the RCS keyword. |
| 100.4 | versionCDate(4) | The date from `ctime()`. |
| 100.5 | versionIdent(5) | The ID from the RCS keyword. |
| 100.6 | versionConfigureOptions(6) | If this agent is configured, options are moved to the config script. |
| 100.10 | versionClearCache(10) | When this is set to `1`, the execution cache is cleared. |
| 100.11 | versionUpdateConfig(11) | When this is set to `1`, the config file is read. |
| 100.12 | versionRestartAgent(12) | When this is set to `1`, the agent is restarted. |
| 100.20 | versionDoDebugging(20) | When this is set to `1`, the device statement is released with a `0`. |
| 101 | snmperrs(101) | Contains `snmpd` error information. |
| 101.1 | snmperrIndex(1) | A fake index for `snmperrs`. |
| 101.2 | snmperrNames(2) | `Snmp.` |
| 101.100 | snmperrErrorFlag(100) | An error flag indicating a problem with the agent. |
| 101.101 | snmperrErrMessage(101) | A message explaining the problem. |
| 102 | mrTable(102) | Modules can be added to `snmpd`, to extend its function.<br>This `mrTable` subtree contains information for each added module. |
| 102.1 | mrEntry(1) | An entry containing the registered `mib oid`. |
| 102.1.1 | mrIndex(1) | The registration slot of the MIB module. |
| 102.1.2 | mrModuleName(2) | The name of the module that registered this OID. |

**Table B.12 snmpFrameworkMIB(10) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 2 | snmpFrameworkMIBObjects(2) | — |
| 2.1 | snmpEngine(1) | — |
| 2.1.1 | snmpEngineID(1) | A unique identifier for SNMP engine operation. |
| 2.1.2 | snmpEngineBoots(2) | The number of times the SNMP engine was (re)initialized since `snmpEngineID` was last set. |
| 2.1.3 | snmpEngineTime(3) | The number of seconds that have elapsed since the value of `snmpEngineBoots` was last set. |
| 2.1.4 | snmpEngineMaxMessageSize(4) | The maximum octet length of SNMP messages that the SNMP engine can transmit and process (as dictated by the minimum value of the |

| | | |
|---|---|---|
| | | maximum size of messages that can be transmitted and processed by all transports). |

**Table B.13 snmpMPDMIB(11) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 2 | snmpMPDMIBObjects(2) | — |
| 2.1 | snmpMPDStats(1) | — |
| 2.1.1 | snmpUnknownSecurityModels(1) | The total number of packets received by the SNMP engine, not including those not supported by the SNMP engine. |
| 2.1.2 | snmpInvalidMsgs(2) | Total number of packets received by the SNMP engine, not including invalid or inconsistent components in SNMP messages. |
| 2.1.3 | snmpUnknownPDUHandlers(3) | The total number of packets received by the SNMP engine, not including those for which PDUs containing `pduType` packets could not be passed. |

**Table B.14 snmpTargetMIB(12) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | snmpTargetObjects(1) | — |
| 1.2 | snmpTargetAddrTable(2) | The transport table is used to create SNMP messages. |
| 2.1 | snmpTargetAddrEntry(1) | The transport address is used to create SNMP operations. |
| 2.1.1 | snmpTargetAddrName(1) | A unique identifier that is locally optional but related to this `snmpTargetAddrEntry`. |
| 2.1.2 | snmpTargetAddrTDomain(2) | The address of the transport type included in the `snmpTargetAddrTAddress` object. |
| 2.1.3 | snmpTargetAddrTAddress(3) | This address format, which contains the transport address, is dependent on the value of the `snmpTargetAddrTDomain` object. |
| 2.1.4 | snmpTargetAddrTimeout(4) | This reflects the expected maximum round-trip time for contacting the transport address defined in this row. |
| 2.1.5 | snmpTargetAddrRetryCount(5) | Specifies the default number of retries when a message, for which a response was created, cannot be received. |
| 2.1.6 | snmpTargetAddrTagList(6) | Contains the tag list used to choose the target address for a particular operation. |
| 2.1.7 | snmpTargetAddrParams(7) | An entry from within the `snmpTargetParamsTable`. |
| 2.1.8 | snmpTargetAddrStorageType(8) | The memory type. |
| 2.1.9 | snmpTargetAddrRowStatus(9) | The status. |
| 1.3 | snmpTargetParamsTable(3) | A table of SNMP target information used to create SNMP messages. |
| 3.1 | snmpTargetParamsEntry(1) | One piece of information for one SNMP set. |
| 3.1.1 | snmpTargetParamsName(1) | A unique identifier that is locally optional but related to this `snmpTargetParamsEntry`. |
| 3.1.2 | snmpTargetParamsMPModel(2) | When this entry is used to create an SNMP message, a certain message processing module has been used. |

| ID | Object Name | Meaning |
|---|---|---|
| 3.1.3 | snmpTargetParamsSecurityModel(3) | The security models for the SNMP messages.<br>SNMP_SEC_MODEL_ANY(0),<br>SNMP_SEC_MODEL_SNMPv1(1),<br>SNMP_SEC_MODEL_SNMPv2c(2),<br>SNMP_SEC_MODEL_USM(3), and<br>SNMP_SEC_MODEL_SNMPv2p(256). |
| 3.1.4 | snmpTargetParamsSecurityName(4) | The securityName specifying the principal in an SNMP message occurs using this entry. |
| 3.1.5 | snmpTargetParamsSecurityLevel(5) | The security level used when this entry is used to create an SNMP message. |
| 3.1.6 | snmpTargetParamsStorageType(6) | The nonVolatile, permanent, or readOnly memory type. |
| 3.1.7 | snmpTargetParamsRowStatus(7) | When the value of this object is active(1), the following objects are not corrected:<br>- snmpTarget ParamsMPModel<br>- snmpTarget ParamsSecurityModel<br>- snmpTarget ParamsSecurityName<br>- snmpTarget ParamsSecurityLevel |

**Table B.15 snmpNotificationMIB(13) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | snmpNotifyObjects(1) | — |
| 1.1 | snmpNotifyTable(1) | Contains the object selecting the host and notification type. |
| 1.1.1 | snmpNotifyEntry(1) | Used to configure the notification entry. |
| 1.1.1.1 | snmpNotifyName(1) | The notification name. |
| 1.1.1.2 | snmpNotifyTag(2) | Used to select entries in the snmpTargetAddrTable. |
| 1.1.1.3 | snmpNotifyType(3) | This is 1 in case of a trap, or 2 in case of a notification. |
| 1.1.1.4 | snmpNotifyStorageType(4) | nonVolatile, permanent, or readOnly. |
| 1.1.1.5 | snmpNotifyRowStatus(5) | The status of the row of this overview. |

**Table B.16 snmpUsmMIB(15) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | usmMIBObjects(1) | — |
| 1.1 | usmStats(1) | — |
| 1.1.1 | usmStatsUnsupportedSecLevels(1) | The total number of packets received by the SNMP engine, not including cases in which a `securityLevel` that is not used or not in the SNMP engine was requested. |
| 1.1.2 | usmStatsNotInTimeWindows(2) | The total number of packets received by the SNMP engine, not including those appearing outside of the SNMP engine. |
| 1.1.3 | usmStatsUnknownUserNames(3) | The total number of packets received by the SNMP engine, not including user views of which the SNMP engine was not notified. |
| 1.1.4 | usmStatsUnknownEngineIDs(4) | The total number of packets received by the SNMP engine, not including `snmpEngineID`s of which the SNMP engine was not notified. |
| 1.1.5 | usmStatsWrongDigests(5) | The total number of packets received by the SNMP engine, not including those that did not have an expected digest value. |
| 1.1.6 | usmStatsDecryptionErrors(6) | The total number of packets received by the SNMP engine, not including those that could not be decrypted. |
| 1.2 | usmUser(2) | — |
| 1.2.1 | usmUserSpinLock(1) | Locks are used so that the various cooperating command generator applications can be reconciled. |

**Table B.17 snmpVacmMIB(16) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | vacmMIBObjects(1) | — |
| 1.2 | vacmSecurityToGroupTable(2) | A table used so that the access management policy for the combination of `securityModel` and `securityName` can be defined for the primary group.<br>This is mapped to `groupName`. |
| 1.2.1 | vacmSecurityToGroupEntry(1) | Used to allocate principals to the group. |
| 1.2.1.1 | vacmSecurityModel(1) | The security model. |
| 1.2.1.2 | vacmSecurityName(2) | The security name. |
| 1.2.1.3 | vacmGroupName(3) | Group name. |
| 1.2.1.4 | vacmSecurityToGroupStorageType(4) | The memory type. |
| 1.2.1.5 | vacmSecurityToGroupStatus(5) | The status. |
| 1.4 | vacmAccessTable(4) | The access permissions table. |
| 1.4.1 | vacmAccessEntry(1) | The access permissions configured in the Local Configuration Datastore (LCD) permitting access to SNMP. |
| 1.4.1.1 | vacmAccessContextPrefix(1) | The value of this object must match `contextName`, so that access permissions can be obtained. |

| ID | Object Name | Meaning |
|---|---|---|
| 1.4.1.2 | vacmAccessSecurityModel(2) | This `securityModel` must be used to obtain access permissions. |
| 1.4.1.3 | vacmAccessSecurityLevel(3) | The minimum security level. |
| 1.4.1.4 | vacmAccessContextMatch(4) | The method by which the context for `exact` or `prefix` requests matches `vacmAccessContextPrefix`. |
| 1.4.1.5 | vacmAccessReadViewName(5) | Used to define the view subtree for `GetRequests`. |
| 1.4.1.6 | vacmAccessWriteViewName(6) | Used to define the view subtree for `SetRequests`. |
| 1.4.1.7 | vacmAccessNotifyViewName(7) | Used to define the view subtree so that objects within trap messages and `InformRequests` can be loaded as `VarBinds`. |
| 1.4.1.8 | vacmAccessStorageType(8) | The memory type. |
| 1.4.1.9 | vacmAccessStatus(9) | The status. |
| 1.5 | vacmMIBViews(5) | — |
| 1.5.1 | vacmViewSpinLock(1) | Locks enable set operation usage to be adjusted when SNMP command generators are used to create or modify a view. |
| 1.5.2 | vacmViewTreeFamilyTable(2) | Locally stored information about a family of a subtree in MIB. |
| 1.5.2.1 | vacmViewTreeFamilyEntry(1) | Information about a particular family of a subtree. |
| 1.5.2.1.1 | vacmViewTreeFamilyViewName(1) | The human-readable name of family of the view subtree. |
| 1.5.2.1.2 | vacmViewTreeFamilySubtree(2) | The MIB subtree that defines the family of the view subtree for `vacmViewTreeFamilyMask`. |
| 1.5.2.1.3 | vacmViewTreeFamilyMask(3) | The mask that defines the family of the view subtree for `vacmViewTreeFamilySubtree`. |
| 1.5.2.1.4 | vacmViewTreeFamilyType(4) | Whether or not the subtree under the OID defined in `vacmViewTreeFamilySubtree` can be accessed. |
| 1.5.2.1.5 | vacmViewTreeFamilyStorageType(5) | The memory type. |
| 1.5.2.1.6 | vacmViewTreeFamilyStatus(6) | The status. |

**Table B.18 >enasExMibQuotaTable(2) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | quotaEntry(1) | Quota management information set for a file system. |
| 1.1 | quotaFSIndex(1) | File system index. |
| 1.2 | quotaFSMntPoint(2) | File system mount point. |
| 1.3 | quotaFSBlockMaxGrace(3) | Grace time for block usage (days). |
| 1.4 | quotaFSFileMaxGrace(4) | Grace time for i-node usage (days). |
| 1.5 | quotaFSStatus(5) | Quota status (off/on). |
| 1.6 | quotaFSUserTable(6) | User. |
| 1.6.1 | quotaUserEntry(1) | User quota entry. |

| ID | Object Name | Meaning |
|---|---|---|
| 1.6.1.1 | quotaUserIndex(1) | User index. |
| 1.6.1.2 | quotaUserUID(2) | UID. |
| 1.6.1.3 | quotaUserBlockCount(3) | Used block count. |
| 1.6.1.4 | quotaUserFileCount(4) | Used i-node count. |
| 1.6.1.5 | quotaUserBlockSoftLimit(5) | Soft limit on block count. |
| 1.6.1.6 | quotaUserFileSoftLimit(6) | Soft limit on i-node count. |
| 1.6.1.7 | quotaUserBlockHardLimit(7) | Hard limit on block count. |
| 1.6.1.8 | quotaUserFileHardLimit(8) | Hard limit on i-node count. |
| 1.6.1.9 | quotaUserBlockGracePeriod(9) | Time (seconds) remaining for the extended period from when the number of blocks exceeded the soft limit |
| 1.6.1.10 | quotaUserFileGracePeriod(10) | Time (seconds) remaining for the extended period from when the number of I-nodes exceeded the soft limit |
| 1.7 | quotaFSGroupTable(7) | Group. |
| 1.7.1 | quotaGroupEntry(1) | Group quota entry. |
| 1.7.1.1 | quotaGroupIndex(1) | Group index. |
| 1.7.1.2 | quotaGroupGID(2) | GID. |
| 1.7.1.3 | quotaGroupBlockCount(3) | Number (KB) of blocks being used). |
| 1.7.1.4 | quotaGroupFileCount(4) | Used i-node count. |
| 1.7.1.5 | quotaGroupBlockSoftLimit(5) | Soft limit on block count. |
| 1.7.1.6 | quotaGroupFileSoftLimit(6) | Soft limit on i-node count. |
| 1.7.1.7 | quotaGroupBlockHardLimit(7) | Hard limit on block count. |
| 1.7.1.8 | quotaGroupFileHardLimit(8) | Hard limit on i-node count. |
| 1.7.1.9 | quotaGroupBlockGracePeriod(9) | Time (seconds) remaining for the extended period from when the number of blocks exceeded the soft limit |
| 1.7.1.10 | quotaGroupFileGracePeriod(10) | Time (seconds) remaining for the extended period from when the number of I-nodes exceeded the soft limit |

**Table B.19 >enasExMibNfs(4) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | enasExMibNfsRpcStats(1) | Number of RPC requests since system activation. |
| 1.1 | nfsCALLS(1) | Total number of RPC requests. |
| 1.2 | nfsBADCALLS(2) | Number or requests deleted at the RPC layer. |
| 1.3 | nfsXDRCALL(3) | Number of non-XDR RPC requests. |
| 2 | enasExMibNfsV2ProcCall(2) | Number of received NfsV2 procedure calls. |
| 2.1 | nfsV2ProcNULL(1) | Number or received NULL procedure calls. |
| 2.2 | nfsV2ProcGETATTR(2) | Number of received GETATTR procedure calls. |

| ID | Object Name | Meaning |
|---|---|---|
| 2.3 | nfsV2ProcSETATTR(3) | Number of received SETATTR procedure calls. |
| 2.4 | nfsV2ProcROOT(4) | Number of received ROOT procedure calls. |
| 2.5 | nfsV2ProcLOOKUP(5) | Number of received LOOKUP procedure calls. |
| 2.6 | nfsV2ProcREADLINK(6) | Number of received READLINK procedure calls. |
| 2.7 | nfsV2ProcREAD(7) | Number of received READ procedure calls. |
| 2.8 | nfsV2ProcWRITECACHE(8) | Number of received WRITECACHE procedure calls. |
| 2.9 | nfsV2ProcWRITE(9) | Number of received WRITE procedure calls. |
| 2.10 | nfsV2ProcCREATE(10) | Number of received CREATE procedure calls. |
| 2.11 | nfsV2ProcREMOVE(11) | Number of received REMOVE procedure calls |
| 2.12 | nfsV2ProcRENAME(12) | Number of received RENAME procedure calls. |
| 2.13 | nfsV2ProcLINK(13) | Number of received LINK procedure calls. |
| 2.14 | nfsV2ProcSYMLINK(14) | Number of received SYMLINK procedure calls. |
| 2.15 | nfsV2ProcMKDIR(15) | Number of received MKDIR procedure calls. |
| 2.16 | nfsV2ProcRMDIR(16) | Number of received RMDIR procedure calls. |
| 2.17 | nfsV2ProcREADDIR(17) | Number of received READDIR procedure calls. |
| 2.18 | nfsV2ProcFSSTAT(18) | Number of received FSSTAT procedure calls. |
| 3 | enasExMibNfsV2TotalProcCall(3) | Statistics of individual nfsV2 calls (in %). |
| 3.1 | nfsV2TotalProcNULL(1) | Ratio (%) of NULL procedure calls to total nfsV2 calls. |
| 3.2 | nfsV2TotalProcGETATTR(2) | Ratio (%) of GETATTR procedure calls to total nfsV2 calls. |
| 3.3 | nfsV2TotalProcSETATTR(3) | Ratio (%) of SETATTR procedure calls to total nfsV2 calls. |
| 3.4 | nfsV2TotalProcROOT(4) | Ratio (%) of ROOT procedure calls to total nfsV2 calls. |
| 3.5 | nfsV2TotalProcLOOKUP(5) | Ratio (%) of LOOKUP procedure calls to total nfsV2 calls. |
| 3.6 | nfsV2TotalProcREADLINK(6) | Ratio (%) of READLINK procedure calls to total nfsV2 calls. |
| 3.7 | nfsV2TotalProcREAD(7) | Ratio (%) of READ procedure calls to total nfsV2 calls. |
| 3.8 | nfsV2TotalProcWRITECACHE(8) | Ratio (%) of WRITECACHE procedure calls to total nfsV2 calls. |
| 3.9 | nfsV2TotalProcWRITE(9) | Ratio (%) of WRITE procedure calls to total nfsV2 calls. |
| 3.10 | nfsV2TotalProcCREATE(10) | Ratio (%) of CREATE procedure calls to total nfsV2 calls. |
| 3.11 | nfsV2TotalProcREMOVE(11) | Ratio (%) of REMOVE procedure calls to total nfsV2 calls (%). |
| 3.12 | nfsV2TotalProcRENAME(12) | Ratio (%) of RENAME procedure calls to total nfsV2 calls. |
| 3.13 | nfsV2TotalProcLINK(13) | Ratio (%) of LINK procedure calls to total nfsV2 calls. |
| 3.14 | nfsV2TotalProcSYMLINK(14) | Ratio (%) of SYMLINK procedure calls to total nfsV2 calls. |
| 3.15 | nfsV2TotalProcMKDIR(15) | Ratio (%) of MKDIR procedure calls to total nfsV2 calls. |
| 3.16 | nfsV2TotalProcRMDIR(16) | Ratio (%) of RMDIR procedure calls to total nfsV2 calls. |
| 3.17 | nfsV2TotalProcREADDIR(17) | Ratio (%) of READDIR procedure calls to total nfsV2 calls. |

| ID | Object Name | Meaning |
|---|---|---|
| 3.18 | nfsV2TotalProcFSSTAT(18) | Ratio (%) of FSSTAT procedure calls to total nfsV2 calls. |
| 4 | enasExMibNfsV3ProcCall(4) | Number of received NfsV3 procedure calls. |
| 4.1 | nfsV3ProcNULL(1) | Number of received NULL procedure calls. |
| 4.2 | nfsV3ProcGETATTR(2) | Number of received GETATTR procedure calls. |
| 4.3 | nfsV3ProcSETATTR(3) | Number of received SETATTR procedure calls. |
| 4.4 | nfsV3ProcLOOKUP(4) | Number of received LOOKUP procedure calls. |
| 4.5 | nfsV3ProcACCESS(5) | Number of received ACCESS procedure calls. |
| 4.6 | nfsV3ProcREADLINK(6) | Number of received READLINK procedure calls. |
| 4.7 | nfsV3ProcREAD(7) | Number of received READ procedure calls. |
| 4.8 | nfsV3ProcWRITE(8) | Number of received WRITE procedure calls. |
| 4.9 | nfsV3ProcCREATE(9) | Number of received CREATE procedure calls. |
| 4.10 | nfsV3ProcMKDIR(10) | Number of received MKDIR procedure calls. |
| 4.11 | nfsV3ProcSYMLINK(11) | Number of received SYMLINK procedure calls. |
| 4.12 | nfsV3ProcMKNOD(12) | Number of received MKNOD procedure calls. |
| 4.13 | nfsV3ProcREMOVE(13) | Number of received REMOVE procedure calls. |
| 4.14 | nfsV3ProcRMDIR(14) | Number of received RMDIR procedure calls. |
| 4.15 | nfsV3ProcRENAME(15) | Number of received RENAME procedure calls. |
| 4.16 | nfsV3ProcLINK(16) | Number of received LINK procedure calls. |
| 4.17 | nfsV3ProcREADDIR(17) | Number of received READDIR procedure calls. |
| 4.18 | nfsV3ProcREADDIRPLUS(18) | Number of received READDIRPLUS procedure calls. |
| 4.19 | nfsV3ProcFSSTAT(19) | Number of received FSSTAT procedure calls. |
| 4.20 | nfsV3ProcFSINFO(20) | Number of received FSINFO procedure calls. |
| 4.21 | nfsV3ProcPATHCONF(21) | Number of received PATHCONF procedure calls. |
| 4.22 | nfsV3ProcCOMMIT(22) | Number of received COMMIT procedure calls. |
| 5 | enasExMibNfsV3TotalProcCall(5) | Statistics of individual NfsV3 calls (in %). |
| 5.1 | nfsV3TotalProcNULL(1) | Ratio (%) of NULL procedure calls to total nfsV3 calls. |
| 5.2 | nfsV3TotalProcGETATTR(2) | Ratio (%) of GETATTR procedure calls to total nfsV3 calls. |
| 5.3 | nfsV3TotalProcSETATTR(3) | Ratio (%) of SETATTR procedure calls to total nfsV3 calls. |
| 5.4 | nfsV3TotalProcLOOKUP(4) | Ratio (%) of LOOKUP procedure calls to total nfsV3 calls. |
| 5.5 | nfsV3TotalProcACCESS(5) | Ratio (%) of ACCESS procedure calls to total nfsV3 calls. |
| 5.6 | nfsV3TotalProcREADLINK(6) | Ratio (%) of READLINK procedure calls to total nfsV3 calls. |
| 5.7 | nfsV3TotalProcREAD(7) | Ratio (%) of READ procedure calls to total nfsV3 calls. |
| 5.8 | nfsV3TotalProcWRITE(8) | Ratio (%) of WRITE procedure calls to total nfsV3 calls. |
| 5.9 | nfsV3TotalProcCREATE(9) | Ratio (%) of CREATE procedure calls to total nfsV3 calls. |

| ID | Object Name | Meaning |
|---|---|---|
| 5.10 | nfsV3TotalProcMKDIR(10) | Ratio (%) of MKDIR procedure calls to total nfsV3 calls. |
| 5.11 | nfsV3TotalProcSYMLINK(11) | Ratio (%) of SYMLINK procedure calls to total nfsV3 calls. |
| 5.12 | nfsV3TotalProcMKNOD(12) | Ratio (%) of MKNOD procedure calls to total nfsV3 calls. |
| 5.13 | nfsV3TotalProcREMOVE(13) | Ratio (%) of REMOVE procedure calls to total nfsV3 calls. |
| 5.14 | nfsV3TotalProcRMDIR(14) | Ratio (%) of RMDIR procedure calls to total nfsV3 calls. |
| 5.15 | nfsV3TotalProcRENAME(15) | Ratio (%) of RENAME procedure calls to total nfsV3 calls. |
| 5.16 | nfsV3TotalProcLINK(16) | Ratio (%) of LINK procedure calls to total nfsV3 calls. |
| 5.17 | nfsV3TotalProcREADDIR(17) | Ratio (%) of READDIR procedure calls to total nfsV3 calls. |
| 5.18 | nfsV3TotalProcREADDIRPLUS(18) | Ratio (%) of READDIRPLUS procedure calls to total nfsV3 calls. |
| 5.19 | nfsV3TotalProcFSSTAT(19) | Ratio (%) of FSSTAT procedure calls to total nfsV3 calls. |
| 5.20 | nfsV3TotalProcFSINFO(20) | Ratio (%) of FSINFO procedure calls to total nfsV3 calls. |
| 5.21 | nfsV3TotalProcPATHCONF(21) | Ratio (%) of PATHCONF procedure calls to total nfsV3 calls. |
| 5.22 | nfsV3TotalProcCOMMIT(22) | Ratio (%) of COMMIT procedure calls to total nfsV3 calls. |

**Table B.20 >enasExMibCifs(5) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | enasExMibCifsItem(1) | CIFS item. |
| 1.1 | cifsWorkGroup(1) | Work group name. |
| 1.2 | cifsServerComment(2) | Server comment. |
| 1.3 | cifsSecurity(3) | Authentication method. |
| 1.4 | cifsPasswordServer(4) | Authentication server. |
| 1.5 | cifsSharesCount(5) | Current share count. |
| 1.6 | cifsSessionCount(6) | Current session count. |
| 1.7 | cifsFileDirectory(7) | File being currently locked. |
| 1.7.1 | cifsFileDirEntry (1) | CIFS access entry. |
| 1.7.1.1 | cifsFileDirEntIndex(1) | File index. |
| 1.7.1.2 | cifsFileDirEntName(2) | File name. |

**Table B.21 >enasExMibNetwork(6) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | enasExMibIPAddressTable(1) | IP address. |
| 1.1 | ipAddressEntry(1) | IP address entry. |
| 1.1.1 | ipAddressIFIndex(1) | Network interface index. |
| 1.1.2 | ipAddressAddr(2) | IP address. |
| 2 | enasExMibDefaultGateway(2) | Default gateway. |

**Table B.22 >enasExMibPerformManager(7) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | enasExMibNWPerformManagerTable(1) | Network performance monitoring. |
| 1.1 | netWorkPMEntry(1) | Network performance monitoring entry. |
| 1.1.1 | ipAddressIFIndex(1) | Serial number for each network interface |
| 1.1.2 | nwpmRcvPacket(2) | (This object no longer available.) |
| 1.1.3 | nwpmSendPacket(3) | (This object no longer available.) |
| 1.1.4 | nwpmCollision(4) | Number of collisions. |
| 1.1.5 | nwpmBuffErrRcvPacket(5) | Number of received packet discards due to insufficient buffer. |
| 1.1.6 | nwpmBuffErrSendPacket(6) | (This object no longer available.) |
| 1.1.7 | nwpmPacketSendCareerErr(7) | Carrier error count at packet send. |
| 1.1.8 | nwpmFrmAlignmentErr(8) | Frame alignment error count. |
| 1.1.9 | nwpmFIFOSendOverRunErr(9) | FIFO overrun error count (send). |
| 1.1.10 | nwpmFIFORcvOverRunErr(10) | FIFO overrun error count (receive). |

## B.2 SNMP Traps

If specific-traps for the NAS Modular system are set in the SNMP manager, you can specify whether or not the SNMP manager receives SNMP traps issued by the NAS Modular system. By setting necessary specific-traps in accordance with the operational procedure, you can make the SNMP manager receive the specific traps issued by the NAS Modular system.

The following shows the enterprise-OID of specific-traps for the NAS Modular system.

.1.3.6.1.4.1.116.3.11.5

The following table lists specific-traps for the NAS Modular system:

**Table B.23 Specific Traps for NAS Modular system**

| ID | Object Name | Meaning |
|---|---|---|
| 0 | enasTrapNotice | This trap might be output when a NAS system that uses TagmaStore USP is being used. |
| 1 | enasEventTrapFatalError | A message of the Fatal Error level was received. |
| 2 | enasEventTrapError | A message of the Error level was received. |
| 3 | enasEventTrapWarning | A message of the Warning level was received. |
| 4 | enasEventTrapInformation | A message of the Information level was received. |

| | | |
|---|---|---|
| 5 | enasQuotaTrapFSSoftLimit | A user or group exceeding the soft limit or grace period for the quota assigned to the file system was detected. |
| 6 | enasQuotaTrapFSLimitExceeded | A user or group exceeding the grace period after exceeding the soft limit for the quota assigned to the file system was detected. |
| 7 | enasCoreTrap | A core file was detected. |
| 8 | enasQuotaTrapSummary | A summary trap for quotas was received from the NAS Modular system. |
| 9 | enasQuotaTrapDetailSuppress | A trap for quotas when individual reports are suppressed was received from the NAS Modular system. |

***Note:*** If the SNMP manager cannot be used to monitor the status of a NAS system that uses TagmaStore USP, you must set 0 (enasTrapNotice) for specific-traps.

The following table lists the groups of MIB objects in the NAS Modular system used for SNMP traps and the tables to be referenced for each group:

**Table B.24 Groups of MIB Objects Used in SNMP Traps and Tables to be Referenced**

| Group Name | Description |
|---|---|
| enasExMibQuotaTrapFS(3) | This is a group related to monitoring of the quotas set for file systems. |
| enasExMibEvent(8) | This is a group related to event monitoring. |

Tables B.24 and B.25 summarize the groups of MIB objects used in SNMP traps.

**Table B.25 enasExMibQuotaTrapFS(3) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | quotaTrapFSSoftLimitTable(1) | Information about traps that exceeded the soft limit for the quota assigned to the file system. |
| 1.1 | quotaSoftLimitEntry(1) | Over soft limit trap entry. |
| 1.1.1 | quotaSoftLimitTrapDate(1) | Trap date and time. |
| 1.1.2 | quotaSoftLimitCHAName(2) | NNC name |
| 1.1.3 | quotaSoftLimitCHANumber(3) | NNC number |
| 1.1.4 | quotaSoftLimitRaidNumber(4) | Device ID. |
| 1.1.5 | quotaSoftLimitFSMntPoint(5) | File system mount point. |
| 1.1.6 | quotaSoftLimitType(6) | User or group type. |
| 1.1.7 | quotaSoftLimitName(7) | User or group name. |
| 1.1.8 | quotaSoftLimitID(8) | UID or GID. |
| 1.1.9 | quotaSoftLimitClass(9) | Over limit type (blocks or i-nodes). |
| 1.1.10 | quotaSoftLimitUsed(10) | Current usage. |

| ID | Object Name | Meaning |
|---|---|---|
| 1.1.11 | quotaSoftLimitSoftLimitValue(11) | Soft limit. |
| 1.1.12 | quotaSoftLimitHardLimitValue(12) | Hard limit. |
| 1.1.13 | quotaSoftLimitRemainGracePeriod(13) | Remaining grace time. |
| 2 | quotaTrapFSLimitExceeded(2) | Information about traps that exceeded the grace period for the quota assigned to the file system. |
| 2.1 | quotaLimitExceededEntry(1) | Over grace time trap entry. |
| 2.2.1 | quotaLimitExceededTrapDate(1) | Trap date and time. |
| 2.2.2 | quotaLimitExceededCHAName(2) | NNC name |
| 2.2.3 | quotaLimitExceededCHANumber(3) | NNC number |
| 2.2.4 | quotaLimitExceededRaidNumber(4) | Device ID. |
| 2.2.5 | quotaLimitExceededFSMntPoint(5) | File system mount point. |
| 2.2.6 | quotaLimitExceededType(6) | User or group type. |
| 2.2.7 | quotaLimitExceededName(7) | User or group name. |
| 2.2.8 | quotaLimitExceededID(8) | UID or GID. |
| 2.2.9 | quotaLimitExceededClass(9) | Over limit type (blocks or i-nodes). |
| 2.2.10 | quotaLimitExceededUsed(10) | Current usage. |
| 2.2.11 | quotaLimitExceededSoftLimitValue(11) | Soft limit. |
| 2.2.12 | quotaLimitExceededHardLimitValue(12) | Hard limit. |
| 2.2.13 | quotaLimitExceededGracePeriodValue(13) | Grace time setting. |
| 3 | quotaTrapFSSummary(3) | Information in the summary trap for quotas assigned to the file system. |
| 3.1 | quotaSummaryEntry(1) | Details in the summary trap for quotas |
| 3.1.1 | quotaSummaryTrapDate(1) | Time when trap occurred |
| 3.1.2 | quotaSummaryCHAName(2) | NNC name |
| 3.1.3 | quotaSummaryCHANumber(3) | NNC number |
| 3.1.4 | quotaSummaryRaidNumber(4) | Device ID |
| 3.1.5 | quotaSummaryFSMntPoint(5) | File system name |
| 3.1.6 | quotaSummaryBlockSoftLimitExceedingUsers(6) | Number of users who exceed their block soft limit |
| 3.1.7 | quotaSummaryBlockSoftLimitExceedingGroups(7) | Number of groups that exceed their block soft limit |
| 3.1.8 | quotaSummaryBlockGracePeriodExpiredUsers(8) | Number of users whose block grace period has expired |
| 3.1.9 | quotaSummaryBlockGracePeriodExpiredGroups(9) | Number of groups whose block grace period has expired |
| 3.1.10 | quotaSummaryFileSoftLimitExceedingUsers(10) | Number of users who exceed their file soft limit |
| 3.1.11 | quotaSummaryFileSoftLimitExceedingGroups(11) | Number of groups that exceed their file soft limit |

| ID | Object Name | Meaning |
|---|---|---|
| 3.1.12 | quotaSummaryFileGracePeriodExpiredUser(12) | Number of users whose file grace period has expired |
| 3.1.13 | quotaSummaryFileGracePeriodExpiredGroups(13) | Number of groups whose file grace period has expired |
| 4 | quotaTrapFSDetailSuppress(4) | Information about individual report suppression traps for the quota assigned to the file system |
| 4.1 | quotaDetailSuppressEntry(1) | Details in the trap for quotas when individual reports are suppressed |
| 4.1.1 | quotaDetailSuppressTrapDate(1) | Time when trap occurred |
| 4.1.2 | quotaDetailSuppressCHAName(2) | NNC name |
| 4.1.3 | quotaDetailSuppressCHANumber(3) | NNC number |
| 4.1.4 | quotaDetailSuppressRaidNumber(4) | Device ID |
| 4.1.5 | quotaDetailSuppressFSMntPoint(5) | File system name |
| 4.1.6 | quotaDetailSuppressType(6) | Difference between user quotas and group quotas |
| 4.1.7 | quotaDetailSuppressBlockSoftLimitExceeding(7) | Number of users or groups that exceed their block soft limit |
| 4.1.8 | quotaDetailSuppressBlockGracePeriodExpired(8) | Number of users or groups whose block grace period has expired |
| 4.1.9 | quotaDetailSuppressFileSoftLimitExceeding(9) | Number of users or groups that exceed their file soft limit |
| 4.1.10 | quotaDetailSuppressFileGracePeriodExpired(10) | Number of users or groups whose file grace period has expired |

**Table B.26 enasExMibEvent(8) Group**

| ID | Object Name | Meaning |
|---|---|---|
| 1 | enasExMibEventTrap(1) | Event notification. |
| 1.1 | eventTrapEntry(1) | Event notification trap entry. |
| 1.1.1 | eventTrapDate(1) | Trap date and time. |
| 1.1.2 | eventTrapGenDate(2) | Event date and time. |
| 1.1.3 | eventTrapCHAName(3) | NNC name |
| 1.1.4 | eventTrapCHANumber(4) | NNC number. |
| 1.1.5 | eventRaidNumber(5) | Device ID. |
| 1.1.6 | eventTrapProcessID(6) | Process ID. |
| 1.1.7 | eventTrapProcessName(7) | Process name. |
| 1.1.8 | eventTrapMsgID(8) | Message ID. |
| 1.1.9 | eventTrapMsg(9) | Event message. |
| 1.1.10 | eventTrapImportanceDeg(10) | Severity level. |
| 1.1.11 | eventTrapSameCount(11) | Number of identical events. |
| 1.1.12 | eventTrapFinalGenerationDate(12) | Last event trap date and time. |
| 1.1.13 | eventTrapThreadFlag(13) | Event flag in trap thread |
| 2 | enasExMibCoreTrap(2) | Core trap. |
| 2.1 | coreTrapEntry(1) | Core trap entry. |
| 2.1.1 | coreTrapTrapDate(1) | Trap date and time. |
| 2.1.2 | coreTrapCHAName(2) | NNC name |
| 2.1.3 | coreTrapCHANumber(3) | NNC number. |
| 2.1.4 | coreTrapRaidNumber(4) | Device ID. |
| 2.1.5 | coreTrapGenerationDate(5) | Trap generated date and time. |
| 2.1.6 | coreTrapDirectoryFileName(6) | Directory name and file name. |
| 2.1.7 | coreTrapSize(7) | Size. |
| 2.1.8 | coreTrapSystemDiskFreeSpace(8) | Free space on NAS OS LU. |
| 2.1.9 | coreTrapSystemDiskUse(9) | Usage rate (%) of the system disk. |

The four severity level values `Information`, `Warning`, `Error`, and `Fatal Error` are used for SNMP trap events sent by the MIB object enasExMibEventTrap(1).

See the severity level value (eventTrapImportanceDeg(10)) to identify the event type. The following table shows the severity level values and their meanings:

**Table B.27 Severity Level for SNMP Trap Event**

| Severity Level Value (eventTrapImportanceDeg(10)) | Meaning |
|---|---|
| 0 | Information |
| 10 | Warning |
| 20 | Error |
| 30 | Fatal Error |

For each event, check the message ID (eventTrapMsgID(8)) and message (eventTrapMsg(9)), see the *NAS Error Codes*, and then take appropriate action.

If the SNMP trap event has the severity level `Information` or `Warning`, only the important information is sent, and the message ID is KAQS11112-I. For details on the KAQS11112-I message, see the *NAS Error Codes*.

## B.3 Obtaining a Definition File for Hitachi MIB Objects

When you import the Hitachi MIB object definitions for a NAS Modular system into the SNMP program that the user uses, obtain a definition file from the CD-ROM provided with the NAS Modular system.

Following is a definition file for Hitachi MIB objects:

`\etc\snmp\E-NAS-EX-MIB.txt`

For details on how to load the definition file for Hitachi MIB objects, see the documentation for each SNMP Manager.

# Appendix C Tasks that Require Saving NAS System LUs

This section describes operations that require you to save NAS system LUs, including NAS OS LUs and NAS Cluster Management LUs.

## C.1 Account Administrator Tasks

The following table lists the tasks that are performed by the account administrator and that require NAS system LUs to be saved:

**Table C.1 Account Administrator Tasks**

| Function | Operation | NAS Cluster Management LU Save Required? | Reference |
|---|---|---|---|
| **Log in, log out** | Logging in | | 3.2.1 |
| | Logging out | | 3.2.2 |
| Managing system administrators | Registering a system administrator | Yes | 3.5.2 |
| | Deleting a system administrator | Yes | *3.5.3* |
| | Editing system administrator user information | Yes | 3.5.4 |
| | Changing the password of a system administrator | Yes | 3.5.5 |
| Editing personal information of the account administrator | Editing user information of the account administrator | Yes | 3.6.2 |
| | Changing the password of the account administrator | Yes | 3.6.3 |

***Note:*** When you perform an operation that requires saving a NAS system LU, you must ask the system administrator to save the LU.

## C.2 System Administrator Tasks

The following table lists the tasks that are performed by the system administrator and that require the NAS system LUs to be saved:

**Table C.2 System Administrator Tasks requiring NAS System LUs to be Saved**

| Function | Operation | NAS OS LU | NAS Cluster Management LU | Reference | |
|---|---|---|---|---|---|
| | | | | GUI | Command |
| Log in, log out | Logging in | -- | -- | *4.2.1* | *5.2* |
| | Logging out | -- | -- | *4.2.2* | - |
| Cluster management | Defining a cluster configuration[#1] | Yes | Yes | *4.5.1* | - |

| | | | | | |
|---|---|---|---|---|---|
| | Changing a cluster configuration[#1] | Yes | -- | *4.5.2* | - |
| | Viewing the status of a cluster and nodes | -- | -- | *4.5.3* | *enas_clstatus*<br>*enas_ndstatus* |
| | Stopping or starting a cluster | -- | -- | *4.5.4* | *enas_clstop*<br>*enas_clstart* |
| | Stopping or starting a node | -- | -- | *4.5.5* | *enas_ndstop*<br>*enas_ndstart* |
| | Performing a forced stop for a cluster or node | -- | -- | *4.5.6* | *enas_clstop*<br>*enas_ndstop* |
| | Viewing resource group status | -- | -- | *4.5.7* | *enas_rgstatus* |
| | Stopping or starting a resource group | -- | -- | *4.5.8* | *enas_rgstop*<br>*enas_rgstart* |
| | Performing a forced stop for a resource group | -- | -- | *4.5.9* | *enas_rgstop* |
| | Disabling and restarting resource group monitoring | -- | -- | *4.5.10* | *enas_rgmon* |
| | Changing the execution node of a resource group | -- | -- | *4.5.11* | *enas_rgmove* |
| | Changing the NNC name[#1] | Yes | Yes | *4.5.13* | - |
| Service management | Viewing service information | -- | -- | *4.6.1* | - |
| | Changing the NFS service configuration | -- | -- | *4.6.2* | - |
| | Changing the CIFS service configuration | -- | -- | *4.6.3* | - |
| | Deleting the cached user mapping information from the CIFS service environment | Yes | Yes | *4.6.4(3)* | - |
| | Checking the IDs and names mapped by using RIDs | -- | -- | - | *enas_umidget* |
| | Rejoining the CIFS service to the Active Directory domain | Yes | Yes | *4.6.4(4)* | - |

| | | | | | |
|---|---|---|---|---|---|
| | Viewing public key information | -- | -- | *4.6.5(2)* | *enas_sshkeylist* |
| | Registering a public key | Yes | -- | *4.6.5(2)* | *enas_sshkeyadd* |
| | Deleting a public key | Yes | -- | *4.6.5(3)* | *enas_sshkeydel* |
| | Deleting a public key file | -- | -- | - | *enas_rmfile* |
| | Changing the FTP service configuration | -- | -- | *4.6.6* | - |
| | Starting NFS services[#2] | Yes | -- | *4.6.7(1)* | - |
| | Stopping NFS services | -- | -- | *4.6.7(2)* | - |
| | Restarting NFS services[#2] | Yes | -- | *4.6.7(3)* | - |
| | Starting CIFS services | Yes | Yes | *4.6.7(1)* | - |
| | Stopping CIFS services | -- | -- | *4.6.7(2)* | - |
| | Restarting CIFS services | Yes | Yes | *4.6.7(3)* | - |
| | Starting FTP services | Yes | -- | *4.6.7(1)* | - |
| | Stopping FTP services | Yes | -- | *4.6.7(2)* | - |
| | Restarting FTP services | Yes | -- | *4.6.7(3)* | - |
| System setup | Checking the communication status for a data LAN port | -- | -- | *4.7.1(2)* | - |
| | Changing the negotiation mode for a data LAN port | Yes | -- | *4.7.1(3)* | - |
| | Viewing the trunking information | -- | -- | *4.7.2(1)* | - |
| | Setting link aggregation[#1] | Yes | -- | *4.7.2(2)* | - |
| | Editing link aggregation information[#1] | Yes | -- | *4.7.2(3)* | - |
| | Setting link alternation[#1] | Yes | -- | *4.7.2(4)* | - |
| | Editing link alternation information[#1] | Yes | -- | *4.7.2(5)* | - |
| | Setting cascaded trunking[#1] | Yes | -- | *4.7.2(6)* | - |
| | Editing cascaded trunking information[#1] | Yes | -- | *4.7.2(7)* | - |
| | Link alternation | -- | -- | *4.7.2(8)* | - |
| | Releasing trunking[#1] | Yes | -- | *4.7.2(9)* | - |
| | Viewing interface and network information | -- | -- | *4.7.3(1)* | - |
| | Setting interface and network information[#1] | Yes | -- | *4.7.3(3)* | - |
| | Editing interface and | Yes | -- | *4.7.3(4)* | - |

| | | | | | |
|---|---|---|---|---|---|
| | network information[#1] | | | | |
| | Deleting interface and network information[#1] | Yes | -- | *4.7.3(5)* | - |
| | Setting information about the DNS server, NIS server, and LDAP server for user authentication[#1] | Yes | -- | *4.7.4* | - |
| | Viewing routing information | -- | -- | *4.7.5(1)* | - |
| | Adding routing information[#1] | Yes | -- | *4.7.5(2)* | - |
| | Deleting routing information[#1] | Yes | -- | *4.7.5(3)* | - |
| | Setting the time for synchronization with the NTP server time | Yes | -- | *4.7.6* | - |
| | Viewing the contents of the system log setup file | -- | -- | *4.7.7(1)* | - |
| | Adding a system log transfer destination | Yes | -- | *4.7.7(2)* | - |
| | Changing a system log transfer destination | Yes | -- | *4.7.7(3)* | - |
| | Deleting a system log transfer destination | Yes | -- | *4.7.7(4)* | - |
| | Setting log file size | Yes | -- | *4.7.8* | - |
| | Setting the period for saving the core file | Yes | -- | *4.7.9* | - |
| | Directly editing system files (when you edit `/etc/hosts`)[#1] | Yes | -- | *4.7.10* | - |
| | Directly editing system files (when you edit `/etc/samba/lmhosts`)[#1] | Yes | -- | *4.7.10* | - |
| | Directly editing system files (when you edit `/etc/snmp/snmpd.conf`) | Yes | -- | *4.7.10* | - |
| | Tuning the performance of the system | Yes | -- | *4.7.11* | - |
| | Viewing SNMP information | -- | -- | *4.7.12(1)* | - |
| | Adding SNMP information | Yes | -- | *4.7.12(2)* | - |
| | Editing SNMP information | Yes | -- | *4.7.12(3)* | - |
| | Deleting SNMP information | Yes | -- | *4.7.12(4)* | - |
| | Selecting the user | Yes | -- | *4.7.13* | - |

| | | | | | |
|---|---|---|---|---|---|
| | interface mode | | | | |
| Virus measures[#3] | Viewing the status of a scan server | -- | -- | *4.8.2* | - |
| | Registering a scan server | Yes | -- | *4.8.3* | - |
| | Changing the registration information for a scan server | Yes | -- | *4.8.4* | - |
| | Deleting a registered scan server | Yes | -- | *4.8.5* | - |
| | Setting scan conditions | Yes | -- | *4.8.6* | - |
| | Starting or stopping the virus scanning functionality | Yes | -- | *4.8.7* | - |
| User management | Viewing user information | -- | -- | *4.9.1(1)* | - |
| | Adding users[#1] | Yes | -- | *4.9.1(2)* | - |
| | Editing user information[#1] | Yes | -- | *4.9.1(3)* | - |
| | Changing a password[#1] | Yes | -- | *4.9.1(4)* | - |
| | Deleting users[#1] | Yes | -- | *4.9.1(5)* | - |
| | Registering and deleting user information as a **Batch Operation**[#1] | Yes | -- | *4.9.1(6)* | - |
| | Viewing group information | -- | -- | *4.9.2(1)* | - |
| | Adding groups[#1] | Yes | -- | *4.9.2(2)* | - |
| | Editing group information[#1] | Yes | -- | *4.9.2(3)* | - |
| | Deleting group information[#1] | Yes | -- | *4.9.2(4)* | - |
| File system management | Viewing file system information | -- | -- | *4.10.2(1)* | *enas_fslist* |
| | Creating a file system | -- | Yes | *4.10.3* | *enas_fscreate* |
| | Mounting a file system | -- | Yes | *4.10.4* | *enas_fsmount* |
| | Unmounting a file system | -- | Yes | *4.10.5* | *enas_fsumount* |
| | Expanding file system capacity | -- | Yes | *4.10.6* | - |
| | Deleting a file system | -- | Yes | *4.10.7* | *enas_fsdelete* |
| | Viewing the settings for automatic failover when a file system is blocked | -- | -- | - | *enas_fsautofo*<br>*enas_fsctl* |
| | Enabling automatic failover when a file | -- | -- | - | *enas_fsautofo* |

| | | | | | |
|---|---|---|---|---|---|
| | system is blocked | | | | *enas_fsctl* |
| | Disabling automatic failover when a file system is blocked | -- | -- | - | *enas_fsautofo*<br>*enas_fsctl* |
| | Viewing the warning notification settings | -- | -- | - | *enas_fsfullmsg*<br>*enas_fsctl* |
| | Enabling warning notification | -- | -- | - | *enas_fsfullmsg*<br>*enas_fsctl* |
| | Disabling warning notification | -- | -- | - | *enas_fsfullmsg*<br>*enas_fsctl* |
| | Viewing the file creation time settings | -- | -- | -- | *enas_fsctl* |
| | Enabling recording of the file creation time | -- | -- | -- | *enas_fsctl* |
| | Disabling recording of the file creation time | -- | -- | -- | *enas_fsctl* |
| | Viewing the access suppression status for the file system | -- | -- | - | *enas_fsctl* |
| Directory operation | Creating the directory | -- | -- | - | *enas_dircreate* |
| | Viewing directory attributes | -- | -- | - | *enas_dirlist* |
| | Changing directory attributes | -- | -- | - | *enas_diredit* |
| | Viewing ACL information | -- | -- | - | *enas_dirgetacl* |
| | Setting an ACL | -- | -- | - | *enas_dirsetacl* |
| File sharing management | Viewing information about NFS shares | -- | -- | *4.11.1(1)* | *enas_nfslist* |
| | Creating an NFS share[#1] | Yes | -- | *4.11.1(2)* | *enas_nfscreate* |
| | Editing information about an NFS share[#1] | Yes | -- | *4.11.1(4)* | *enas_nfsedit* |
| | Deleting an NFS share[#1] | Yes | -- | *4.11.1(5)* | *enas_nfsdelete* |
| | Viewing the NFS environment settings of the NAS OS | -- | -- | - | *enas_nfs_opt_list* |
| | Changing the NFS environment settings of the NAS OS | Yes | -- | - | *enas_nfs_opt_set* |

| | | | | | |
|---|---|---|---|---|---|
| | Deleting the mount information for NFS clients | Yes | -- | - | *enas_nfs_mount_del* |
| | Viewing the mount information for NFS clients | -- | -- | - | *enas_nfs_mount_list* |
| | Deleting file lock information for NFS client hosts | -- | -- | - | *enas_nfs_locks_clear* |
| | Viewing information about CIFS shares | -- | -- | *4.11.2(2)* | *enas_cifslist* |
| | Creating a CIFS share | Yes | Yes | *4.11.2(3)* | *enas_cifscreate* |
| | Editing information about a CIFS share | Yes | Yes | *4.11.2(6)* | *enas_cifsedit* |
| | Deleting a CIFS share | Yes | Yes | *4.11.2(7)* | *enas_cifsdelete* |
| Quota management on a file system basis | Viewing information about the quota set for a file system | -- | -- | *4.12.2* | *enas_quotaget* |
| | Setting the user quota for a file system | -- | -- | *4.12.3* | *enas_quotaset* |
| | Setting the group quota for a file system | -- | -- | *4.12.4* | *enas_quotaset* |
| | Setting the default quota for a file system | -- | -- | *4.12.5* | *enas_quotaset* |
| | Setting the quota grace period for a file system | Yes | -- | *4.12.6* | *enas_quotaset* |
| Subtree quota management | Viewing information about the quota set for a directory | -- | -- | - | *stquota* |
| | Viewing information about the user or group quota set for a directory | -- | -- | - | *stquotalist* |
| | Setting the quota for a directory | -- | -- | - | *stquotaset* |
| | Setting the user quota for a directory | -- | -- | - | *stquotaset* |
| | Setting the group quota for a directory | -- | -- | - | *stquotaset* |
| | Setting the default quota for a directory | -- | -- | - | *stquotaset* |
| | Applying the subtree quota for an existing directory | -- | -- | - | *stquotaset* |
| | Setting the quota grace period for a directory | -- | -- | - | *stquotaset* |
| | Removing the quota set | -- | -- | - | *stquotaset* |

| | | | | | |
|---|---|---|---|---|---|
| | for a directory | | | | |
| Error information management | Managing system messages | -- | -- | *4.13.1* | - |
| | Managing system logs | -- | -- | *4.13.2* | - |
| | Managing other types of log files | -- | -- | *4.13.3* | - |
| | Downloading or deleting log files in a **Batch Operation** | -- | -- | *4.13.4* | - |
| | Managing core files | -- | -- | *4.13.5* | - |
| Program management | Viewing program information | -- | -- | *4.14.1* | - |
| | Installing programs | Yes | -- | *4.14.2* | - |
| | Uninstalling programs | Yes | -- | *4.14.2* | - |
| Editing personal information of system administrators | Viewing user information of the system administrator | -- | -- | *4.15.1* | - |
| | Editing user information of the system administrator | -- | Yes | *4.15.2* | - |
| | Changing the password of the system administrator | -- | Yes | *4.15.3* | - |
| Saving NAS System LUs | Enabling and disabling periodic saving of a NAS OS LU | Yes | -- | *4.16.2(2)* | - |
| | Setting up an interval for periodic saving of a NAS OS LU | Yes | -- | *4.16.2(3)* | - |
| | Enabling and disabling periodic saving of a NAS Cluster Management LU | -- | -- | *4.16.3(2)* | - |
| | Setting up an interval for periodic saving of a NAS Cluster Management LU | Yes | -- | *4.16.3(3)* | - |
| Check the network settings and communications | Displaying the network setting information | -- | -- | - | *enas_netstat* |
| | Displaying the connection to a specified host | -- | -- | - | *enas_ping* |
| | Displaying the path that leads to the specified host | -- | -- | - | *enas_traceroute* |
| Manage FC port | Executing the `enas_fcparm` command | Yes | -- | - | *enas_fcparm* |
| Backup and restore operations | Installing NetBackup | -- | -- | #4 | |
| | Granting access permissions for the NDMP server and media | -- | -- | #4 | |

| | | | | |
|---|---|---|---|---|
| | server | | | |
| | Setting up the NDMP storage device | -- | -- | #4 |
| | Adding the NDMP storage unit and policies | -- | -- | #4 |
| | Setting the NDMP environment variables | -- | -- | #4 |
| | Mounting a file system to be backed up or restored | -- | -- | #4 |
| | Delete NFS or CIFS shares from a file system to be backed up or restored | -- | -- | #4 |
| | Backing up or restoring with NetBackup | -- | -- | #4 |
| | Checking the operating status of the NDMP server | -- | -- | #4 |
| | Stopping an NDMP server | -- | -- | #4 |
| | Restarting an NDMP server | -- | -- | #4 |
| | Starting an NDMP server | -- | -- | #4 |
| | Performing a forced stop of the NDMP server | -- | -- | #4 |
| | Changing the password of an NDMP server | -- | -- | #4 |
| | Displaying and modifying NDMP server timeout information | Yes | -- | #4 |
| Tape device management | Executing the `tapeadd` command | Yes | -- | #4 |
| | Executing the `tapedel` command | Yes | -- | #4 |
| | Executing the `tapelist` command | -- | -- | #4 |
| Remote copy operations | Executing the `horc_devlist` command | -- | -- | #4 |
| | Executing the `horc_logremove` command | -- | -- | #4 |
| | Executing the `horc_printenv` command | -- | -- | #4 |
| | Executing the `horc_pvol_freeze` command | -- | -- | #4 |

| | | | | |
|---|---|---|---|---|
| | Executing the `horc_pvol_unfreeze` command | -- | -- | #4 |
| | Executing the `horc_setenv` command | Yes | -- | #4 |
| | Executing the `horc_svol_define` command | -- | Yes | #4 |
| | Executing the `horc_svol_delete` command | -- | Yes | #4 |
| | Executing the `horc_svol_import` command | Yes | Yes | #4 |
| | Executing the `horc_svol_vmdefine` command | -- | Yes | #4 |
| | Executing the `horc_svol_vmdelete` command | -- | Yes | #4 |
| | Executing the `horc_svol_vmimport` command | Yes | Yes | #4 |
| | Executing the `horc_unsetenv` command | Yes | -- | #4 |
| Differential-data snapshot operations | Setting a differential-data storage device | -- | Yes | #5 |
| | Setting an automatic creation schedule | -- | Yes | #5 |
| | Creating a differential-data snapshot (including operations by an automatic creation schedule) | -- | -- | #5 |
| | Deleting a differential-data snapshot and creating a new one at the same time | -- | -- | #5 |
| | Displaying the status of a differential-data snapshot | -- | -- | #5 |
| | Mounting a differential-data snapshot (including operations by an automatic creation schedule) | Yes | Yes | #5 |
| | Unmounting a differential-data snapshot (including operations by an automatic creation schedule) | Yes | Yes | #5 |

| | | | |
|---|---|---|---|
| Automatically creating a file share for a differential-data snapshot | Yes | Yes | #5 |
| Deleting a differential-data snapshot | -- | -- | #5 |
| Removing a differential-data storage device | -- | Yes | #5 |
| Expanding a differential-data storage device | -- | Yes | #5 |
| Changing the configuration of a differential-data storage device | -- | -- | #5 |

***Note 1:*** The NAS OS LU in the other node that makes up the cluster must be saved.

***Note 2:*** The target LU must be saved only when the target LU is started or restarted after the configuration setting is changed.

***Note 3:*** Operation when a NAS Anti Virus Agent license is set up.

***Note 4:*** Operation when a NAS Backup Restore license is set up. For details, see the *Hitachi AMS/WMS NAS Backup Restore User's Guide*.

***Note 5:*** Operation on NAS Sync Image. For details, see the manual *Hitachi AMS/WMS NAS Sync Image User's Guide*

### C.2.1 Operations performed by the system administrator (when using Storage Navigator Modular)

The following table shows the operations performed by the system administrator through Storage Navigator Modular, in which the NAS system LUs need to be saved. For details on how to perform these operations, see the manual *Storage Navigator Modular User's Guide*.

**Table C.3 Sys Admin Ops Requiring NAS System LUs to be Saved (when SN Modular is used)**

| Function | Operation | NAS OS LU | NAS Cluster Management LU |
|---|---|---|---|
| Setting the NTP server | Setting the NTP server#1 | Yes | -- |
| Setting the time zone | Setting the time zone#1 | Yes | -- |
| Setting LAN information for NAS Units | Setting LAN information for NAS Units | Yes | Yes |
| Setting/canceling a license | Locking/unlocking a license | -- | -- |
| Setting the IP address of the LAN port for maintenance | Setting and changing the IP address of the LAN port for maintenance#1 | Yes | -- |

Legend: Yes: Saving is required. --: Saving is not required.

#1: The NAS OS LU in the other node that makes up the cluster must be saved.

## C.3 End User Tasks

The following table lists the tasks that are performed by the end user and that require the NAS system LUs to be saved:

**Table C.4 End-User Tasks**

| Function | Operation | NAS OS LU Save Required? | NAS Cluster Management LU Save Required? | Reference |
|---|---|---|---|---|
| Log in, log out | Logging in | -- | -- | 7.2.1 |
| | Logging out | -- | -- | 7.2.2 |
| Displaying a **List of File Shares** | Viewing a list of NFS file shares | -- | -- | 7.5 |
| | Viewing a list of CIFS file shares | -- | -- | 7.5.1 |
| Displaying information about the quota set for a file system | Viewing user quota information | -- | -- | 7.6.1 |
| | Viewing group quota information | -- | -- | 7.6.2 |
| Changing passwords | Changing your password. See ***Note.*** | Yes | No | 7.7 |
| Editing comments | Editing your user comment. See ***Note.*** | Yes | No | 7.8 |

Legend: Yes = Saving is required - = Saving is not required

***Note:*** Save NAS system LUs periodically in preparation for end users who perform the operations that requires the NAS system LUs to be saved. If an error occurs before the NAS system LUs are saved, an operation that is performed by the end user (for example, changing the password or comment) might be canceled and the previous status restored. If this situation occurs, the system administrator must ask the end user to set the information again.

***Note:*** When an end-user performs an operation that requires a NAS system LU to be saved, the system administrator must save the LU.

## C.4 Maintenance Tasks

When your HDS representative perform operations that require the NAS system LUs to be saved, a system administrator must save the NAS system LUs, as requested by your HDS representative.

The following table lists the tasks that are performed by your HDS representative and require saving the NAS system LUs:

**Table C.5 Maintenance Tasks**

| Function | Operation | NAS OS LU Save Required? | NAS Cluster Management LU Save Required? |
|---|---|---|---|
| Installation or uninstallation for the programs running on a NAS Unit | Performing upgrade installation. See ***Note***. | Yes | -- |
| | Performing version upgrade installation. See ***Note***. | Yes | -- |
| | Performing option program installation. See ***Note***. | Yes | -- |
| | Performing option program uninstallation. See ***Note***. | Yes | -- |
| Routing information settings | Viewing a listing of routing information | -- | -- |
| | Adding routing information. | Yes | -- |
| | Deleting routing information. | Yes | -- |

Legend: Yes = Saving is required - = Saving is not required

***Note:*** The NAS OS LU in the other node that makes up the cluster must be saved.

# Appendix D Output of Network Information

## D.1 Output content of network information

A system administrator can check the routing information and settings for external servers by using the information of the network information log group downloaded from the **List of RAS Information** (Batch-download) window.

The network information log group includes the following log files:

- `enas_routelist.log`
- `log_ifconfig`
- `log_interfaces_check`

The interface names output to these log files differ from the actual names displayed in the NAS Manager GUI. The following table shows the correspondence between the output interface names and the actual names:

**Table D.1 Interface Names Output to enas_routelist.log and log_ifconfig Difference**

| Type | Output interface name | Actual interface name |
|---|---|---|
| Maintenance interface | eth0 | mtp1 |
| Management interface | eth1 | mng1 |
| User interface | eth2 | gbe1 |
| | eth3 | gbe2 |
| | eth4 | gbe3 |
| | eth5 | gbe4 |

For a VLAN interface, the interface name is output in the following format:

*physical-interface-name.VLAN-ID*

Example:

```
eth2.0010
```

Also, the information of interfaces that are used for internal communications between NAS Units (mtp1, stnet0, and stnet1) is output to these log files.

The following sections describe the contents that are output to individual log files.

## D.2 Output content of the enas_routelist.log file

The following shows an output example of the `enas_routelist.log` file.

```
NNC0(DF-NNC0) 2005/08/31 22:04:31
Target     Netmask     Gateway     Flags  MSS Iface
10.208.15.1   255.255.255.255 0.0.0.0     UH    - eth1
172.16.100.0  255.255.255.0  172.16.100.27  UG   400 eth3.0100
172.16.100.0  255.255.255.0  0.0.0.0     U     - eth3.0100
172.19.232.0  255.255.255.0  0.0.0.0     U     - eth3.1000
10.208.151.0  255.255.255.0  0.0.0.0     U     - eth1
172.16.200.0  255.255.255.0  172.16.200.27  UG   400 eth2.0200
172.16.200.0  255.255.255.0  0.0.0.0     U     - eth2.0200
172.19.243.0  255.255.255.0  0.0.0.0     U     - eth3.1011
172.16.110.0  255.255.255.0  172.16.110.27  UG  65535 eth4.0110
172.16.110.0  255.255.255.0  0.0.0.0     U     - eth4.0110
172.16.120.0  255.255.255.0  172.16.120.27  UG  65535 eth5.0120
172.16.120.0  255.255.255.0  0.0.0.0     U     - eth5.0120
172.29.1.0   255.255.255.0  0.0.0.0     U     - stnet0
172.19.231.0  255.255.255.0  0.0.0.0     U     - eth2.0999
172.29.2.0   255.255.255.0  0.0.0.0     U     - stnet1
10.197.181.0  255.255.255.0  0.0.0.0     U     - eth0
default     0.0.0.0     10.208.151.1  UG    - eth1
```

The following table lists and describes the information that is output to the `enas_routelist.log` file.

**Table D.2 Information That Is Output to the enas_routelist.log File**

| Output line | Output contents |
|---|---|
| Line 1 | Outputs the title in the following format:<br><br>*NNC-number*（*NNC-name*）*output-date*<br><br>The output date and time appear in the format of *YYYY*/*MM*/*DD hh*:*mm*:*ss*, for example, `2004/11/22 13:14:15`. |
| Line 2 | Outputs the column header for the items output in the third line and below. |
| Line 3 and below | Outputs the contents of each item:<br>`Target`<br>Outputs the network address of the output target. For the default route, `default` is output.<br>`Netmask`<br>Outputs the netmask of the output target network. `255.255.255.255` is output for the host. `0.0.0.0` is output for the default route.<br>`Gateway`<br>Outputs the IP address of the gateway.<br>`Flags`<br>Outputs the following statuses of the output target network:<br>`U`<br>Indicates the route is enabled.<br>`H` |

| | |
|---|---|
| | Indicates the target is the host.<br>`G`<br>Indicates the gateway is used.<br>`R`<br>Indicates a recoverable dynamic route.<br>`D`<br>Indicates the dynamic settings made by demon or replacement.<br>`M`<br>Indicates the changes made by route control demon or replacement.<br>`A`<br>Indicates the settings are made by the `addrconf` command.<br>`C`<br>Indicates a cache entry.<br>`!`<br>Indicates a rejected route.<br>`MSS`<br>Outputs the default maximum segment in the TCP connection of this route. When a routing is added and this item is not set, `-` is output.<br>`Iface`<br>Outputs the interface name. |

### D.2.1 Output content of the log_ifconfig File

The following shows an output example of the `log_ifconfig` file.

```
eth0    Link encap:Ethernet HWaddr 00:00:E1:2D:65:70
      inet addr:10.197.181.90 Bcast:10.197.181.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:4400 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3697 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:618930 (604.4 KiB) TX bytes:1501472 (1.4 MiB)
      Interrupt:25

eth1    Link encap:Ethernet HWaddr 00:00:E1:2D:65:71
      inet addr:10.208.136.42 Bcast:10.208.136.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:38081 errors:0 dropped:0 overruns:0 frame:0
      TX packets:14544 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:3502569 (3.3 MiB) TX bytes:5978244 (5.7 MiB)
      Interrupt:26

eth2    Link encap:Ethernet HWaddr 00:00:E1:2D:65:6D
      inet addr:192.168.31.200 Bcast:192.168.31.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:24 errors:0 dropped:0 overruns:0 frame:0
      TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:2450 (2.3 KiB) TX bytes:5376 (5.2 KiB)
      Interrupt:73

lo     Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:729842 errors:0 dropped:0 overruns:0 frame:0
      TX packets:729842 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:73319957 (69.9 MiB) TX bytes:73319957 (69.9 MiB)

stnet0   Link encap:Ethernet HWaddr 00:00:00:00:00:00
      inet addr:172.29.1.1 Mask:255.255.255.0
      UP RUNNING NOARP MTU:2016 Metric:1
      RX packets:2952 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3111 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:32
      RX bytes:2314152 (2.2 MiB) TX bytes:2557166 (2.4 MiB)

stnet1   Link encap:Ethernet HWaddr 00:00:00:00:00:00
      inet addr:172.29.2.1 Mask:255.255.255.0
      UP RUNNING NOARP MTU:2016 Metric:1
      RX packets:33472 errors:0 dropped:0 overruns:0 frame:0
      TX packets:33585 errors:0 dropped:1 overruns:0 carrier:0
      collisions:0 txqueuelen:32
      RX bytes:2549800 (2.4 MiB) TX bytes:3153234 (3.0 MiB)
```

The following table lists and describes the information that is output to the `log_ifconfig` file.

**Table D.3 Information That Is Output to the log_ifconfig File**

| Output item | Output contents |
|---|---|
| ethx (x is a variable value.) | Outputs an interface name. When lo is output for the interface name, it indicates a loopback. Also, ethx: y is sometimes displayed (y is a variable value). y is the alias number for the actual IP address. Only the service IP address#1 is output in this format. 0 is output for the service IP address that belongs to the resource group of the node where log_ifconfig is output. 1 is output when a failover is occurring in the resource group of the other node. |
| Link encap | Outputs the type of the link media. |
| HWaddr | Outputs the MAC address. |
| inet addr | Outputs the IP address. |
| Bcast | Outputs the broadcast address. |
| Mask | Outputs the subnet mask. |
| UP | Outputs UP when the interface is running. |
| BROADCAST | Outputs BROADCAST when the broadcast is used. |
| RUNNING | Outputs RUNNING when the interface is in a ready state. |
| MULTICAST | Outputs MULTICAST when multicast is enabled. |
| MTU | Outputs the MTU size. |
| Metric | Outputs a metric value. |
| RX, TX | Outputs a statistical value of the interface. |
| Interrupt | Outputs the interrupt number used by the interface. |

#1: If resource groups have been failed over or stopped, the information of service IP addresses might not be output to the log_ifconfig file, or that the information of both nodes is output. For example, when the nodes NAS-01 and NAS-02 make up a cluster, the output information varies as follows depending on the condition.

When a resource group on the node NAS-01 has been stopped

The information of service IP addresses for the node NAS-01 is not output to the log_ifconfig file.

When a resource group on the node NAS-02 has been failed over to the node NAS-01

As the information of service IP addresses for the node NAS-01, the information of the nodes NAS-01 and NAS-02 is output to the log_ifconfig file.

### Output content of the log_interfaces_check file

The following shows an example output of the `log_interfaces_check` file.

```
Checking DNS configuration...
OK

Checking NIS configuration...
OK

Checking NTP configuration...
OK

Checking LDAP configuration (for user authentication)...
OK

Checking authentication server configuration (for CIFS)...
OK

Checking LDAP configuration (for user mapping)...
unusing LDAP
```

Connection statuses between a NAS Unit and various servers (as shown in the following table) are output to the `log_interfaces_check` file.

**Table D.4 Connection Statuses That Are Output to the log_interfaces_check File**

| Messages | Description | See |
|---|---|---|
| `Checking DNS configuration...` | Connection status between a NAS Unit and the DNS server is output. | 0 |
| `Checking NIS configuration...` | Connection status between a NAS Unit and the NIS server is output. | 0 |
| `Checking NTP configuration...` | Connection status between a NAS Unit and the NTP server is output. | 0 |
| `Checking LDAP configuration (for user authentication)...` | Connection status between a NAS Unit and the LDAP server for user authentication is output. | 0 |
| `Checking authentication server configuration (for CIFS)...` | Connection status between a NAS Unit and the authentication server for CIFS clients is output. | 0 |
| `Checking LDAP configuration (for user mapping)...` | Connection status between a NAS Unit and the LDAP server for user mapping is output. | 0 |

If there are problems on several servers, the message **Aborted: More than 1 errors occurred** might be output, and the connection status between a NAS Unit and the individual server is not output.

## Connection statuses of the DNS server

The following table lists and describes the output information that shows the connection statuses between a NAS Unit and the DNS server.

**Table D.5 Output Showing Connection Statuses Between a NAS Unit and DNS Server**

| Messages | Description | Action |
|---|---|---|
| `OK` | A DNS server has been correctly specified. | None. |
| `unusing DNS` | A DNS server has not been specified in NAS Manager. | When you use a DNS server, specify the information of the DNS server in the **DNS, NIS, LDAP Setup** window. |
| `Warning: DNS server does not respond.`<br>`No respond servers:` *IP-address-of-the-DNS-server-specified-in-NAS-Manager* | The DNS server specified in NAS Manager does not respond. | Make sure that the following are satisfied:<br>▪ Devices on the path between the NAS Unit and the DNS server to be used are working normally.<br>▪ The IP address of the DNS server that is specified in NAS Manager is correct.<br>▪ The DNS server is working normally. |
| `Warning: DNS server's domain differs from default domain name.`<br>`DNS server's domain:` *domain-name-for-which-the-DNS-server-responded*<br>`default domain name:` *default-domain-name-specified-in-NAS-Manager* | The default domain name specified in NAS Manager has not been registered in the DNS server. In the DNS server, *domain-name-for-which-the-DNS-server-responded* has been registered. | Make sure that the default domain name is correctly specified in the **DNS, NIS, LDAP Setup** window. |
| `Error: cannot access DNS server.` *cause-of-the-error* | Another error has occurred. | Contact the maintenance personnel. |

## Connection statuses of the NIS server

The following table lists and describes the output information that shows the connection statuses between a NAS Unit and the NIS server.

**Table D.6 Output Showing Connection Statuses Between NAS Unit and NIS Server**

| Messages | Description | Action |
|---|---|---|
| `OK` | An NIS server has been correctly specified. | None. |
| `unusing NIS` | An NIS server has not been | When you use an NIS server, specify the information of the NIS |

| | | |
|---|---|---|
| | specified. | server in the **DNS, NIS, LDAP Setup** window. |
| `Warning: NIS server does not respond.`<br>`No respond servers:` *name-or-IP-address-of-the-NIS-server-specified-in-NAS-Manager*#1 | The NIS server specified in NAS Manager does not respond. | Make sure that the following are satisfied:<br>▪ Devices on the path between the NAS Unit and the NIS server to be used are working normally.<br>▪ The name or IP address of the NIS server that is specified in NAS Manager is correct.<br>▪ The NIS server is working normally. |
| `Warning: The specified NIS server name cannot be resolved.`<br>`NIS server name:` *name-of-the-NIS-server-specified-in-NAS-Manager* | Resolving the name of the NIS server specified in NAS Manager failed. | Make sure that the name of the NIS server can be correctly resolved. |
| `Warning: The specified NIS domain is invalid.`<br>`NIS domain name:` *NIS-domain-name-of-the-NIS-server-specified-in-NAS-Manager* | The NIS domain name specified in NAS Manager is incorrect. | Make sure that the NIS domain name is correctly specified in the **DNS, NIS, LDAP Setup** window. |
| `Error: cannot access NIS server.` *cause-of-the-error* | Another error has occurred. | Contact the maintenance personnel. |

#1: When the broadcast is used, Broadcast is displayed.

## Connection statuses of the NTP server

The following table lists and describes the output information that shows the connection statuses between a NAS Unit and the NTP server.

**Table D.7 Output Showing Connection Statuses Between NAS Unit and NTP Server**

| Messages | Description | Action |
|---|---|---|
| `OK` | An NTP server has been correctly specified. | None. |
| `Error: unusing NTP` | An NTP server has not been specified. | Use Storage Navigator Modular to specify the NTP server. |
| `Warning: NTP server does not respond.`<br>`No respond servers:` *name-or-IP-address-of-the-NTP-server-specified-in-NAS-Manager* | The NTP server specified in NAS Manager does not respond. | Make sure that the following are satisfied:<br>▪ Devices on the path between the NAS Unit and the NTP server to be used are working normally.<br>▪ The name or IP address of the NTP server specified in NAS |

| | | |
|---|---|---|
| | | Manager is correct.<br>▪ The NTP server is working normally. |
| `Warning: The specified NTP server name cannot be resolved.`<br>`NTP server name:` *name-of-the-NTP-server-specified-in-NAS-Manager* | Resolving the name of the NTP server specified in NAS Manager failed. | Make sure that the name of the NTP server can be correctly resolved. |
| `Error: cannot access NTP server.` *cause-of-the-error* | Another error has occurred. | Contact the maintenance personnel. |

## Connection statuses of the LDAP server for user authentication

The following table lists and describes the output information that shows the connection statuses between a NAS Unit and the LDAP server for user authentication.

**Table D.8 Output Statuses Between NAS Unit and LDAP Server for User Auth**

| Messages | Description | Action |
|---|---|---|
| `OK` | An LDAP server for user authentication has been correctly specified. | None. |
| `unusing LDAP` | An LDAP server for user authentication has not been specified. | When you perform user authentication on an LDAP server, specify the information of the LDAP server in the **DNS, NIS, LDAP Setup** window. |
| `Error: LDAP server(`*IP-address-of-the-LDAP-server-specified-in-NAS-Manager*`:`*port-number*`) has not been connected.` | The LDAP server specified in NAS Manager does not respond. | Make sure that the following are satisfied:<br>▪ Devices on the path between the NAS Unit and the LDAP server to be used are working normally.<br>▪ The name or IP address of the LDAP server specified in NAS Manager is correct.<br>▪ The LDAP server is working normally. |
| `Warning: LDAP server(`*IP-address-of-the-LDAP-server-specified-in-NAS-Manager*`:`*port-number*`) has been connected, but the time limitation occurred.` | A timeout occurred while checking the connection between a NAS Unit and the LDAP server specified in NAS Manager. | Make sure that the information of the LDAP server is correctly specified in the **DNS, NIS, LDAP Setup** window. |
| `Warning: LDAP server(`*IP-address-of-the-LDAP-server-specified-in-NAS-Manager*`:`*port-number*`) has been connected, but the size limitation` | The number of entries that can be acquired from the LDAP server (which is specified in NAS Manager) has reached the limit. The number of entries that can be acquired from the LDAP server | Make sure that the information of the LDAP server is correctly specified in the **DNS, NIS, LDAP Setup** window. Also, check the setting for the number of entries that can be acquired from the LDAP server. |

| | | |
|---|---|---|
| occurred. | might be limited. | |
| Warning: The password of LDAP administrator seems to be invalid. | The password of the LDAP server administrator set in NAS Manager is incorrect. | Check whether the password of the LDAP server administrator has been set correctly. |
| Error: /etc/libnss-ldap.conf is not found. | The configuration file for the LDAP server does not exist. There might be a problem in the NAS OS. | Contact the maintenance personnel. |

## Connection statuses of the authentication server for CIFS clients

The following table lists and describes the output information that shows the connection statuses between a NAS Unit and the authentication server for CIFS clients (the domain controller or Windows NT server).

**Table D.9 Output Statuses Between NAS Unit and Auth Server for CIFS Clients**

| Messages | Description | Action |
|---|---|---|
| OK | An authentication server for CIFS clients has been correctly specified. | None. |
| unusing authentication server | NAS Manager authenticates CIFS clients. The NT server authentication, NT domain authentication, and Active Directory are not used. | When you use the NT server authentication, NT domain authentication, or Active Directory, specify the information of the server to be used in the **CIFS Service Management** window. |
| Error: rpc error. Server: *name-of-the-authentication-server-specified-in-NAS-Manager* | The authentication server for CIFS clients that is specified in NAS Manager does not respond. | Make sure that the following are satisfied:<br>▪ Devices on the path between the NAS Unit and the authentication server for CIFS clients (which is used) are working normally.<br>▪ The name or IP address of the authentication server for CIFS clients that is specified in NAS Manager is correct.<br>▪ The authentication server for CIFS clients is working normally. |
| Error: timeout. Server: *name-of-the-authentication-server-specified-in-NAS-Manager* | A timeout occurred while checking the connection with the authentication server for CIFS clients that is specified in NAS Manager. | Make sure that the following are satisfied:<br>▪ Devices on the path between the NAS Unit and the authentication server for CIFS clients (which is used) are normally working.<br>▪ The name or IP address of the authentication server for CIFS clients that is specified in NAS Manager is correct.<br>▪ The authentication server for CIFS clients is working |

| | | |
|---|---|---|
| | | normally. |
| `Error: name resolution failure. Server:` *name-of-the-authentication-server-specified-in-NAS-Manager* | Resolving the name of the authentication server for CIFS clients failed. | Make sure that the name of the CIFS server can be correctly resolved. |
| `Error:` *cause-of-the-error.* `Server:` *name-of-the-authentication-server-specified-in-NAS-Manager* | Another error has occurred. | Contact the maintenance personnel. |

## Status of the connection with the LDAP server for user mapping

The following table lists and describes the output information that shows the connection statuses between a NAS Unit and the LDAP server for user mapping.

**Table D.10 Output Statuses Between NAS Unit and LDAP Server for User Mapping**

| Messages | Description | Action |
|---|---|---|
| `OK` | An LDAP server for user mapping has been correctly specified. | None. |
| `unusing LDAP` | An LDAP server for user mapping has not been specified. | When you use an LDAP server for user mapping, specify the information of the LDAP server in the **CIFS Service Management** window. |
| `Error: LDAP search timeout.` | The LDAP server specified in NAS Manager does not respond. | Make sure that the following are satisfied:<br>▪ Devices on the path between the NAS Unit and the LDAP server to be used are working normally.<br>▪ The name or IP address of the LDAP server specified in NAS Manager is correct.<br>▪ The LDAP server is working normally. |
| `Error: LDAP server name or LDAP server port number is invalid.` | The name or port number of the LDAP server that is specified in NAS Manager is incorrect, or the LDAP server has been stopped. | Make sure that the following are satisfied:<br>▪ Devices on the path between the NAS Unit and the LDAP server to be used are working normally.<br>▪ The name or IP address of the LDAP server that is specified in NAS Manager is correct.<br>▪ The LDAP server is working normally. |
| `Error: LDAP suffix is not specified.` | The LDAP server root DN has not been specified in NAS Manager. | Specify the LDAP server root DN in the **CIFS Service Management** window. |

| | | |
|---|---|---|
| `Error: LDAP administrator DN is not specified.` | The LDAP server administrator DN has not been specified in NAS Manager. | Specify the LDAP server administrator DN in the **CIFS Service Management** window. |
| `Error: LDAP administrator password is not specified.` | The LDAP server administrator password has not been specified in NAS Manager. | Specify the LDAP server administrator password in the **CIFS Service Management** window. |
| `Error: LDAP user map DN or LDAP server root DN is invalid.` | One of the following specified in NAS Manager is incorrect:<br>▪ The user mapping account DN<br>▪ LDAP server root DN | Make sure that each DN is correctly specified in the **CIFS Service Management** window. |
| `Error: LDAP administrator password is invalid.` | The LDAP server administrator password specified in NAS Manager is incorrect. | Check the password specified in the LDAP server, and then change the password in the **CIFS Service Management** window. |
| `Error: LDAP server root DN or LDAP administrator DN or LDAP administrator password is invalid.` | The LDAP server administrator DN specified in NAS Manager is incorrect. | Make sure that the LDAP server administrator DN is correctly specified in the **CIFS Service Management** window. |
| `Error: objectClass=sambaUnixIdPool does not exist.` | The initial setup for the LDAP server failed. Entries used for user mapping cannot be updated. | Restart the CIFS service after confirming that:<br>▪ The schema file created for the LDAP server has been loaded correctly.<br>▪ Write permissions have been set on the entries to be used for user mapping.<br>▪ The user specified for the LDAP server administrator DN in the **CIFS Service Management** window has administrator privileges. |
| `Error: objectClass=sambaUnixIdPool is multiple.` | The initial settings for the LDAP server are incorrect. | Multiple entries that were used for the LDAP user mapping account exist on the specified LDAP server. Among those entries, delete the entries other than ones used for the LDAP user mapping account entry specified in the **CIFS Service Management** window. |
| `Error: open smb.conf failed.` | The `/etc/samba/smb.conf` file could not be opened because of a problem in the NAS OS. | Contact the maintenance personnel. |
| `Error: open cifs.conf failed.` | The `/enas/conf/cifs.conf` file could not be opened because of a problem in the NAS OS. | Contact the maintenance personnel. |
| `Error: cannot access LDAP server.` *cause-of-the-error* | Another error has occurred. | Contact the maintenance personnel. |

# Appendix E Checking Network Communication

## E.1 Checking Network Communication

When necessary, a system administrator checks whether communication can be established between the NAS Modular system and a client. This section describes how to check communication between the NAS Modular system and a client, and actions to be taken when communication cannot be established.

### E.1.1 Checking items that are prerequisite for network communication

To check items that are prerequisite for communication between a NAS Modular system and a client:

1. From the client, execute the `ping` command for a machine that belongs to the same network as the NAS Modular system, or for the router that routs communications.

   Make sure that the client can communicate with machines that do not belong to the NAS Modular system, and that it cannot communicate only with the NAS Modular system. If the client cannot communicate with machines that do not belong to the NAS Modular system, make sure that relay devices are running normally. For example, make sure that relay devices such as switches and routers are powered on, and all cables are plugged in.

2. In the **List of RAS Information** window, make sure that a warning-level link-down message is not output.

   If a warning-level link-down message is output, contact maintenance personnel.

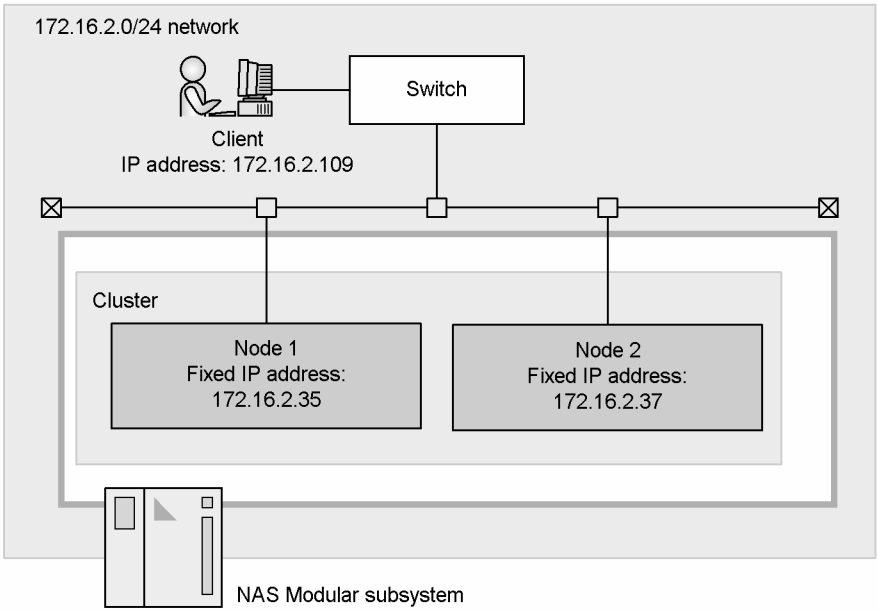
3. In the **List of RAS Information** window, make sure that the message KAQG70000-E is not output (make sure that a failover is not occurring).

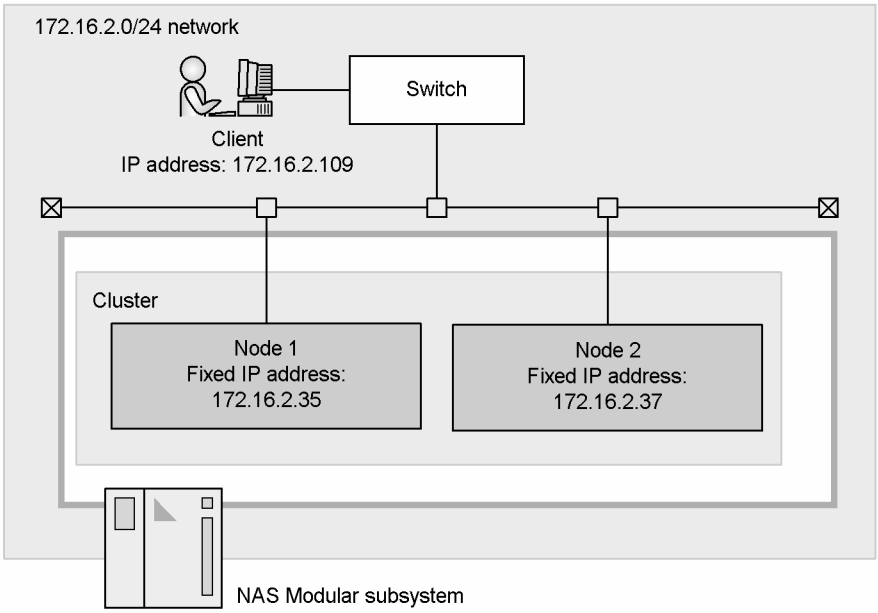
   If a failover is occurring, contact maintenance personnel.

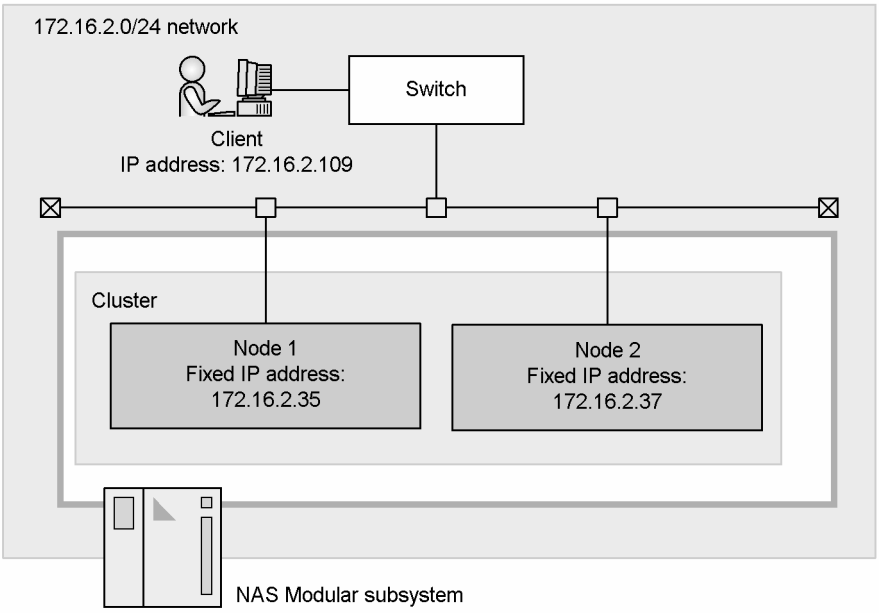
### E.1.2 Performing checks for each network configuration

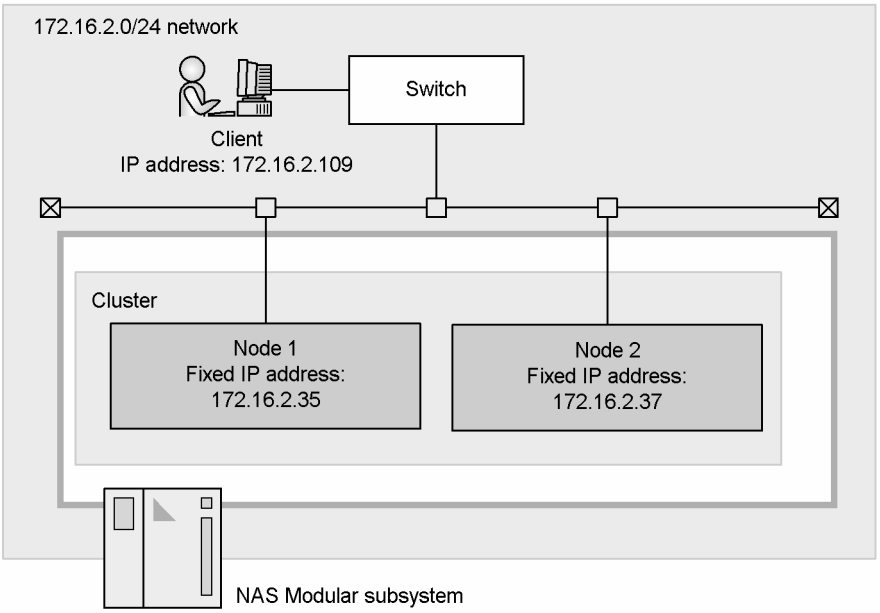
Before checking network communication, check whether the NAS Modular system and the client belong to the same network.

The following shows an example when the NAS Modular system and the client belong to the same network.


172.16.2.0/24 network
Switch
Client
IP address: 172.16.2.109
Cluster
Node 1
Fixed IP address:
172.16.2.35
Node 2
Fixed IP address:
172.16.2.37
NAS Modular subsystem


172.16.2.0/24 network
Switch
Client
IP address: 172.16.2.109
Cluster
Node 1
Fixed IP address:
172.16.2.35
Node 2
Fixed IP address:
172.16.2.37
NAS Modular subsystem


172.16.2.0/24 network
Switch
Client
IP address: 172.16.2.109
Cluster
Node 1
Fixed IP address:
172.16.2.35
Node 2
Fixed IP address:
172.16.2.37
NAS Modular subsystem


172.16.2.0/24 network
Switch
Client
IP address: 172.16.2.109
Cluster
Node 1
Fixed IP address:
172.16.2.35
Node 2
Fixed IP address:
172.16.2.37
NAS Modular subsystem

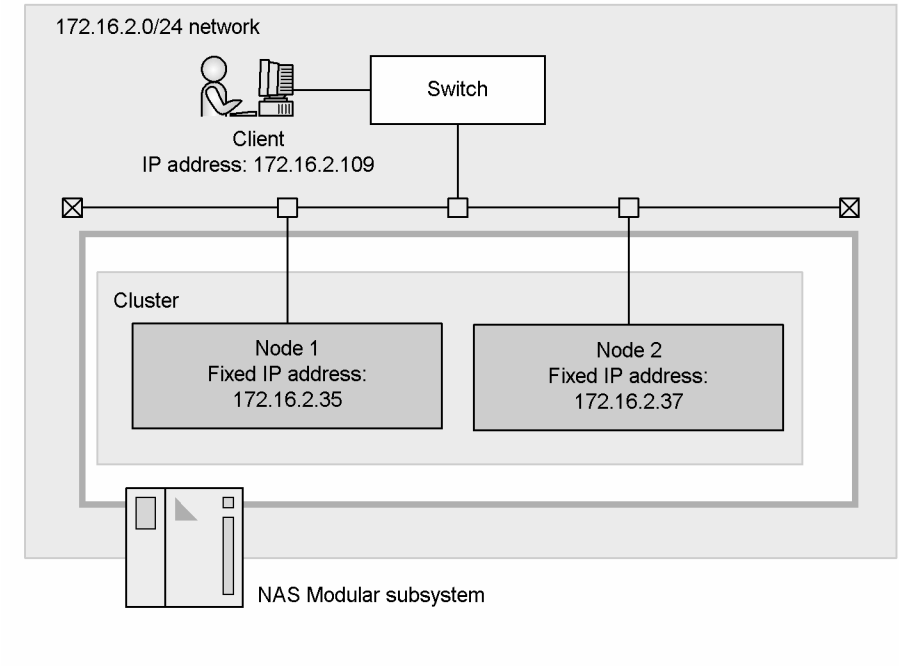



**Figure E.1 Configuration When NAS Modular System and Client in Same Network**

The following shows an example when the NAS Modular system and the client belong to different networks.

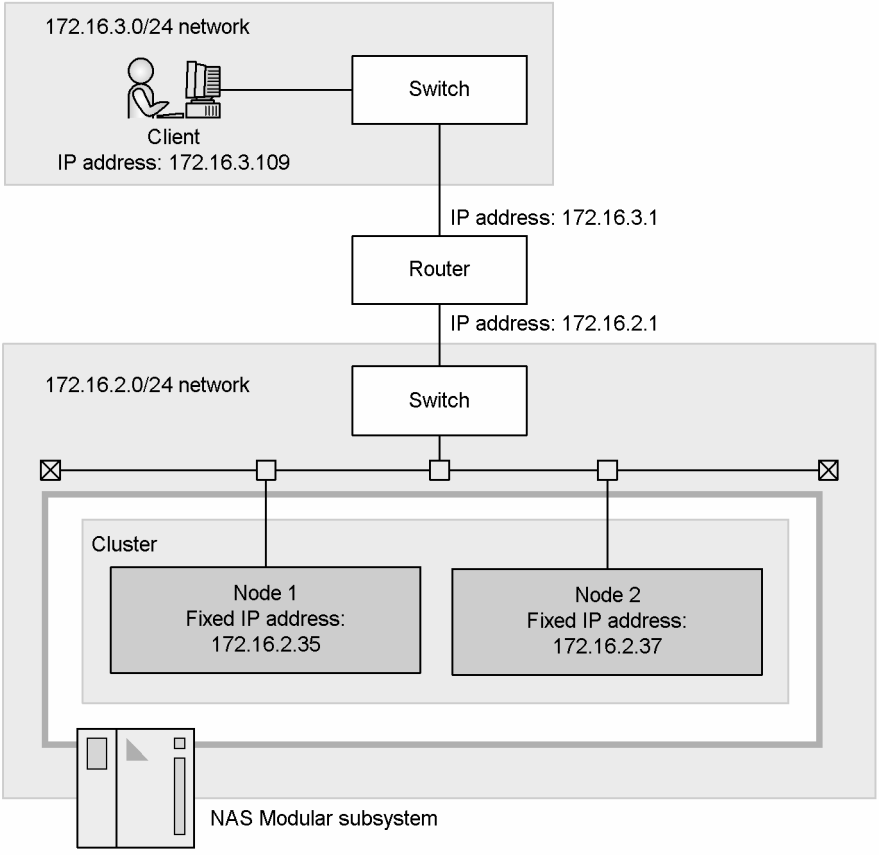



**Figure E.2 Configuration When NAS Modular System and Client in Different Networks**

### E.1.3 Checking communication within the network

When the NAS Modular system and the client belong to the same network, perform the following steps to check the communication within the network. When the NAS Modular system and the client belong to different networks, perform the same steps, assuming the router is the client.

To check communication within the network:

1. From one node, specify the fixed IP address of the other node, and execute the `enas_ping` command.

   If communication cannot be established, the setting of the IP address or netmask for the NAS Modular system is invalid, or the setting of the VLAN for the NAS Modular system or switch is invalid. For actions to be taken, see 0 and 0.

2. From one node, specify the `-s` option in the `enas_ping` command, and execute it for the other node.

If communication cannot be established, the setting of the MTU value for the NAS Modular system or switch is invalid. For actions to be taken, see 0.

3. Execute the `enas_ping` command for the client.

   If communication cannot be established, the setting of the IP address or netmask for the client is invalid, or the setting of the VLAN for the switch or client is invalid. For actions to be taken, see 0 and 0.

4. Specify the `-s` option in the `enas_ping` command, and execute it for the client.

   If communication cannot be established, the setting of the MTU value for the switch or client is invalid. For actions to be taken, see 0.

### E.1.4 Checking communication between different networks

To check communication between different networks when the NAS Modular system and the client belong to different networks:

1. Specify the network gateway address on the client side, and execute the `enas_ping` command.

   When `Network is unreachable` is output, the routing setting for the NAS Modular system is invalid. When the communication cannot be established, the routing setting for the router is invalid. For actions to be taken, see 0.

2. Specify the `-n` option and the client's IP address in the `enas_traceroute` command, and execute it.

   If communication cannot be established, an error occurs in the network from the router to the client. Check if there are any problems from the router to the client.

### E.1.5 Actions to be taken when communication cannot be established

If you check the network communication and find that communication is not available, you must check the settings. If the settings are invalid, change them to the correct settings, and check the operation again.

### E.1.6 Checking the IP address and netmask

Check the network addresses for the NAS Modular system and client.

- NAS Modular system: In the **List of Interfaces** window, check the fixed IP address, service IP address, and netmask.
- Client: Check the IP address and netmask.

If the network addresses for the NAS Modular system and the client are different, change the settings to be the same network address.

### E.1.7 Checking the VLAN ID

When the VLAN is set, check the VLAN settings for the NAS Modular system, switch, and client.

NAS Modular system

Check the VLAN ID in the **List of Interfaces** window.

Switch

Check the VLAN setting for the port connected to the NAS Modular system and client. When multiple switches are routed, check the VLAN setting for the port connected between switches. Also, check whether the port is set to be tagged or untagged.

Client

When the tagged VLAN is set, check the VLAN ID for the tagged VLAN.

If the VLAN ID settings are different among the NAS Modular system, switch, and client, change the setting so that they have the same VLAN ID. If the tagged or untagged setting for the switch is incorrect, specify the correct setting.

### E.1.8 Checking the MTU value

When you change the MTU setting, for example, to use a Jumbo Frame, check the settings of the MTU values for the NAS Modular system, switch, and client.

NAS Modular system

Check the MTU value in the **List of Interfaces** window.

Switch

Check the MTU value of the port connected to the NAS Modular system and client. When multiple switches are routed, check the MTU value for the port connected between switches.

Client

Check the MTU value.

When the MTU value for the switch is smaller than the MTU values set for the NAS Modular system and client, increase the value for the switch so that it is larger than the values for the NAS Modular system and client.

### E.1.8 Checking the routing

Check whether gateways appropriate for the NAS Modular system, router, switch, and client are set.

NAS Modular system

In the List of Routing window, check whether the gateways (such as router and switch) that can reach the client are specified.

Router and switch

Check whether the gateways that can reach the client and NAS Modular system are specified.

Client

Check whether the gateways that can reach the NAS Modular system are specified.

If gateways appropriate for the NAS Modular system, router, switch, and client are not set, change the appropriate gateway setting.

## Examples of checking network communication

This section describes examples of checking the network communication.

## Example of checking a network by using the enas_ping command

The following describes an example of checking a network by using the `enas_ping` command.

Successful example:

The following gives an example of command execution and an explanation when the communication is successful.

```
$ sudo enas_ping 172.16.2.109 -c 3
PING 172.16.2.109 (172.16.2.109): 56 data bytes
64 bytes from 172.16.2.109: icmp_seq=0 ttl=255 time=1.7 ms
64 bytes from 172.16.2.109: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 172.16.2.109: icmp_seq=2 ttl=255 time=0.2 ms

--- 172.16.2.109 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.7/1.7 ms
$
$
$ sudo enas_ping 172.16.2.109 -c 3 -s 9000
PING 172.16.2.109 (172.16.2.109): 9000 data bytes
9008 bytes from 172.16.2.109: icmp_seq=0 ttl=255 time=3.8 ms
9008 bytes from 172.16.2.109: icmp_seq=1 ttl=255 time=0.9 ms
9008 bytes from 172.16.2.109: icmp_seq=2 ttl=255 time=1.0 ms

--- 172.16.2.109 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.9/1.9/3.8 ms
$
```

The first `enas_ping` command sent a 56-byte ICMP packet to the machine with the IP address of `172.16.2.109` for three times, and the machine received it three times. From the result, you can see that communication was performed correctly. The next `enas_ping` command sent a 9,000-byte ICMP packet to the same client, and the packet loss was 0%. The communication at this time was also performed correctly.

Failed example 1:

The following gives an execution example and explanation when the NAS Modular system cannot communicate with a machine in the same network.

```
$ sudo enas_ping 172.16.2.109 -c 3
PING 172.16.2.109 (172.16.2.109): 56 data bytes

--- 172.16.2.109 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
$
```

The `enas_ping` command sent a 56-byte ICMP packet to the machine with the IP address of `172.16.2.109` for three times, but the machine could not receive it even once. From the result, you can see the NAS Modular system was not able to communicate with the machine that has the specified IP address. Check the settings for the IP address, netmask, and VLAN ID for the NAS Modular system, switch, and client. If necessary, change the settings.

Failed example 2:

The following gives an execution example and explanation when the MTU value for the switch is not specified correctly.

The MTU value for the interface in the NAS Modular system is 9,000. The following example shows the case when 9,000 is not specified for the MTU value for the switch.

```
$ sudo enas_ping 172.16.2.109 -c 3
PING 172.16.2.109 (172.16.2.109): 56 data bytes
64 bytes from 172.16.2.109: icmp_seq=0 ttl=255 time=6.7 ms
64 bytes from 172.16.2.109: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 172.16.2.109: icmp_seq=2 ttl=255 time=0.2 ms

--- 172.16.2.109 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.2/2.3/6.7 ms
$ sudo enas_ping 172.16.2.109 -c 3 -s 9000
PING 172.16.2.109 (172.16.2.109): 9000 data bytes

--- 172.16.2.109 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
$
```

The first `enas_ping` command sent a 56-byte ICMP packet to the machine with the IP address of `172.16.2.109` for three times, and the machine received it for three times. From the result, you can see that communication was performed correctly. The next `enas_ping` command sent a 9,000-byte ICMP packet to the same client, but the communication failed with a packet loss of 100%. Check the settings for the MTU value for the NAS Modular system, switch, and client. If necessary, change the settings.

Failed example 3:

The following gives an execution example and explanation when the NAS Modular system cannot communicate with a machine in a different network. In the example, the gateway address of the different network is specified and the `enas_ping` command is executed.

```
$ sudo enas_ping 172.16.3.251 -c 3
enas_ping: sendto: Network is unreachable
enas_ping: sendto: Network is unreachable
enas_ping: sendto: Network is unreachable
PING 172.16.3.251 (172.16.3.251): 56 data bytes
enas_ping: wrote 172.16.3.251 64 chars, ret=-1
enas_ping: wrote 172.16.3.251 64 chars, ret=-1
enas_ping: wrote 172.16.3.251 64 chars, ret=-1

--- 172.16.3.251 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
$
$
$ sudo enas_netstat -rn
Kernel IP routing table
Destination   Gateway     Genmask     Flags  MSS Window irtt Iface
172.16.2.0    0.0.0.0     255.255.255.0  U    40 0     0 rdn0.0002
172.29.1.0    0.0.0.0     255.255.255.0  U    40 0     0 stnet0
10.197.181.0  0.0.0.0      255.255.255.0  U    40 0     0 mtp1
10.208.136.0  0.0.0.0      255.255.255.0  U    40 0     0 mng1
172.29.2.0    0.0.0.0     255.255.255.0  U    40 0     0 stnet1
0.0.0.0     10.208.136.1  0.0.0.0     UG    40 0     0 mng1
$
```

In this example, neither the target gateway for `172.16.3.1` nor the default route is specified. `Network is unreachable` is output because the route to reach the specified IP address is not specified. Check the routing setting for the NAS Modular system, and if necessary, specify the setting again.

## Example of checking communication by using the enas_traceroute command

The following describes an example of checking a network by using the `enas_traceroute` command.

Successful example:

The following gives an execution example and explanation when the communication route to a machine in a different network is set correctly.

```
$ sudo enas_traceroute -n 172.16.3.109
traceroute to 172.16.3.109 (172.16.3.109), 30 hops max, 38 byte packets
 1 172.16.2.1  1.764 ms 3.839 ms 4.000 ms
 2 172.16.3.109 3.839 ms 2.587 ms 0.293 ms
$
```

In this example, the NAS Modular system communicates with the machine with the IP address of `172.16.3.109` via the router with the IP address of `172.16.2.1`.

Failed example:

The following gives an execution example and explanation when an error occurs in the route between the router and the client.

```
$ sudo enas_traceroute -n 172.16.3.109
traceroute to 172.16.3.109 (172.16.3.109), 30 hops max, 38 byte
packets
 1 172.16.2.1  1.728 ms 3.786 ms 3.934 ms
 2 * * *
 3 * *
$
```

From the execution result of the `enas_traceroute` command, you can see that the communication to the gateway with the IP address of `172.16.2.1` was established, however, the communication beyond the gateway could not be established. Make sure that the settings for the router and other relay devices are correct, and the routing setting for the client is correct. If necessary, change the settings.

# Acronyms and Abbreviations

| | |
|---|---|
| ACL | access control list |
| ADAM | Active Directory Application Mode |
| ADSI | Active Directory Service Interface |
| AMS | Adaptable Modular Storage |
| ARP | address resolution protocol |
| BDC | backup domain controller |
| CCI | command control interface |
| CHA | channel adapter |
| CIFS | common internet file system |
| CTL | controller |
| CSV | comma-separated value |
| CU | control unit |
| DASD | direct access storage device |
| DNS | domain name system |
| DSA | digital signal algorithm |
| FC | fiber channel |
| FTP | file transfer protocol |
| GID | group identifier |
| Hi-Star | Hierarchical Star Network |
| HIXFS | Hitachi NAS enhancement XFS |
| IP | Internet Protocol |
| JRE | Java Runtime Environment |
| JVM | Java Virtual Machine |
| LAN | local-area network |
| LDAP | Lightweigh Directory Access Protocol |
| LDEV | logical device |
| LDIF | LDAP Data Interchange Format |
| LU | logical unit |
| LUN | logical unit (also called device emulation or device type) |
| LVM | logical volume manager |
| MIB | management information base |
| MSS | max segment size |
| MTU | maximum transmission unit |
| NDMP | network data management protocol |
| NetBackup | VERITAS NetBackup DataCenter 4.5 |
| NFS | network file system |
| NNC | NAS node controller |

| | |
|---|---|
| OS | operating system |
| PCI | peripheral component interconnect |
| PDC | primary domain controller |
| P-VOL | primary volume |
| RAID | redundant array of independent disks |
| RAS | reliability availability scalability |
| RCU | remote control unit |
| RID | relative identification |
| RIO | remote IO |
| RSA | Rivest-Shamir-Adelman |
| RMI | remote method invocation |
| RPC | remote procedure call |
| SATA | Serial AT Attachment |
| SCSI | small computer system interface |
| SID | security identifier |
| SIM | service information message |
| SNMP | simple network management protocol |
| SSH | secure shell |
| STP | Spanning Tree Protocol |
| S-VOL | secondary volume |
| SVP | service processor |
| sync | synchronous |
| TCP | Transmission Control Protocol |
| TSD | Technical Support Division |
| TTL | time to live |
| VLAN | virtual LAN |
| VOL | volume |
| WMS | Workgroup Modular Storage |
| WWW | world wide web |
| XDR | external data representation |
| XFS | extended file system |

# Glossary

### Account administrator

The user who oversees the system administrators in a NAS Modular system. An account administrator is permitted to register and delete system administrators.

### ACL

Data set for resources, such as access permissions for Windows users on the network, and servers and files that can be accessed. This is used for managing usage permissions for devices and information on the network.

### Backup server

A server that controls backup and restore operated via a LAN.

### CIFS

A protocol that provides file-sharing services to Windows users.

### Cluster

A redundant configuration that enables a service to continue when an error occurs or maintenance work is performed. In a NAS Modular system, each cluster consists of two NAS Units. When an error occurs in one NAS Unit, the other NAS Unit in the cluster inherits the services (failover functionality), and the failover enables continuous operation of the NFS and CIFS file-sharing services provided by the NAS Modular system.

### Command device

A control device in the NAS Modular subsystem for accepting commands used for controlling the NAS Modular subsystem.

### Data LAN port

The ports (gbe1 to gbe4) on a NAS Unit used to connect to the data LAN.

### Device file

An area created by dividing a RAID group.

### Dump LU

A logical unit that contains information held in memory when a fatal error occurred in a NAS Modular system. One dump LU is assigned to each NAS Unit.

### End user

A user who accesses file systems in the disk array by using the file-sharing services provided by the NAS Modular system. End users can use the NAS Manager GUI to view usage, access statuses, and quota information set for the file systems. However, users registered by the user mapping functionality cannot use the NAS Manager GUI.

### Error information LU

A logical unit that is used when the data in a dump LU is converted to a format that the user can view. This LU is shared by all the NAS Units in the NAS Modular subsystem.

### failback

The migration of a failed-over resource group back to the original node in the cluster after error recovery or maintenance of a NAS Unit is completed.

### Failover

The relocation of a resource group to the other node in a cluster when an error occurs in a NAS Unit or when maintenance is required. Failovers enable continuous operation of the NFS and CIFS file-sharing services provided by the NAS Modular system.

### fixed IP address

An IP address set for a specific interface in a NAS Unit.

### Logical volume

An area created by dividing a volume group into one or more areas using a volume manager. On NAS Modular systems, this corresponds to file systems, differential-data storage devices and differential-data snapshots created using the volume manager. In a NAS Modular system, the number of logical volumes that can be created for one node is 4,096.

### LVM

A type of volume manager. See *volume manager* for more information.

M

### Maintenance personnel

Hitachi engineers who maintain NAS Modular systems.

### Management LAN port

The port (mng1) on a NAS Unit used to connect to the management LAN.

### Media server

A server that controls a tape device installed outside the disk array.

### NAS Anti Virus Agent

A program used to scan for viruses in data shared with users over CIFS in a NAS Modular system. NAS Anti Virus Agent is an optional program of NAS Manager.

### NAS Backup Restore

A program used for backing up data shared by users in a NAS Modular system. NAS Backup Restore is an optional program of NAS Manager.

### NAS Cluster Management LU

An LU that stores settings information for NAS Modular systems, such as cluster configuration information and file system information.

### NAS Data Control

One of the programs incorporated in the NAS OS. NAS Data Control is a required program of a NAS Modular system.

### NAS interface board

A board that is inserted into a slot (CTL0 or CTL1) on the controller for connection to an NNC.

### NAS Manager

A program that enables efficient setup, operation, and management of a NAS Modular system. NAS Manager is a required program of a NAS Modular system.

### NAS Modular subsystem

A subsystem in which a NAS Unit is connected to a disk array of the TagmaStore AMS/WMS series for use as a NAS server.

### NAS Modular system

A NAS system that uses a NAS Modular subsystem to provide file-sharing services.

### NAS OS

An operating system that provides Network Attached Storage (NAS) functionality in a NAS Modular system. The NAS OS consists of NAS Data Control and NAS File Sharing.

### NAS OS LU

A logical unit that contains the NAS OS and the programs that run on the NAS OS.

### NAS Sync Image

A program used to create differential-data snapshots of data shared with users in a NAS Modular system. NAS Sync Image is an optional program of NAS Manager.

### NAS system LU

A logical unit that contains configuration and management information about a NAS Modular system, such as NAS OS LUs and a NAS Cluster Management LU.

### NAS Unit

A device connected to a disk array of the TagmaStore AMS/WMS series to create a NAS Modular subsystem that is used as a NAS server. A Gigabit Ethernet adapter and a CPU are mounted on a NAS Unit.

### NFS

A protocol that provides file-sharing services to UNIX users.

### Node

A cluster component. In a NAS Modular system, each cluster consists of two NAS Units. One NAS Unit corresponds to one component of a cluster.

### Program package

A generic name for the `deb` file. This is specified when you install a program on the NAS OS LU.

### Quota

The maximum block space and maximum number of i-nodes available to a user, In the NAS Modular system, the limits can be applied for each file system, or each directory immediately below the mount point.

### Resource

The smallest unit of information available in a resource group, including NFS share settings, CIFS share settings, file system information, and service IP address information.

### Resource group

A management unit that manages, as a group, multiple resources such as NFS share settings, CIFS share settings, file system information, and service IP address information. A service can be started and stopped for each resource group. If an error occurs, failover occurs for each resource group.

### Scan server

A server that scans a LAN for viruses in data shared by CIFS in a NAS Modular system.

### Service IP address

An IP address used by a user when connecting to a service running in a resource group. By using a service IP address, the user can continue to use the service when an error has occurred on a node and the resource group fails over to the other normally running node.

### ShadowImage

A program for replicating user data within the TagmaStore AMS/WMS series disk array, bypassing the host system.

### subtree quota

The quota set for a directory residing immediately under the mount point directory. Subtree quotas are used to control the amount of block usage and i-node usage for each directory. Subtree quotas can also be set for users and groups.

### System administrator

A user who manages a NAS Modular system by using NAS Manager. The system administrator sets up a NAS Modular system and monitors the system operation and error information.

### Trunking

A link denotes a connection between devices. Trunking (that is, combining links) is a technology used to create a group of ports as a virtual network interface. The NAS Modular system allows you to configure a network by using a virtual network interface whose setup is based on trunking.

### User LU

A logical unit that contains user data of file systems.

### User mapping

A function that dynamically assigns a user ID or group ID on the NAS Modular system when a user or group registered in the domain controller accesses a CIFS share for the first time.

### VLAN

A VLAN is technology that virtually divides a physical network configuration (a LAN). In the NAS Modular system, an IEEE802.1Q tag-based VLAN can be used.

### Volume group

An area that is made up of one or more device files by a volume manager. In a NAS Modular system, 128 volume groups can be created for one node.

In NAS Manager, a volume group is made up of a file system. In NAS Sync Image, a volume group is made up of a file system, a differential-data storage device, and a differential-data snapshot.

### Volume manager

Functionality for volume management. In the NAS Modular system, LVM is used as the volume manager. This functionality enables you to create volume groups combining device files and to create logical volumes out of volume groups.