

Hitachi Data Ingestor Cluster Administrator's Guide

FASTFIND LINKS

[Product Version](#)

[Getting Help](#)

[Contents](#)

© 2013- 2016 Hitachi, Ltd. All rights reserved.

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, Ltd.

Hitachi, Ltd., reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. This document contains the most current information available at the time of publication. When new or revised information becomes available, this entire document will be updated and distributed to all registered users.

Some of the features described in this document might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Data Systems Corporation at <https://portal.hds.com>.

Notice: Hitachi, Ltd., products and services can be ordered only under the terms and conditions of the applicable Hitachi Data Systems Corporation agreements. The use of Hitachi, Ltd., products is governed by the terms of your agreements with Hitachi Data Systems Corporation.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., in the United States and other countries.

Archivas, Essential NAS Platform, HiCommand, Hi-Track, ShadowImage, Tagmaserve, Tagmasoft, Tagmasolve, Tagmastore, TrueCopy, Universal Star Network, and Universal Storage Platform are registered trademarks of Hitachi Data Systems Corporation.

AIX, AS/400, DB2, Domino, DS8000, Enterprise Storage Server, ESCON, FICON, FlashCopy, IBM, Lotus, OS/390, RS6000, S/390, System z9, System z10, Tivoli, VM/ESA, z/OS, z9, zSeries, z/VM, z/VSE are registered trademarks and DS6000, MVS, and z10 are trademarks of International Business Machines Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Microsoft product screen shots are reprinted with permission from Microsoft Corporation.



Contents

Preface.....	xiii
Intended audience.....	xiv
Product version.....	xiv
Release notes.....	xiv
Organization of HDI manuals.....	xiv
Referenced documents.....	xv
Abbreviation conventions.....	xvii
Document conventions.....	xviii
Convention for storage capacity values.....	xix
Getting help.....	xx
Comments.....	xx
1 Logging on.....	1-1
Logging on to the system.....	1-2
2 Managing system administrator accounts.....	2-1
Adding an account.....	2-2
Changing an account password.....	2-2
3 Managing shared directories.....	3-1
Creating a shared directory.....	3-2
Referencing other HDI data as read-only via the linked HCP.....	3-3
Changing the policy and schedule for migrating data to HCP.....	3-4
Importing data from another file server.....	3-5
Using the CIFS protocol to import data from another file server.....	3-5
When domain authentication is used (with no local account files).....	3-6
When domain authentication is used (with some local account files).....	3-9
When only local authentication is used.....	3-12
Using the NFS protocol to import data from another file server.....	3-15
4 Setting up the access environment from clients.....	4-1
Setting up the access environment from CIFS clients.....	4-2
Joining nodes to an Active Directory® domain.....	4-2
Rejoining an Active Directory domain.....	4-5

Joining nodes to an NT domain.....	4-5
Configuring a workgroup.....	4-7
Identifying users by user mapping.....	4-8
Collecting CIFS client access logs.....	4-10
Setting up the access environment from NFS clients.....	4-12
Improving the GUI operation for a large system.....	4-12
5 Showing previous data.....	5-1
Showing previous data on HCP.....	5-2
6 Managing disk capacity.....	6-1
Expanding file system capacity.....	6-2
Limiting the capacity used per file share.....	6-2
Limiting the capacity used by a user or group.....	6-3
7 Protecting user data.....	7-1
Setting up virus scanning.....	7-2
Backing up data to a tape device.....	7-2
Restoring data from a tape device.....	7-4
8 Backing up the system configuration.....	8-1
Manually backing up system configuration.....	8-2
Regularly backing up system configuration.....	8-2
9 Changing the network configuration.....	9-1
Changing the IP address of a node.....	9-2
Changing the host name of a node.....	9-3
Adding and deleting routing information.....	9-4
Adding routing information.....	9-4
Deleting routing information.....	9-4
Changing the negotiation mode.....	9-5
Changing the negotiation mode (for a non-cascaded trunk port).....	9-5
Changing the negotiation mode (for a cascaded trunk port).....	9-6
Setting up redundant link configuration.....	9-8
Setting link aggregation.....	9-8
Setting link alternation.....	9-8
Combining link aggregation and link alternation (cascaded trunking).....	9-9
Performing manual link alternation.....	9-10
Setting up a VLAN.....	9-10
10 Monitoring the system.....	10-1
Using SNMPv2.....	10-2
Using SNMPv3.....	10-3
Using error email notifications.....	10-7
11 Controlling a node and OS.....	11-1
Stopping or starting a node.....	11-2

Stopping a node.....	11-2
Starting a node.....	11-3
Shutting down and restarting the OS on a node.....	11-4
Shutting down the OS on a node.....	11-4
Restarting the OS on a node.....	11-5
Shutting down the OSs on both nodes.....	11-6
Starting the OSs of both nodes at the same time.....	11-7
12 Changing the connection between nodes and storage systems.....	12-1
Changing the ports assigned to an LU.....	12-2
Reconfiguring an LU path.....	12-3
Adding an LU path.....	12-4
Deleting an LU path.....	12-4
Changing an LU path.....	12-5
Reconfiguring an FC path.....	12-5
Adding an FC path.....	12-5
Changing or deleting an FC path.....	12-6
Replacing FC switches.....	12-7
Connecting an additional storage system.....	12-7
Before connecting an additional storage system.....	12-7
Connecting an additional storage system.....	12-8
Detaching a storage system.....	12-9
13 Setting up an environment for command and GUI operations.....	13-1
Setting up the SSH environment to use commands.....	13-2
Setting up a public key certificate.....	13-2
14 Performing an update installation.....	14-1
Performing an upgrade or overwrite installation of Hitachi File Services Manager.....	14-2
Updating software.....	14-3
Updating the software on a node.....	14-4
When the software is updated after setting up linking with an HCP system for a version earlier than 3.2.0-00.....	14-6
Creating a user account with the same name as the data access account..	14-6
Setting up a user account for a tenant administrator in Hitachi File Services Manager.....	14-7
A Operations provided by the GUI.....	A-1
GUI operations.....	A-2
B Basic GUI operations.....	B-1
Notes on using the GUI.....	B-2
Hitachi File Services Manager main window.....	B-3
Global tasks bar area.....	B-4
Explorer menu.....	B-5
Navigation area.....	B-6
Application bar area.....	B-6
Application area (window).....	B-6
Operation dialog boxes.....	B-7

Confirmation dialog boxes.....	B-9
Results dialog boxes.....	B-11

C GUI reference..... C-1

Shares window.....	C-5
Edit Share dialog box.....	C-7
Basic tab.....	C-8
Access Control tab.....	C-9
CIFS subtab.....	C-9
NFS subtab.....	C-12
Namespace tab.....	C-14
Advanced tab.....	C-15
CIFS subtab.....	C-15
Change Share Quota dialog box.....	C-19
share window.....	C-21
CIFS Share tab.....	C-23
Properties subtab.....	C-23
Special Permitted Users subtab.....	C-27
Special Permitted Groups subtab.....	C-27
NFS Share tab.....	C-28
Properties subtab.....	C-28
Hosts subtab.....	C-28
File System tab.....	C-29
Namespace tab.....	C-31
File Systems window.....	C-33
File System tab.....	C-34
Add Share dialog box.....	C-38
Basic tab.....	C-40
Namespace tab.....	C-43
Edit File System dialog box.....	C-44
WORM tab.....	C-44
Namespace tab.....	C-46
Advanced tab.....	C-52
Expand File System dialog box.....	C-52
Basic tab.....	C-52
Namespace tab.....	C-54
Advanced tab.....	C-54
File System subtab.....	C-54
Mount File System dialog box.....	C-54
Edit Quota dialog box.....	C-55
List of Quota Information page.....	C-56
Quota Setup page.....	C-59
Grace Period Setup page.....	C-60
Monitoring Setup page.....	C-61
Default Quota Setup page.....	C-62
file-system window.....	C-62
Properties tab.....	C-66
Shares tab.....	C-68
LUs tab.....	C-70
LUs subtab.....	C-70
Pools subtab.....	C-72
WORM tab.....	C-72

Work Space tab.....	C-73
Work Space LUs subtab.....	C-73
Namespace tab.....	C-74
Processing Nodes window.....	C-78
File Servers tab.....	C-79
Content Platform tab.....	C-81
Add Processing Node dialog box.....	C-82
When File Servers type is selected.....	C-83
Basic tab.....	C-83
Storage System tab.....	C-84
When Content Platform type is selected.....	C-84
Edit Node dialog box.....	C-85
Basic tab.....	C-86
Storage System tab.....	C-86
processing-node window.....	C-86
Physical Nodes tab.....	C-89
physical-node window.....	C-91
Shares tab.....	C-93
File Systems tab.....	C-95
File System subtab.....	C-95
LUs tab.....	C-99
LUs subtab.....	C-99
Pools subtab.....	C-101
Settings tab.....	C-102
Basic subtab.....	C-102
Advanced subtab.....	C-103
Create and Share File System dialog box.....	C-103
Basic tab.....	C-105
Access Control tab.....	C-108
CIFS subtab.....	C-108
NFS subtab.....	C-111
Directory subtab (A file system of the Advanced ACL type).....	C-114
Directory subtab (A file system of the Classic ACL type).....	C-115
WORM tab.....	C-115
Namespace tab.....	C-117
Advanced tab.....	C-121
CIFS subtab.....	C-121
File System subtab.....	C-125
Striping subtab.....	C-126
Create File System dialog box.....	C-126
Basic tab.....	C-128
WORM tab.....	C-130
Namespace tab.....	C-132
Advanced tab.....	C-136
File System subtab.....	C-136
Striping subtab.....	C-136
Health Monitor window.....	C-137
Hardware tab.....	C-140
Internal HDD subtab.....	C-140
Fan subtab.....	C-141
Temperature subtab.....	C-141
Power Supply subtab.....	C-142

Internal RAID Battery subtab.....	C-142
BMC Status subtab.....	C-143
Network tab.....	C-144
Ethernet Interface subtab.....	C-144
FC Path subtab.....	C-145
Memory tab.....	C-146
Memory Total subtab.....	C-147
Details subtab.....	C-147
System Software window.....	C-147
System Software Installation Wizard.....	C-148
Local Users dialog box.....	C-150
List of Users / Groups page.....	C-151
List of Users / Groups page (for List of users).....	C-151
List of Users / Groups page (for List of groups).....	C-152
Change Password page.....	C-153
Edit User page.....	C-153
Add User page.....	C-154
Batch Operation page.....	C-156
CSV file format.....	C-156
Execution result file format.....	C-158
Edit Group page.....	C-162
Add Group page.....	C-162
Check for Errors dialog box.....	C-163
List of RAS Information page.....	C-164
List of RAS Information page (for List of messages).....	C-165
List of RAS Information page (for List of system logs).....	C-167
List of RAS Information page (for List of other log files).....	C-167
List of RAS Information page (for Batch-download).....	C-168
List of RAS Information page (for List of core files).....	C-169
List of RAS Information page (for Server check).....	C-170
List of RAS Information page (for Transfer all logs including the virtual server logs).....	C-170
Transfer All Files page.....	C-171
Backup Configuration dialog box.....	C-171
Save System Settings Menu page.....	C-173
Save All System Settings page.....	C-173
Upload Saved Data page.....	C-176
Schedule Settings for Saving All System Settings page.....	C-177
Network & System Configuration dialog box.....	C-178
System Setup Menu page.....	C-179
System Setup Menu page (Setting Type: network).....	C-179
System Setup Menu page (Setting Type: system).....	C-180
List of Data Ports page.....	C-181
Negotiation Mode Setup page.....	C-183
List of Trunking Configurations page.....	C-187
Link Aggregation Setup page.....	C-191
Link Alternation Setup page.....	C-191
Edit Cascaded Trunking page.....	C-192
List of Interfaces page.....	C-192
Edit Interface page.....	C-195
Add Interface page.....	C-196
DNS, NIS, LDAP Setup page.....	C-197

List of Routings page.....	C-200
Add Routing page.....	C-201
Time Setup page.....	C-203
Syslog Setup page.....	C-204
Edit Syslog Setup page.....	C-205
Add Syslog Setup page.....	C-205
Log File Capacity Setup page.....	C-206
Edit File Capacity page.....	C-208
Core File Auto. Deletion Setup page.....	C-208
Edit System File page.....	C-209
Performance Tuning page.....	C-213
List of SNMPs page.....	C-214
Edit SNMP page.....	C-215
Add SNMP page.....	C-215
Select User Interface page.....	C-216
Access Protocol Configuration dialog box.....	C-217
List of Services page.....	C-218
CIFS Service Management page.....	C-222
CIFS Service Management page (Setting Type: Basic).....	C-223
CIFS Service Management page (Setting Type: User mapping).....	C-225
CIFS Service Management page (Setting Type: Security).....	C-231
CIFS Service Management page (Setting Type: Performance).....	C-235
CIFS Service Management page (Setting Type: Administration).....	C-238
Setting Events Logged to the CIFS Access Log page.....	C-239
Select Authentication Mode page.....	C-240
Local Authentication page.....	C-241
NT Domain Authentication page.....	C-241
Active Directory Authentication page.....	C-241
FTP Service Management page.....	C-242
Select FTP Users page.....	C-247
NFS Service Management page.....	C-248
SFTP Service Management page.....	C-251
Select SFTP Users page.....	C-255
Public Key List page.....	C-256
Add Public Key page.....	C-257
CIFS Service Maintenance page.....	C-258
CIFS service information.....	C-259
CIFS default information.....	C-263
User mapping information.....	C-265
Cluster Management dialog box.....	C-268
Define Cluster Configuration page.....	C-269
Browse Cluster Status page.....	C-271
Browse Cluster Status page (for Cluster / Node status).....	C-271
Modify Cluster Configuration page.....	C-276
Modify Host Name page.....	C-277
Browse Cluster Status page (for Resource group status).....	C-278
Proxy Server Settings window.....	C-281
Configure Proxy Server dialog box.....	C-282
Virus Scan Server Configuration dialog box.....	C-283
List of Scanner Servers page.....	C-283
Edit Scanner Server page.....	C-286
Add Scanner Server page.....	C-287

Scan Conditions page.....	C-287
Scanning Software page.....	C-293
Activate License dialog box.....	C-293
HCP-name window.....	C-294
storage-system-name window.....	C-295
Users and Permissions window.....	C-296
Users window.....	C-297
Add User dialog box.....	C-300
Change Authentication Method dialog box.....	C-301
user-ID window.....	C-302
Edit Profile dialog box.....	C-303
Change Password dialog box.....	C-304
Change Permission dialog box.....	C-305
Permissions window.....	C-306
application window.....	C-307
Security window.....	C-308
Password window.....	C-309
Password dialog box.....	C-310
Account Lock window.....	C-311
Account Lock dialog box.....	C-312
Warning Banner window.....	C-313
Edit Message dialog box.....	C-314
User Profile window.....	C-316
Configuration Wizard.....	C-317
2. Node settings page.....	C-319
4. Cluster settings page.....	C-320
5. Network settings page.....	C-322
6. Optional settings page.....	C-322
6-1. DNS settings page.....	C-323
6-2. Time settings page.....	C-323
6-3. HCP settings page.....	C-324
6-4. User authentication settings page.....	C-326
Selecting the protocol.....	C-326
Selecting the CIFS user authentication method.....	C-327
Specifying local authentication settings.....	C-327
Specifying Active Directory authentication settings.....	C-329
When RIDs is selected as the user mapping method.....	C-330
When Active Directory schema is selected as the user mapping method..	C-331
Selecting an external server.....	C-331
When using an NIS server.....	C-332
When using an LDAP server.....	C-332
9. Completion page.....	C-333
HDvM Connection Management dialog box.....	C-334
Edit HDvM Settings dialog box.....	C-335
Migration Tasks dialog box.....	C-336
migration-task page.....	C-340
Task Information tab.....	C-341
History tab.....	C-344
Download Report dialog box.....	C-345
Failed dialog box.....	C-345
Policy Information dialog box.....	C-346
Migration Task Wizard.....	C-348

2. Task Settings page.....	C-350
3. Schedule Settings page.....	C-350
4. Policy Settings page.....	C-351
File Systems dialog box.....	C-352
Stop Task dialog box.....	C-353
Migrate Immediately dialog box.....	C-354
Enable Task dialog box.....	C-354
Disable Task dialog box.....	C-355
Delete Task dialog box.....	C-355
D Operation performed by end users.....	D-1
List of operations.....	D-2
Logging on.....	D-2
Basic GUI operations.....	D-2
GUI layout.....	D-2
Notes about using the GUI.....	D-3
GUI reference.....	D-3
List of File Shares page (for List of NFS File Shares).....	D-3
List of File Shares page (for List of CIFS File Shares).....	D-4
Display Quota page (for User Quota Info.).....	D-4
Display Quota page (for Group Quota Info.).....	D-6
Password Setup page.....	D-8
User Info. Setup page.....	D-8
E Backing up and restoring quota information.....	E-1
Backing up quota information.....	E-2
Output location when a mount point is specified.....	E-2
Output location when a directory under the mount point is specified.....	E-4
Cautions when backing up quota information.....	E-7
Restoring quota information.....	E-9
Restoring quota information at the file system level.....	E-9
Restoring quota information at the directory level.....	E-11
Cautions for restoring quota information.....	E-12
F Reserved words.....	F-1
List of reserved words.....	F-2
G MIB objects.....	G-1
List of MIB objects.....	G-2
MIB objects for responding to SNMP get requests.....	G-3
MIB objects used for SNMP traps.....	G-69
H Acronyms.....	H-1
Acronyms used in the HDI manuals.....	H-2

Glossary

Index



Preface

This manual describes how to operate a Hitachi Data Ingestor (HDI) system in a cluster configuration.

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

This preface includes the following information:

- [Intended audience](#)
- [Product version](#)
- [Release notes](#)
- [Organization of HDI manuals](#)
- [Referenced documents](#)
- [Abbreviation conventions](#)
- [Document conventions](#)
- [Convention for storage capacity values](#)
- [Getting help](#)
- [Comments](#)

Intended audience

This manual is intended for system administrators who operate and manage an HDI system.

In addition, the user must have:

- A basic knowledge of storage systems
- A basic knowledge of Hitachi Content Platform (HCP) systems
- A basic knowledge of networks
- A basic knowledge of file sharing services
- A basic knowledge of SAN
- A basic knowledge of CIFS
- A basic knowledge of NFS
- A basic knowledge of UNIX
- A basic knowledge of Windows
- A basic knowledge of Web browsers

Product version

This document revision applies to Hitachi Data Ingestor version 4.2.1 or later.

Release notes

Release notes can be found on the documentation CD. Release notes contain requirements and more recent product information that may not be fully described in this manual. Be sure to review the release notes before installation.

Organization of HDI manuals

HDI manuals are organized as shown below.

Note that whether HDI nodes can be set up in a redundant configuration depends on the HDI model. A configuration where nodes are made redundant is called a cluster configuration, and a configuration where a node is not made redundant with another node is called a single-node configuration. Which manuals you need to read depends on which configuration you are going to use.

Manual title	Description
<i>Hitachi Data Ingestor Installation and Configuration Guide</i> , MK-90HDI002	You must read this manual first to use an HDI system. This manual contains the information that you must be aware of before starting HDI system operation,

Manual title	Description
	as well as the environment settings for an external server.
<i>Hitachi Data Ingestor Cluster Getting Started Guide, MK-90HDI001</i>	This manual explains how to set up an HDI system in a cluster configuration.
<i>Hitachi Data Ingestor Cluster Administrator's Guide (This manual)</i>	This manual provides procedures for using HDI systems in a cluster configuration, as well as provides GUI references.
<i>Hitachi Data Ingestor Cluster Troubleshooting Guide, MK-90HDI029</i>	This manual provides troubleshooting information for HDI systems in a cluster configuration.
<i>Hitachi Data Ingestor Single Node Getting Started Guide, MK-90HDI028</i>	This manual explains how to set up an HDI system in a single-node configuration.
<i>Hitachi Data Ingestor Single Node Administrator's Guide, MK-90HDI039</i>	This manual explains the procedures for using HDI systems in a single-node configuration, as well as provides GUI references.
<i>Hitachi Data Ingestor Single Node Troubleshooting Guide, MK-90HDI030</i>	This manual provides troubleshooting information for HDI systems in a single-node configuration.
<i>Hitachi Data Ingestor CLI Administrator's Guide, MK-90HDI034</i>	This manual describes the syntax of the commands that can be used for HDI systems in a cluster configuration or a single-node configuration.
<i>Hitachi Data Ingestor API References, MK-90HDI026</i>	This manual explains how to use the API for HDI systems in a cluster configuration or a single-node configuration.
<i>Hitachi Data Ingestor Error Codes, MK-90HDI005</i>	This manual contains messages for HDI systems in a cluster configuration or a single-node configuration.
<i>Hitachi Data Ingestor File System Protocols (CIFS/NFS) Administrator's Guide, MK-90HDI035</i>	This manual contains the things to keep in mind before using the CIFS or NFS service of an HDI system in a cluster configuration or a single-node configuration from a CIFS or NFS client.

The *Cluster Administrator's Guide* and the *Single Node Administrator's Guide* are available in HTML and PDF formats. All other manuals are available in only PDF format.

Referenced documents

Hitachi Virtual Storage Platform G1000

- *Hitachi Data Ingestor Array Features Administrator's Guide*

Hitachi Virtual Storage Platform G200, G400, G600, G800

- *Hitachi Data Ingestor Array Features Administrator's Guide*

Hitachi Virtual Storage Platform F400, F600, F800

- *Hitachi Data Ingestor Array Features Administrator's Guide*

Hitachi Virtual Storage Platform

- *Hitachi Data Ingestor Array Features Administrator's Guide*

Hitachi Universal Storage Platform V/VM

- *Hitachi Data Ingestor Array Features Administrator's Guide*

Hitachi Unified Storage VM

- *Hitachi Data Ingestor Array Features Administrator's Guide*

Hitachi Unified Storage 100 series

- *Hitachi Data Ingestor Array Features Administrator's Guide for Hitachi AMS2000/HUS100 series*
- *Hitachi Storage Navigator Modular 2 Command Line Interface (CLI) User's Guide*
- *Hitachi Storage Navigator Modular 2 Graphical User Interface (GUI) User's Guide*

Hitachi AMS2000 series

- *Hitachi Data Ingestor Array Features Administrator's Guide for Hitachi AMS2000/HUS100 series*
- *Hitachi Storage Navigator Modular 2 Command Line Interface (CLI) User's Guide*
- *Hitachi Storage Navigator Modular 2 Graphical User Interface (GUI) User's Guide*

Hitachi Content Platform

- *Hitachi Content Platform Administering HCP*
- *Hitachi Content Platform Managing a Tenant and Its Namespaces*
- *Hitachi Content Platform Managing the Default Tenant and Namespace*
- *Hitachi Content Platform Replicating Tenants and Namespaces*
- *Hitachi Content Platform HCP Management API Reference*
- *Hitachi Content Platform Using a Namespace*
- *Hitachi Content Platform Using the Default Namespace*
- *Hitachi Content Platform HCP Metadata Query API Reference*
- *Hitachi Content Platform Searching Namespaces*
- *Hitachi Content Platform Using HCP Data Migrator*
- *Hitachi Content Platform Installing an HCP System*

- *Hitachi Content Platform Third-Party Licenses and Copyrights*
- *Hitachi Content Platform HCP-DM Third-Party Licenses and Copyrights*
- *Hitachi Content Platform Installing an HCP SAIN System - Final On-site Setup*
- *Hitachi Content Platform Installing an HCP RAIN System - Final On-site Setup*

Abbreviation conventions

This manual uses the following abbreviations for product names:

Abbreviation	Full name or meaning
Active Directory	Active Directory(R)
Device Manager	Hitachi Device Manager Software
Dynamic Provisioning	Hitachi Dynamic Provisioning
Dynamic Tiering	Hitachi Dynamic Tiering
File Services Manager	A generic name for the following: <ul style="list-style-type: none"> • Configuration Manager • Hitachi File Services Manager
HCP	Hitachi Content Platform
HDI	Hitachi Data Ingestor
Hitachi AMS2000 series	Hitachi Adaptable Modular Storage 2000 series
HUS100 series	A generic name for the following: <ul style="list-style-type: none"> • Hitachi Unified Storage 150 • Hitachi Unified Storage 130 • Hitachi Unified Storage 110
HUS VM	Hitachi Unified Storage VM
Internet Explorer	Windows(R) Internet Explorer(R)
Universal Storage Platform V/VM	A generic name for the following: <ul style="list-style-type: none"> • Hitachi Universal Storage Platform V • Hitachi Universal Storage Platform VM
Virtual Storage Platform	Hitachi Virtual Storage Platform
VSP F400, F600, F800	A generic name for the following: <ul style="list-style-type: none"> • Hitachi Virtual Storage Platform F400 • Hitachi Virtual Storage Platform F600 • Hitachi Virtual Storage Platform F800
VSP G1000	Hitachi Virtual Storage Platform G1000
VSP G200, G400, G600, G800	A generic name for the following: <ul style="list-style-type: none"> • Hitachi Virtual Storage Platform G200 • Hitachi Virtual Storage Platform G400

Abbreviation	Full name or meaning
	<ul style="list-style-type: none"> • Hitachi Virtual Storage Platform G600 • Hitachi Virtual Storage Platform G800
Windows	Microsoft(R) Windows(R) Operating System
Windows Server 2003	<p>A generic name for the following:</p> <ul style="list-style-type: none"> • Microsoft(R) Windows Server(R) 2003, Standard Edition Operating System • Microsoft(R) Windows Server(R) 2003, Enterprise Edition Operating System • Microsoft(R) Windows Server(R) 2003, Datacenter Edition Operating System • Microsoft(R) Windows Server(R) 2003, Web Edition Operating System
Windows Server 2003 R2	<p>A generic name for the following:</p> <ul style="list-style-type: none"> • Microsoft(R) Windows Server(R) 2003 R2, Standard Edition • Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition • Microsoft(R) Windows Server(R) 2003 R2, Datacenter Edition
Windows Server 2008	<p>A generic name for the following:</p> <ul style="list-style-type: none"> • Microsoft(R) Windows Server(R) 2008 Enterprise • Microsoft(R) Windows Server(R) 2008 Enterprise 32-bit • Microsoft(R) Windows Server(R) 2008 Standard • Microsoft(R) Windows Server(R) 2008 Standard 32-bit • Microsoft(R) Windows Server(R) 2008 R2 Enterprise • Microsoft(R) Windows Server(R) 2008 R2 Standard
Windows Server 2012	<p>A generic name for the following:</p> <ul style="list-style-type: none"> • Microsoft(R) Windows Server(R) 2012 Datacenter • Microsoft(R) Windows Server(R) 2012 Essentials • Microsoft(R) Windows Server(R) 2012 Foundation • Microsoft(R) Windows Server(R) 2012 Standard • Microsoft(R) Windows Server(R) 2012 R2 Datacenter • Microsoft(R) Windows Server(R) 2012 R2 Essentials • Microsoft(R) Windows Server(R) 2012 R2 Foundation • Microsoft(R) Windows Server(R) 2012 R2 Standard

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click OK .
<i>Italic</i>	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: <code>copy source-file target-file</code> <i>Note:</i> Angled brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or entered by the user. Example: <code># pairdisplay -g oradb</code>
[] square brackets	Indicates optional values. Example: [a b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a b } indicates that you must choose either a or b.
vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a b] indicates that you can choose a, b, or nothing. { a b } indicates that you must choose either a or b.

This document uses the following icons to draw attention to information:

Icon	Label	Description
	Note	Calls attention to important and/or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.

Convention for storage capacity values

Storage capacity values (e.g., drive capacity) are calculated based on the following values:

Capacity Unit	Physical Value	Logical Value
1 KB	1,000 bytes	1,024 (2 ¹⁰) bytes
1 MB	1,000 KB or 1,000 ² bytes	1,024 KB or 1,024 ² bytes
1 GB	1,000 MB or 1,000 ³ bytes	1,024 MB or 1,024 ³ bytes
1 TB	1,000 GB or 1,000 ⁴ bytes	1,024 GB or 1,024 ⁴ bytes
1 PB	1,000 TB or 1,000 ⁵ bytes	1,024 TB or 1,024 ⁵ bytes
1 EB	1,000 PB or 1,000 ⁶ bytes	1,024 PB or 1,024 ⁶ bytes

Capacity Unit	Physical Value	Logical Value
1 block	-	512 bytes

Getting help

[Hitachi Data Systems Support Connect](#) is the destination for technical support of products and solutions sold by Hitachi Data Systems. To contact technical support, log on to Hitachi Data Systems Support Connect for contact information: https://support.hds.com/en_us/contact-us.html.

[Hitachi Data Systems Community](#) is a global online community for HDS customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hds.com, register, and complete your profile.

Comments

Please send us your comments on this document: doc.comments@hds.com. Include the document title, number, and revision, and refer to specific section(s) and paragraph(s) whenever possible.

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

Logging on

This chapter describes how to log on to the system.

- [Logging on to the system](#)

Logging on to the system

A system administrator can operate and manage a Hitachi Data Ingestor (HDI) system from a Web browser by logging on.

To log on to the system:

1. Enter the following URL in your Web browser's address bar.

`http://management-server-IP-address-or-host-name:port-number-for-HBase-Storage-Mgmt-Web-Service/FileServicesManager/`

The specification differs depending on whether SSL is used for communication between the management server and the management client.

Example:

`http://example:23015/FileServicesManager/` (for non-SSL communication)

`https://example:23016/FileServicesManager/` (for SSL communication)

23015 is the default for *port-number-for-HBase-Storage-Mgmt-Web-Service*.

2. In the Login window, specify a user ID and the password, and then click **Login**.

The Hitachi File Services Manager main window is shown.



Note:

- If authentication by an external authentication server is enabled, use the password that is registered on the server.
- The account might be locked after repeated log on failures. If the account is locked, ask a system administrator who has the Admin (user management) permission to unlock the account.
- If you are accessing the GUI for the first time, use the following built-in account to log on and then add a system administrator account to Hitachi File Services Manager.

User ID: `System`

Password: `manager` (default)

- To prevent unauthorized access, make sure that you change the password at the first log on.
-

Managing system administrator accounts

This chapter describes how to manage the system administrator accounts.

- [Adding an account](#)
- [Changing an account password](#)

Adding an account

A system administrator that has Admin (user management) permission can add an account and set permissions for the system administrator (user) that uses the GUI.

GUI used by this operation

- [Users window on page C-297](#)
- [Add User dialog box on page C-300](#)
- [user-ID window on page C-302](#)
- [Change Permission dialog box on page C-305](#)

To Add a system administrator

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Administration**, and then **User Management**.
2. Select **Users and Permissions - Users** from the object tree, and then click **Add User** from the Users window.
3. In the **Add User** dialog box, specify the required information, and then click **OK**.
4. Select **Users and Permissions - Users - user-ID** from the object tree, and then click **Change Permission** from the *user-ID* window.
5. In the **Change Permission** dialog box, specify the required information, and then click **OK**.

Changing an account password

A system administrator can change their own password. A system administrator who has Admin (user management) permission can also change the passwords of other system administrators.



Note: If the management server is operated in a cluster configuration, perform the following operation on both the executing node and standby node if you want to change the System account password.

GUI used by this operation

- [User Profile window on page C-316](#)
- [Change Password dialog box on page C-304](#)

To change the password of a system administrator

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Settings**, and then **User Profile**.
2. Select **User Profile**, and then click **Change Password** from the User Profile window.

3. In the **Change Password** dialog box, specify the required information, and then click **OK**.
4. Verify that the processing results are correct, and then click **Close**.

Managing shared directories

This chapter describes how to manage the shared directories.

- [Creating a shared directory](#)
- [Referencing other HDI data as read-only via the linked HCP](#)
- [Changing the policy and schedule for migrating data to HCP](#)
- [Importing data from another file server](#)

Creating a shared directory

This section explains how to create a shared directory.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Create and Share File System dialog box on page C-103](#)
- [Migration Task Wizard on page C-348](#)

To create a shared directory

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the desired physical node, and then in the **Shares** tab in the window that is shown, click **Create and Share File System**.



Note: If data is migrated to the HCP system, the file system is linked to the HCP system at the file system level in the **Create and Share File System** dialog box displayed by clicking **Create and Share File System**. Therefore, if you want to link to the HCP system at the share level, use the **Create File System** dialog box rather than the **Create and Share File System** dialog box to create a file system. Then, allocate the namespace to the file share that is added directly below the mount point by using the **Add Share** dialog box.

3. In the **Basic** tab of the **Create and Share File System** dialog box, specify a share name, access protocols to be used (CIFS, NFS, or both), the share capacity, and other options.
Use a namespace and specify **Content sharing** to share data with other HDI systems via the linked HCP.
 - If not synchronizing data with other HDI systems: Select **Off** for **Content sharing**, and then specify the quota for namespace allocation of the migration destination.
 - If sharing data among HDI systems by using the read-write-content-sharing functionality: Select **On (Read/Write)** for **Content sharing**, and then specify the information about the migration-destination namespace.
 - If roaming among HDI systems is enabled for home directory data created for each end user: Select **Home directory** for **Content sharing**, and then specify the information about the migration-destination namespace. You must specify **CIFS** for the access protocol.

If you want to set quotas for users, groups, and file shares created directly below the shared directory, enable quotas. For details about how to set quotas for users and groups, see [Limiting the capacity used by a user or group on page 6-3](#). For details about how to set quotas for file shares created directly below the shared directory, see [Limiting the capacity used per file share on page 6-2](#).

4. If you selected the CIFS protocol in step 3, view the **CIFS** subtab of the **Access Control** tab, and then change the settings as necessary.
5. If you selected the NFS protocol in step 3, view the **NFS** subtab of the **Access Control** tab and change the settings as necessary.
6. If you selected only NFS for access protocols in step 3, clear the **Enable Advanced ACL type** check box in the **File System** subtab of the **Advanced** tab.
7. View the **Directory** subtab of the **Access Control** tab and change settings as necessary.
8. If you want to apply WORM to the files in the shared directory, specify the necessary information in the **WORM** tab.
If the WORM function is enabled, any file can be prevented from being changed or deleted for a set period of time. Verify and change the default settings as necessary. Note that if you specify **On (Read/Write)** or **Home directory** for **Content sharing**, you cannot enable the WORM functionality. Note that after enabling the WORM functionality, you cannot disable the WORM functionality.
9. View the **Namespace** tab, and change the settings as necessary.
10. View the **File System** subtab and the **Striping** subtab of the **Advanced** tab, and change settings as necessary.
Enable striping if you want to use striping, which divides contiguous data blocks of a file system into blocks of a desired size, and then evenly spread out the blocks across multiple LUs to increase access speed. Select two or more LUs that have the same capacity from **Select from existing LUs** in the **Basic** tab.
11. Click **OK**.
12. Verify the information shown in the confirmation dialog box, and then click **Confirm**.
13. Verify that the processing results are correct, and then click **Close**.

Referencing other HDI data as read-only via the linked HCP

This section describes referencing other HDI data as read-only via the linked HCP.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Create and Share File System dialog box on page C-103](#)

To reference other HDI data as read-only via the linked HCP

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.

2. In the object tree, select the desired physical node, and then in the **Shares** tab in the window that is shown, click **Create and Share File System**.



Note: In the **Create and Share File System** dialog box displayed by clicking **Create and Share File System**, the file system is linked to the HCP system at the file system level. Therefore, if you want to link to the HCP system at the share level, use the **Create File System** dialog box rather than the **Create and Share File System** dialog box to create a file system. Then, allocate the namespace to the file share that is added directly below the mount point by using the **Add Share** dialog box.

3. In the **Basic** tab of the **Create and Share File System** dialog box, specify a share name, the access protocols to be used (CIFS, NFS, or both), the namespace settings, and the share capacity.
Use a namespace, and specify **On (Read-Only)** for **Content sharing**.
4. If you selected the CIFS protocol in step 3, view the **CIFS** subtab of the **Access Control** tab and the **CIFS** subtab of the **Advanced** tab, and then change the settings as necessary.
5. If you selected the NFS protocol in step 3, view the **NFS** subtab of the **Access Control** tab and change the settings as necessary.
6. If you selected only NFS for access protocols in step 3, clear the **Enable Advanced ACL type** check box in the **File System** subtab of the **Advanced** tab.
7. View the **Directory** subtab of the **Access Control** tab and change the settings as necessary.
8. In the **Namespace** tab, specify the necessary information.
Specify the system information for the HCP namespace whose data you want to show and specify a namespace-access account.
If you are using the replication functionality in the HCP system, also specify the system information for the replica HCP system.
9. Click **Test Connection for Primary** to verify whether you can connect to the HCP system. If you have specified replica system information, click **Test Connection for Replica** to verify whether you can connect to the replica HCP system.
10. Click **OK**.
11. Verify the information shown in the confirmation dialog box, and then click **Confirm**.
12. Verify that the processing results are correct, and then click **Close**.

Changing the policy and schedule for migrating data to HCP

This section explains how to change the policy and schedule for migrating data to the HCP system.

GUI used for this operation

- [Migration Tasks dialog box on page C-336](#)

- [Migration Task Wizard on page C-348](#)

To edit the policy and schedule for migrating data to the HCP system

1. From the global task bar area of the Hitachi File Services Manager main window, select **Go**, and then select **Migration Tasks**.
2. In the **Migration Tasks** dialog box, select the target task, and then click **Edit Task**.
3. In the **2. Task Settings** page in the **Migration Task Wizard**, specify the required information.
4. In the **3. Schedule Settings** page, specify the required information.
5. In the **4. Policy Settings** page, specify the required information.
If you do not specify a policy, all files will be migrated.
6. In the **5. Confirmation** page, select **I have confirmed the above settings.**, and then click **Apply**.

Importing data from another file server

This section describes how to import file share data that is used in another file server to the HDI system. You can import data from multiple file servers at the same time. Up to 20 shares per HDI cluster can be imported at the same time. The import method depends on the protocol to be used. If you want to use the CIFS protocol, see [Using the CIFS protocol to import data from another file server on page 3-5](#). If you want to use the NFS protocol, see [Using the NFS protocol to import data from another file server on page 3-15](#). If the type of import-source share differs from the protocol to be used, some information such as file attributes might not be properly imported. Use the same protocol as the share type to import data. Note that import cannot be performed from a share that uses both the CIFS and NFS protocols.

Using the CIFS protocol to import data from another file server

This section describes how to import data from another file server by using the CIFS protocol.

Before importing data, you must set up the CIFS service configuration definition on both nodes. Only files that are in a non-WORM file system and are accessed by CIFS clients can be imported. The directory path of each file must be no more than 4,095 bytes, including the file name.

The following information and objects are not imported:

- File system attributes such as quota and share settings
- Symbolic links
- SACL (System ACL) and quota information for files and directories
- Encryption, compression, and not-content-indexed attributes for files and directories (The settings are removed.)

- Accounts that are not registered on the domain controller and accounts other than `Everyone`, `CREATOR OWNER`, or `CREATOR GROUP` (when domain authentication is used)
- Accounts that cannot be resolved by HDI: accounts that are not registered in user mapping as trusted domains, original accounts for accounts that are transferred by using Active Directory domains, and deleted accounts
- The directories and files of the following names: `.history`, `.snaps`, `.arc`, `.system_gi`, `.system_reorganize`, `.backupdates`, `.temp_backupdates`, `lost+found`, `.lost+found`

System directories that are used by the server and that are in CIFS shares targeted for importing sometimes fail to be imported. If this happens, revise the owner accounts as well as any other accounts for which file access permissions for the directories that failed to be imported are set, and then perform the import again.

No more than 700 ACEs set for files and directories can be imported. The imported files have archive attributes as DOS attributes. Also, the attributes for NTFS ACL are converted into the corresponding attributes for Advanced ACL. For details about correspondence between NTFS ACL and Advanced ACL attributes, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

If domain authentication is used and no import-target files exist for which the owners or ACLs are local accounts or accounts that are not resolved by HDI, import the files as described in [When domain authentication is used \(with no local account files\) on page 3-6](#).

If domain authentication is used and import-target files exist for which the owners or ACLs are local accounts or accounts that are not resolved by HDI, import the files as described in [When domain authentication is used \(with some local account files\) on page 3-9](#).

If only local authentication is used for the import-source file server, import the files as described in [When only local authentication is used on page 3-12](#).

For details about the user mapping method used when data is imported, see [Identifying users by user mapping on page 4-8](#).

When domain authentication is used (with no local account files)

This section describes how to import data from another file server by using the CIFS protocol when domain authentication is used, and there are no import-target files whose owners are local accounts.

GUI used for this operation

- [DNS, NIS, LDAP Setup page on page C-197](#)
- [CIFS Service Management page on page C-222](#)
- [Create and Share File System dialog box on page C-103](#)
- [Migration Task Wizard on page C-348](#)

- [List of RAS Information page on page C-164](#)

To import data from another file server by using the CIFS protocol when domain authentication is used, and there are no import-target files whose owners are local accounts

1. Create a data access account for importing.
Create an account for accessing shared data in an external authentication server. Set up an account so that the account can access all data in the shares to be imported. Specify the account name using no more than 256 characters and the password using no more than 128 characters. You can use alphanumeric characters, sign characters except backslashes (\), and multi-byte characters that are encoded in UTF-8.
2. Connect the HDI system to the network in which the HDI system can access the import-source file server.
3. Set the same DNS, NIS, and LDAP information for the HDI system as the one set for the import-source file server.
Set the information so that the name resolution and user authentication work when clients access the HDI system in the same way as when clients access the import-source file server. Also set up user and group mapping by the external authentication server.
4. Create and share the import-target file system in the HDI system. Specify **Off** for the **Content sharing** setting.
Create a non-WORM file system whose ACL type is Advanced ACL.
Do not create any files or directories in the file system until an import is started in step 12. If a file or directory path is the same as one in the import-source file system, the file or directory corresponding to that path in the import-source file system is not imported.
5. Set a migration task.
If you want to migrate file system data updated during an import, set a task so that data is regularly migrated. Note that an import might take longer than expected because an import temporarily stops when a migration is performed. To decrease the amount of time required for an import, set a task in step 16, after the import finishes.
6. Set up the import information by using the `datamigrateconfadd` command.
7. Verify that the target files and directories can be imported by using the `datamigratetest` command.
8. Set the file system free capacity levels at which imports are stopped and resumed by using the `datamigratelimitset` command.
9. Notify the clients who are using the import-source file server of the import schedule.
10. Set the shares in the import-source file server as read-only.
If an import-source file or directory is updated after the import starts, the file or directory might not be properly imported.
11. Use MMC (Microsoft Management Console) (or some other similar tool) to disconnect the session connected to the import-source file server.

For details about how to disconnect sessions, see the documentation for the import-source file server.

12. Start the data import by using the `datamigratestart` command.
If you want to set subtree quotas for the import-target directories, run the `datamigratestart` command with the `--type on-demand` option specified for the share that is the highest in the hierarchy. After that, set subtree quotas. After setting the quotas, run the `datamigratectl` command with the `--type all` option specified.
If you do not want to set subtree quotas, run the `datamigratestart` command with the `--type all` option specified, for the share that is highest in hierarchy.
The import starts in the background.
13. Inform the clients that they can start accessing shares in the HDI system.
Clients can access the shares in the HDI system during data importing. You can use the `datamigratestatus` command to check the import progress. The KAQM37163-I system message is output when importing finishes.
14. Verify the import result by using the `datamigratestatus` and `datamigrateconflist` commands.
If files or directories are moved while an import is being performed, those files might not have been imported. Confirm that all the files were imported.
If importing failed for some files, take action according to the recovery procedure described in the *Cluster Troubleshooting Guide*.
If no files failed, but the number of import-source files differs from the number of files that were successfully imported, repeat this procedure starting with step 12. The files that were not imported will be imported.
The KAQM37233-I message might be output if a node failure occurs or the file system capacity is insufficient. If this happens, the KAQM37233-I message is still output after an all-file import is performed again. Run the `datamigratestatus` command with the `--incompletionlist` option to verify that the displayed files are all imported. If the files have been imported, no action is necessary. If some files have not been imported, take action by, for example, manually copying the files one-by-one.
15. Confirm that all files have been imported, and then use the `datamigrateconfdel` command to cancel the data import setting.
If you cancel the setting, you can no longer restart the import, not even by resetting the import information.
16. Set a migration task.
Set a task if you did not set a task in step 5. If you set a task in step 5 and a migration has not been performed yet, run the `arcmodectl` command with the `--init-migration enable` option to enable initial mode for migration tasks. If 1,000,000 or more files are to be imported, execute the `arcmodectl` command with the `--init-migration enable` and `-t repeat` options specified to enable initial mode every time a task is executed. If you specify the `-t repeat` option, when the number of files to be migrated drops below 1,000,000, disable initial mode.

17. Remove the import-source file server.

If a failure occurred during data importing, take action according to the recovery procedure described in the *Cluster Troubleshooting Guide*.

When domain authentication is used (with some local account files)

This section describes how to import data from another file server by using the CIFS protocol when domain authentication is used, and there are some import-target files whose owners are local accounts.

If the import-source file server is Microsoft® Windows Server®, before importing data, download the Microsoft Visual C++ 2010 Redistributable Package (x86) from Microsoft Download Center, and then install it on the import-source file server.

GUI used for this operation

- [DNS, NIS, LDAP Setup page on page C-197](#)
- [CIFS Service Management page on page C-222](#)
- [Create and Share File System dialog box on page C-103](#)
- [Migration Task Wizard on page C-348](#)
- [List of RAS Information page on page C-164](#)

To import data from another file server by using the CIFS protocol when domain authentication is used, and there are some import-target files whose owners are local accounts

1. Create a data access account for import.
Create an account for accessing shared data in an external authentication server. Set up an account so that the account can access all data in the shares to be imported. Specify the account name using no more than 256 characters and the password using no more than 128 characters. You can use alphanumeric characters, sign characters except backslashes (\), and multi-byte characters that are encoded in UTF-8.

2. On the import-source file server, verify the local accounts, and then create a mapping file for using the accounts in the HDI system.
To create a mapping file for Microsoft® Windows Server®, use the mapping generation tool (`sidlist.exe`) that is stored in the following location in the HDI installation media.

installation-media-drive: \tool\sidlist

Copy the `sidlist.exe` to a desired directory on the import-source file server, and then run it by specifying the absolute path of the `sidlist.exe` and the mapping file.

Example of the `sidlist.exe` when stored in the `tool` directory on the D drive:

```
D:\>d:\tool\sidlist.exe >d:\tool\mappingfile.txt
```

The entries are output to a mapping file as follows:

```
[MAPDEF]
SID=account-SID
SRC_NAME=import-source-account-name
KIND=account-type (u (user) or g (group))
DST_NAME=import-target-account-name
```

Change the `DST_NAME` to the accounts that are registered for the domain. Specify the names in the form of *domain-name\account-name*.

Verify the character encoding of the mapping file (use UTF-8).

For servers other than Microsoft® Windows Server®, manually create a mapping file that contains the above entry for the local accounts.

3. Connect the HDI system to the network in which the HDI system can access the import-source file server.
4. Transfer the mapping file that you created in step 2 to the HDI system. Transfer the file to the home directory for the SSH account (`/home/nasroot`).
5. Set the same DNS, NIS, and LDAP information for the HDI system as the one set for the import-source file server.
Set the information so that the name resolution and user authentication work when clients access the HDI system in the same way as when clients access the import-source file server. Also set up user and group mapping by the external authentication server.
6. Create and share the import-target file system in the HDI system. Specify **Off** for the **Content sharing** setting.
Create a non-WORM file system whose ACL type is Advanced ACL.
Do not create any files or directories in the import-target file system until an import is started in step 15. If a file or directory path is the same as one in the import-source file system, the file or directory corresponding to that path in the import-source file system is not imported.
7. Set a migration task.
If you want to migrate file system data updated during an import, set a task so that data is regularly migrated. Note that an import might take longer than expected because an import temporarily stops when a migration is performed. To decrease the amount of time required for an import, set a task in step 20, after the import finishes.
8. Set up the import information by using the `datamigrateconfadd` command.
Use the `--mapdef` option to enable local account mapping.
9. Verify that the target files and directories can be imported by using the `datamigratetest` command.
10. Set the file system free capacity levels at which imports are stopped and resumed by using the `datamigratelimitset` command.
11. Verify the mapping for the local accounts by using the `datamigrateconflist` command.
If the information shown does not match the accounts that are used for the HDI system, re-create the mapping file by using the mapping

generation tool, and then reconfigure the mapping by using the `datamigrateconfedit` command.

12. Notify the clients who are using the import-source file server of the import schedule.
13. Set the shares in the import-source file server as read-only.
If an import-source file or directory is updated after the import starts, the file or directory might not be properly imported.
14. Use MMC (Microsoft Management Console) (or some other similar tool) to disconnect the session connected to the import-source file server.
For details about how to disconnect sessions, see the documentation for the import-source file server.
15. Start the data import by using the `datamigratestart` command.
If you want to set subtree quotas for the import-target directories, run the `datamigratestart` command with the `--type on-demand` option specified for the share that is the highest in the hierarchy. After that, set subtree quotas. After setting the quotas, run the `datamigratectl` command with the `--type all` option specified.
If you do not want to set subtree quotas, run the `datamigratestart` command with the `--type all` option specified, for the share that is highest in hierarchy.
The import starts in the background.
16. Inform the clients that they can start accessing shares in the HDI system.
Clients can access the shares in the HDI system during data importing. You can use the `datamigratestatus` command to check the import progress. The KAQM37163-I system message is output when importing finishes.
17. Check the import result by using the `datamigratestatus` and `datamigrateconflist` commands.
If files or directories are moved while an import is being performed, those files might not have been imported. Confirm that all the files were imported.
If importing failed for some files, take action according to the recovery procedure described in the *Cluster Troubleshooting Guide*.
If no files failed, but the number of import-source files differs from the number of files that were successfully imported, repeat this procedure starting with step 14. The files that were not imported will be imported.
The KAQM37233-I message might be output if a node failure occurs or the file system capacity is insufficient. If this happens, the KAQM37233-I message is still output after an all-file import is performed again. Run the `datamigratestatus` command with the `--incompletionlist` option to verify that the displayed files are all imported. If the files have been imported, no action is necessary. If some files have not been imported, take action by, for example, manually copying the files one-by-one.
18. Confirm that all files have been imported, and then use the `datamigrateconfdel` command to cancel the data import setting.

If you cancel the setting, you can no longer restart the import, not even by resetting the import information.

19. Delete the mapping file that you transferred in step 4 from the HDI system.
20. Set a migration task.
Set a task if you did not set a task in step 7. If you set a task in step 7 and a migration has not been performed yet, run the `arcmodectl` command with the `--init-migration enable` option to enable initial mode for migration tasks. If 1,000,000 or more files are to be imported, execute the `arcmodectl` command with the `--init-migration enable` and `-t repeat` options specified to enable initial mode every time a task is executed. If you specify the `-t repeat` option, when the number of files to be migrated drops below 1,000,000, disable initial mode.
21. Remove the import-source file server.

If a failure occurred during data importing, take action according to the recovery procedure described in the *Cluster Troubleshooting Guide*.

When only local authentication is used

This section describes how to import data from another file server by using the CIFS protocol when only local authentication is used.

If the import-source file server is Microsoft® Windows Server®, before importing data, download the Microsoft Visual C++ 2010 Redistributable Package (x86) from Microsoft Download Center, and then install it on the import-source file server.

GUI used for this operation

- [DNS, NIS, LDAP Setup page on page C-197](#)
- [Local Users dialog box on page C-150](#)
- [Create and Share File System dialog box on page C-103](#)
- [Migration Task Wizard on page C-348](#)
- [List of RAS Information page on page C-164](#)

To import data from another file server by using the CIFS protocol when only local authentication is used

1. Create a data access account for importing.
Create an account for accessing shared data in the import-source file server. Set up an account so that the account can access all data in the shares to be imported. Specify the account name using no more than 256 characters and the password using no more than 128 characters. You can use alphanumeric characters, sign characters except backslashes (\), and multi-byte characters that are encoded in UTF-8.
2. On the import-source file server, verify the local accounts, and then create a mapping file for using the accounts in the HDI system.

To create a mapping file for Microsoft® Windows Server®, use the mapping generation tool (`sidlist.exe`) that is stored in the following location in the HDI installation media.

`installation-media-drive:\tool\sidlist`

Copy the `sidlist.exe` to a desired directory on the import-source file server, and then run it by specifying the absolute path of the `sidlist.exe` and the mapping file.

Example of the `sidlist.exe` when stored in the `tool` directory on the `D` drive:

```
D:\>d:\tool\sidlist.exe >d:\tool\mappingfile.txt
```

Verify the character encoding of the mapping file, and then save the file in the UTF-8 format.

The entries are output to a mapping file as follows:

```
[MAPDEF]
SID=account-SID
SRC_NAME=import-source-account-name
KIND=account-type (u (user) or g (group))
DST_NAME=import-target-account-name
```

If you want to use different names in the HDI system than the ones that have been used on the import-source file server for some accounts, edit the `DST_NAME` for those accounts.

If you use domain accounts, specify the names in the form of `domain-name\account-name`.

Verify the character encoding of the mapping file (use UTF-8).

For servers other than Microsoft® Windows Server®, manually create a mapping file that contains the above entry for the local accounts.

3. Connect the HDI system to the network in which the HDI system can access the import-source file server.
4. Transfer the mapping file that you created in step 2 to the HDI system. Transfer the file to the home directory for the SSH account (`/home/nasroot`).

5. Register the local accounts that were used on the import-source file server to the HDI system.

Register the users and groups by using the names for `DST_NAME` in step 2 and specifying desired UIDs and GIDs.

6. Create and share the import-target file system in the HDI system. Specify **Off** for the **Content sharing** setting.

Create a non-WORM file system whose ACL type is Advanced ACL.

Do not create any files or directories in the import-target file system until an import is started in step 15. If a file or directory path is the same as one in the import-source file system, the file or directory corresponding to that path in the import-source file system is not imported.

7. Set a migration task.

If you want to migrate file system data updated during an import, set a task so that data is regularly migrated. Note that an import might take

longer than expected because an import temporarily stops when a migration is performed. To decrease the amount of time required for an import, set a task in step 20, after the import finishes.

8. Set up the import information by using the `datamigrateconfadd` command.
Use the `--mapdef` option to enable local account mapping.
9. Verify that the target files and directories can be imported by using the `datamigratetest` command.
10. Set the file system free capacity levels at which imports are stopped and resumed by using the `datamigratelimitset` command.
11. Verify the mapping for the local accounts by using the `datamigrateconflist` command.
If the information shown does not match the accounts that are used for the HDI system, re-create the mapping file by using the mapping generation tool, and then reconfigure the mapping by using the `datamigrateconfedit` command.
12. Notify the clients who are using the import-source file server of the import schedule.
13. Set the shares in the import-source file server as read-only.
If an import-source file or directory is updated after the import starts, the file or directory might not be properly imported.
14. Use MMC (Microsoft Management Console) (or some other similar tool) to disconnect the session connected to the import-source file server.
For details about how to disconnect sessions, see the documentation for the import-source file server.
15. Start the data import by using the `datamigratestart` command.
If you want to set subtree quotas for the import-target directories, run the `datamigratestart` command with the `--type on-demand` option specified for the share that is the highest in the hierarchy. After that, set subtree quotas. After setting the quotas, run the `datamigratectl` command with the `--type all` option specified.
If you do not want to set subtree quotas, run the `datamigratestart` command with the `--type all` option specified, for the share that is highest in hierarchy.
The import starts in the background.
16. Inform the clients that they can start accessing shares in the HDI system. Clients can access the shares in the HDI system during data importing. You can use the `datamigratestatus` command to check the import progress. The KAQM37163-I system message is output when importing finishes.
17. Check the import result by using the `datamigratestatus` and `datamigrateconflist` commands.
If files or directories are moved while an import is being performed, those files might not have been imported. Confirm that all the files were imported.

If importing failed for some files, take action according to the recovery procedure described in the *Cluster Troubleshooting Guide*.

If no files failed, but the number of import-source files differs from the number of files that were successfully imported, repeat this procedure starting with step 14. The files that were not imported will be imported.

The KAQM37233-I message might be output if a node failure occurs or the file system capacity is insufficient. If this happens, the KAQM37233-I message is still output after an all-file import is performed again. Run the `datamigratestatus` command with the `--incompletionlist` option to verify that the displayed files are all imported. If the files have been imported, no action is necessary. If some files have not been imported, take action by, for example, manually copying the files one-by-one.

18. Confirm that all files have been imported, and then use the `datamigrateconfdel` command to cancel the data import setting.
If you cancel the setting, you can no longer restart the import, not even by resetting the import information.
19. Delete the mapping file that you transferred in step 4 from the HDI system.
20. Set a migration task.
Set a task if you did not set a task in step 7. If you set a task in step 7 and a migration has not been performed yet, run the `arcmodectl` command with the `--init-migration enable` option to enable initial mode for migration tasks. If 1,000,000 or more files are to be imported, execute the `arcmodectl` command with the `--init-migration enable` and `-t repeat` options specified to enable initial mode every time a task is executed. If you specify the `-t repeat` option, when the number of files to be migrated drops below 1,000,000, disable initial mode.
21. Remove the import-source file server.

If a failure occurred during data importing, take action according to the recovery procedure described in the *Cluster Troubleshooting Guide*.

Using the NFS protocol to import data from another file server

This section describes how to import data from another file server by using the NFS protocol.

Before importing data, you must set up the NFS service configuration definition on both nodes. Only files that are in a non-WORM file system and are accessed by NFS clients can be imported. The directory path of each file must be no more than 4,095 bytes, including the file name.

The following information and objects are not imported:

- ACL and quota information for files and directories
- File system attributes such as quota and share settings
- Socket files

- The directories and files of the following names: `.history`, `.snaps`, `.arc`, `.system_gi`, `.system_reorganize`, `.backupdates`, `.temp_backupdates`, `lost+found`, `.lost+found`

GUI used for this operation

- [DNS, NIS, LDAP Setup page on page C-197](#)
- [Create and Share File System dialog box on page C-103](#)
- [Migration Task Wizard on page C-348](#)
- [List of RAS Information page on page C-164](#)

To import data from another file server by using the NFS protocol when only local authentication is used

1. Connect the HDI system to the network in which the HDI system can access the import-source file server.
2. Set the same DNS, NIS, and LDAP information for the HDI system as the one set for the import-source file server.
Set the information so that the name resolution and user authentication work when clients access the HDI system in the same way as when clients access the import-source file server. Also set up user and group mapping by the external authentication server.
3. Configure the shared directory on the import-source file server so that the directory can be accessed from the HDI system.
 - Set the HDI IP address as a client that can access the shared directory. If you use the front-end LAN, use the virtual IP address as the connection-source IP address. If you use the management LAN, use the management IP address as the connection-source IP address.
 - Set the directory as read-only, and enable clients to access the directory by using the root permissions that clients start with.
4. Create and share the import-target file system in the HDI system.
Create a non-WORM file system. Specify **Off** for the **Content sharing** setting.
Do not create any files or directories in the import-target file system until an import is started in step 11. If a file or directory path is the same as one in the import-source file system, the file or directory corresponding to that path in the import-source file system is not imported.
5. Set a migration task.
If you want to migrate file system data updated during an import, set a task so that data is regularly migrated. Note that an import might take longer than expected because an import temporarily stops when a migration is performed. To decrease the amount of time required for an import, set a task in step 15, after the import finishes.
6. Set up the import information by using the `datamigrateconfadd` command.

7. Verify that the target files and directories can be imported by using the `datamigratetest` command.
8. Set the file system free capacity levels at which imports are stopped and resumed by using the `datamigratelimitset` command.
9. Notify the clients who are using the import-source file server of the import schedule.
10. Set the shares in the import-source file server as read-only.
If an import-source file or directory is updated after the import starts, the file or directory might not be properly imported.
11. Start the data import by using the `datamigratestart` command.
If you want to set subtree quotas for the import-target directories, run the `datamigratestart` command with the `--type on-demand` option specified, for the share that is the highest in the hierarchy. After that, set subtree quotas. After setting the quotas, run the `datamigratectl` command with the `--type all` option specified.
If you do not want to set subtree quotas, run the `datamigratestart` command with the `--type all` option specified, for the share that is highest in hierarchy.
The import starts in the background.
12. Inform the clients that they can start accessing shares in the HDI system.
Clients can access the shares in the HDI system during data importing. You can use the `datamigratestatus` command to check the import progress. The KAQM37163-I system message is output when importing finishes.
13. Check the import result by using the `datamigratestatus` and `datamigrateconflist` commands.
If files or directories are moved while an import is being performed, those files might not have been imported. Confirm that all the files were imported.
If importing failed for some files, take action according to the recovery procedure described in the *Cluster Troubleshooting Guide*.
If no files failed, but the number of import-source files differs from the number of files that were successfully imported, repeat this procedure starting with step 11. The files that were not imported will be imported.
The KAQM37233-I message might be output if a node failure occurs or the file system capacity is insufficient. If this happens, the KAQM37233-I message is still output after an all-file import is performed again. Run the `datamigratestatus` command with the `--incompletionlist` option to verify that the displayed files are all imported. If the files have been imported, no action is necessary. If some files have not been imported, take action by, for example, manually copying the files one-by-one. Note that, if hard links for which different subtree quotas are set have not been imported to the import-source and import-target, check, and if necessary, revise the quota settings, and then create hard links for each.
14. Confirm that all files have been imported, and then use the `datamigrateconfdel` command to cancel the data import setting.

If you cancel the setting, you can no longer restart the import, not even by resetting the import information.

15. Set a migration task.

Set a task if you did not set a task in step 5. If you set a task in step 5 and a migration has not been performed yet, run the `arcmodectl` command with the `--init-migration enable` option to enable initial mode for migration tasks. If 1,000,000 or more files are to be imported, execute the `arcmodectl` command with the `--init-migration enable` and `-t repeat` options specified to enable initial mode every time a task is executed. If you specify the `-t repeat` option, when the number of files to be migrated drops below 1,000,000, disable initial mode.

16. Remove the import-source file server.

If a failure occurred during data importing, take action according to the recovery procedure described in the *Cluster Troubleshooting Guide*.

Setting up the access environment from clients

This chapter describes how to set up the HDI system access environment from clients that use shared directories.

- [Setting up the access environment from CIFS clients](#)
- [Identifying users by user mapping](#)
- [Collecting CIFS client access logs](#)
- [Setting up the access environment from NFS clients](#)
- [Improving the GUI operation for a large system](#)

Setting up the access environment from CIFS clients

This section describes how to set up the access environment from CIFS clients according to the network model that is used.

Joining nodes to an Active Directory® domain

A node can join an Active Directory domain to allow users belonging to the same domain or trusted domains to access HDI shared directories.

Prerequisites for joining a node to an Active Directory domain

Obtain the following Active Directory domain information that will be used during the joining procedure:

- DNS name and NetBIOS name of the domain that the node is joining
- Domain controller server name. Another name (alias) cannot be specified.
- Name and password of the domain controller user
- IP address of the DNS server used by the domain

Verify that the DNS server used by the domain is configured as follows:

- Virtual IP addresses for the nodes and the corresponding host names have been registered.
- The SRV records required for deploying the Active Directory service have been registered.
- All the IP addresses registered for the host names of the domain controllers can be used to communicate with the nodes.
- An IP address is not dynamically added to the host name for the domain controller.

The nodes need to be able to search for the domain controller of the domain with which a trust relationship has been established. If all the following conditions are satisfied, edit the `/etc/cifs/lmhosts` file:

- The domain to which the nodes belong has a trust relationship with another domain.
- Either the domain to which the nodes belong or a domain with which the nodes have a trust relationship is an NT domain.
- The nodes and a domain that has a trust relationship with the nodes exist on different network segments.

For details about how to edit the `/etc/cifs/lmhosts` file, see [Edit System File page on page C-209](#).

In the HDI system, create a shared directory that can use the CIFS protocol.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Network & System Configuration dialog box on page C-178](#)

- [Access Protocol Configuration dialog box on page C-217](#)
- [Cluster Management dialog box on page C-268](#)

To join an Active Directory domain

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type:** *network*) of the **Network & System Configuration** dialog box, click **DNS, NIS, LDAP Setup**.
4. In the **DNS, NIS, LDAP Setup** page, specify information about the DNS server used for the Active Directory domain, and click **OK**.
If a confirmation dialog box is shown, click **OK**.
5. In the **System Setup Menu** page, click **Close**.
6. In the **Advanced** subtab of the **Settings** tab of the *physical-node-name* window, click **Access Protocol Configuration**.
7. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **CIFS**, and then click **Modify Configuration**.
8. In the **CIFS Service Management** page (**Setting Type:** *Basic*), click **Change Authentication Mode**.
9. In the **Select Authentication Mode** page, select **Active Directory authentication** from the options, and then click **OK**.
10. In the **Active Directory Authentication** page, specify the necessary information, and then click **OK**.
11. In the **CIFS Service Management** page (**Setting Type:** *Basic*), click **OK**.
12. In the **CIFS Service Management** page, specify the necessary information, and then click **OK**.
Every time you switch the setting type and specify the information, click **OK**.
When an Active Directory domain is joined, Hitachi Data Systems recommends that you use user mapping to manage user information. For details about how to use user mapping, see [Identifying users by user mapping on page 4-8](#).
13. In the confirmation page, click **End of Settings**.
14. In the **List of Services** page, restart the CIFS service. Also, restart the NFS, FTP, or SFTP service as needed.
Inform any clients using the service of the temporary stoppage before starting. Select the target service and click **Restart**. For details about whether the NFS, FTP, and SFTP services need to be restarted, see [Conditions that the NFS, FTP, and SFTP services need to be restarted on page 4-4](#).



Note: If you restart the CIFS service during degenerated operation, only the services in the resource groups that belong to the failover-destination node will be restarted.

15. Repeat steps 6 to 14 on the other node so that the service settings within the cluster are the same.
16. Restart the OS.
Restart the operating systems of both nodes comprising the cluster.

Notes on after joining a node to an Active Directory domain

- If the Active Directory authentication is set, make sure that the system times of the domain controller, the HDI system, and CIFS clients are the same. If there is a time difference of more than 5 minutes among these systems, authentication might fail when CIFS clients access the HDI system.
- After changing the Active Directory domain, if you immediately change the settings to rejoin the nodes to their 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** page, click **Rejoin Active Directory Domain** to rejoin the nodes to the Active Directory domain.
- If you join the nodes to another Active Directory domain that has the same name as the previous one, an unnecessary computer account might remain in the previous Active Directory domain. Use the domain controller of the previous Active Directory domain to delete the unnecessary computer account.
- When a user registered in a domain attempts to access the CIFS share of an HDI system from a client machine that is not registered in the domain, user authentication might fail. In this case, use the **CIFS Service Maintenance** page to verify whether the NetBIOS name of the Active Directory domain has been set correctly.
- If Active Directory is used for user authentication, only users authenticated by Active Directory can access CIFS shares. Users locally authenticated by the HDI system cannot access CIFS shares.

Conditions that the NFS, FTP, and SFTP services need to be restarted

The NFS service needs to be restarted in the following cases:

- When using an Active Directory domain controller and KDC server together, and a different name is set rather than that of the domain to which the KDC server using the NFS service belongs, or that of the KDC server

The FTP or SFTP service needs to be restarted in the following cases:

- If the FTP or SFTP service settings allow users authenticated with Active Directory to log on, and the authentication type is changed from Active Directory to another type or from another type to Active Directory.

Rejoining an Active Directory domain

If a domain controller failure or a domain configuration change occurs while Active Directory is being joined, connection to the CIFS share might not be possible. In this case, the node can join the Active Directory domain again to restore the connection to the CIFS share.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Access Protocol Configuration dialog box on page C-217](#)

To rejoin the Active Directory domain

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Access Protocol Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **CIFS**, and then click **Service Maintenance**.
4. In the **CIFS Service Maintenance** page, click **Rejoin Active Directory Domain**.

The selected CIFS service is rejoined to the Active Directory domain.



Note: If an attempt to rejoin the Active Directory domain fails, manually delete any computer accounts remaining on the Active Directory domain, and try again.

Joining nodes to an NT domain

A node can join an NT domain to allow users belonging to the same domain or trusted domains to access HDI shared directories.

Prerequisites for joining a node to an NT domain

Obtain the following NT domain information that will be used during the joining procedure:

- DNS name and NetBIOS name of the domain that the node is joining
- Domain controller server name. Another name (alias) cannot be specified.
- User name and password of the domain controller administrator
- IP address of the DNS server used by the domain

The nodes need to be able to search for the domain controller of the domain with which a trust relationship has been established. If all the following conditions are satisfied, edit the `/etc/cifs/lmhosts` file:

- The domain to which the nodes belong has a trust relationship with another domain.

- Either the domain to which the nodes belong or a domain with which the nodes have a trust relationship is an NT domain.
- The nodes and a domain that has a trust relationship with the nodes exist on different network segments.

For details about how to edit the `/etc/cifs/lmhosts` file, see [Edit System File page on page C-209](#).

Make sure that the network segment to which the nodes are connected does not contain computers that are not servers and whose names are the same as the domain controller server name specified in the **NT Domain Authentication** page. When the nodes are connected to multiple network segments (including VLANs), verify the above condition for all the network segments to be connected.

In the HDI system, create a shared directory that can use the CIFS protocol.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Access Protocol Configuration dialog box on page C-217](#)
- [Cluster Management dialog box on page C-268](#)

To join an NT domain

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Access Protocol Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **CIFS** from the options, and then click **Modify Configuration**.
4. In the **CIFS Service Management** page (**Setting Type: Basic**), click **Change Authentication Mode**.
5. In the **Select Authentication Mode** page, select **NT domain authentication** from the options, and then click **OK**.
6. In the **NT Domain Authentication** page, specify the necessary information, and then click **OK**.
7. In the **CIFS Service Management** page (**Setting Type: Basic**), click **OK**.
8. In the **CIFS Service Management** page, specify the necessary information, and then click **OK**.

Every time you switch the setting type and specify the information, click **OK**.

When an NT domain is joined, Hitachi Data Systems recommends that you use user mapping to manage user information. For details about how to use user mapping, see [Identifying users by user mapping on page 4-8](#).

9. In the confirmation page, click **End of Settings**.
10. In the **List of Services** page, restart the CIFS service. Also, restart the FTP or SFTP service as needed.
Inform any clients using the service of the temporary stoppage before starting. Select the target service and click **Restart**. The FTP or SFTP service needs to be restarted if the FTP or SFTP service settings allow users authenticated with Active Directory to log on, and the authentication type is changed from Active Directory.



Note: If you restart the CIFS service during degenerated operation, only the services in the resource groups that belong to the failover-destination node will be restarted.

11. Repeat steps 2 to 10 on the other node so that the settings within the cluster are the same.
12. Restart the OS.
Restart the operating systems of both nodes comprising the cluster.

Configuring a workgroup

In a workgroup, nodes authenticate users who access nodes.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Access Protocol Configuration dialog box on page C-217](#)
- [Cluster Management dialog box on page C-268](#)
- [Local Users dialog box on page C-150](#)

To configure a workgroup

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Access Protocol Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **CIFS** from the options, and then click **Modify Configuration**.
4. In the **CIFS Service Management** page (**Setting Type: Basic**), click **Change Authentication Mode**.
5. In the **Select Authentication Mode** page, select **Local authentication** from the options, and then click **OK**.
6. In the **Local Authentication** page, specify the necessary information, and then click **OK**.
7. In the **CIFS Service Management** page (**Setting Type: Basic**), click **OK**.

8. In the **CIFS Service Management** page, specify the necessary information, and then click **OK**.
Every time you switch the setting type and specify the information, click **OK**.
9. In the confirmation page, click **End of Settings**.
10. In the **List of Services** page, restart the CIFS service. Also, restart the FTP or SFTP service as needed.
Inform any clients using the service of the temporary stoppage before starting. Select the target service and click **Restart**. The FTP or SFTP service needs to be restarted if the FTP or SFTP service settings allow users authenticated with Active Directory to log on, and the authentication type is changed from Active Directory.



Note: If you restart the CIFS service during degenerated operation, only the services in the resource groups that belong to the failover-destination node will be restarted.

11. Repeat steps 2 to 10 on the other node so that the settings within the cluster are the same.
12. Restart the OS.
Restart the operating systems of both nodes comprising the cluster.
13. In the **Basic** subtab of the **Settings** tab in the *physical-node-name* window, click **Local Users**.
14. In the **List of Users / Groups** page (for *List of users*) of the **Local Users** dialog box, select **List of groups** from the drop-down list, and then click **Display**.
15. In the **List of Users / Groups** page (for *List of groups*), click **Add New Group**.
16. In the **Add Group** page, add groups that access shared directories on the node, and then click **OK**.
To enable the group to access CIFS shared directories, select **Apply to CIFS ACL environment**.
17. In the **List of Users / Groups** page (for *List of groups*), select **List of users** from the drop-down list, and then click **Display**.
18. In the **List of Users / Groups** page (for *List of users*), click **Add New User**.
19. In the **Add User** page, add users that access shared directories on the node, and then click **OK**.
To enable the user to access CIFS shared directories, select **Apply to CIFS environment**.

Identifying users by user mapping

When user mapping is used, because the user ID and group ID are assigned for the CIFS clients managed by the Active Directory domain and NT domain, the HDI system can identify users.

User-mapping methods

User mapping using RIDs: When a CIFS client accesses the HDI file system, the RIDs (relative identifiers) comprising the SID are converted, and the user ID and group ID are automatically assigned.

User mapping using LDAP: User IDs and group IDs are assigned according to the user information registered in the LDAP server database. These IDs can be registered manually in advance, or automatically in the LDAP server database when a CIFS client accesses the HDI.

User mapping using Active Directory schema: When Active Directory authentication is used, correspondence for different identify IDs between NFS clients and CIFS clients can be managed as a user attribute. User IDs and group IDs are assigned according to the user information already registered in the domain controller.

Prerequisites for user mapping

- To change the user mapping method, you need to re-create the file systems after you migrate the data by using the Windows backup function.
- When 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.
- Make sure that the user IDs and group IDs used for user mapping do not overlap with those registered for the HDI system, NIS server, or user authentication LDAP server.
- If the RID or LDAP method is used to automatically assign user IDs and group IDs, the range of used IDs is reserved. The ID range can only have the maximum value changed.

To prevent the ID range used for user mapping from becoming non-extensible due to overlap with IDs registered for the HDI system, NIS server, or user authentication LDAP server, Hitachi Data Systems recommends that numerical IDs larger than those used for user mapping should not be used for the HDI system, NIS server, or user authentication LDAP server.

- When using LDAP user mapping, create a tree on the LDAP server that contains the user IDs and group IDs, before setting up the HDI system.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Access Protocol Configuration dialog box on page C-217](#)

To use user mapping

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Access Protocol Configuration** in the **Advanced** subtab of the **Settings** tab.

3. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **CIFS**, and then click **Modify Configuration**.
4. In the **CIFS Service Management** page (**Setting Type: Basic**), select **User mapping** from **Setting Type**, and then click **Display**.
5. In the **CIFS Service Management** page (**Setting Type: User mapping**), specify the necessary information in **User mapping setup**, and click **OK**.
6. In the confirmation page, click **End of Settings**.
7. Restart the CIFS service.
Inform the clients that are using the service of the temporary stoppage before starting. Select the target service, and click **Restart**.

**Note:**

- If you restart the CIFS service during degenerated operation, only the services in the resource groups that belong to the failover-destination node will be restarted.
 - Even if a user registered on the domain controller is registered with the same name as for the HDI, the NIS server, or the LDAP server for user authentication, the user ID and group ID assigned by user mapping will be used when the user accesses a CIFS share.
 - You can use commands to view information about users and groups mapped by the RID method. For details about how to view user mapping information, see the *CLI Administrator's Guide*.
-
8. Repeat steps 2 to 7 on the other node so that the settings within the cluster are the same.

Collecting CIFS client access logs

You can specify when CIFS client access logs (CIFS access logs) should be collected.

Specified settings are applied to the entire CIFS service. However, if events that are recorded as the CIFS access log are specified for each CIFS share by using the `cifscreate` command or the `cifsedit` command, the settings for each CIFS share are given priority over the settings for the entire CIFS service. When the settings for the CIFS service are changed, verify the settings for each CIFS share as well as the settings for the entire CIFS service.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Add Share dialog box on page C-38](#)
- [Network & System Configuration dialog box on page C-178](#)
- [Access Protocol Configuration dialog box on page C-217](#)

To collect CIFS client access logs

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, select the target file system, and then click **Add Share** in the **File System** subtab of the **File Systems** tab.
3. In the **Add Share** dialog box, specify the required information, and then click **OK**.
Create the directory to which log files are backed up.
4. Set up the directory to which log files are backed up by using the `cifslogctl` command.
5. Configure the system so that the warning is output when the used capacity of file system exceed the threshold by using the `fsfullmsg` command.
6. In the object tree, select the target node, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
7. In the **System Setup Menu** page (**Setting Type:** `network`) of the **Network & System Configuration** dialog box, select **system** from **Setting Type**, and then click **Display**.
8. In the **System Setup Menu** page (**Setting Type:** `system`), click **Edit System File**.
9. In the **Edit System File** page, set up SNMP trap notification, and then click **OK**.
For details about how to set up SNMP trap, see [Chapter 10, Monitoring the system on page 10-1](#)
10. In the **System Setup Menu** page, click **Log File Capacity Setup**.
11. In the **Log File Capacity Setup** page, click **Edit**.
12. In the **Edit File Capacity** page, specify the log file capacity and the number of log files to be saved, and then click **OK**.
13. Close the **Network & System Configuration** dialog box.
14. In the object tree, select the target node, and in the window that is shown, click **Access Protocol Configuration** in the **Advanced** subtab of the **Settings** tab.
15. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **CIFS** from the options, and then click **Modify Configuration**.
16. In the **CIFS Service Management** page (**Setting Type:** `Basic`), select **Security** from **Setting Type**, and then click **Display**.
17. In the **CIFS Service Management** page (**Setting Type:** `Security`), select **Use** for **CIFS access log**, and then click **Set Up** in **Events logged to the CIFS access log**.
18. In the **Setting Events Logged to the CIFS Access Log** page, select events that you want to record as the CIFS access log, and then click **OK**.

19. In the **CIFS Service Management** page (**Setting Type:** *Security*), click **OK**.
20. In the confirmation page, click **End of Settings**.

Setting up the access environment from NFS clients

This section explains how to enable NFS clients to access shared directories.

If Kerberos authentication is used, set up an NTP server to synchronize the times of the HDI system and the NFS client hosts.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Access Protocol Configuration dialog box on page C-217](#)

To enable NFS clients to access shared directories

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Access Protocol Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **NFS** from the options, and then click **Modify Configuration**.
4. In the **NFS Service Management** page, specify the required information, and then click **OK**.
5. In the **List of Services** page, select **NFS**, and then click **Restart**.
6. Repeat steps 2 to 5 on the other node so that the settings within the cluster are the same.

Improving the GUI operation for a large system

If you manage an HDI system that has more than 10,000 clients, you can improve the performance of the Hitachi File Services Manager GUI by limiting the number of users and groups for which the SNMP manager references the quota information, and switching from GUI operation mode to command operation mode.

If you limit the number of users and groups for which the SNMP manager references the quota information, the MIBs for certain users and groups might not be able to be obtained by the `get` requests.

In command operation mode, processing is suppressed for the following operations in windows where a timeout might occur:

- Setting user or group quotas for a file system (the **Quota Setup** page of the **Edit Quota** dialog box)
- Showing user or group quota information for a file system (the **List of Quota Information** page of the **Edit Quota** dialog box)

Use commands to perform these operations.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Network & System Configuration dialog box on page C-178](#)

To improve the GUI operation for a large system

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type**: *network*) of the **Network & System Configuration** dialog box, select **system** from the **Setting Type** drop-down list, and then click **Display**.
4. In the **System Setup Menu** page (**Setting Type**: *system*), click **Edit System File**.
5. On the **Edit System File** page, from the **File type** drop-down list, select the `snmpd.conf` file, and then click **Display**.
6. Append the following two lines to the file.


```
std_quota_max 10000
std_stquota_max 10000
```
7. Click **OK**.
8. In the **System Setup Menu** page (**Setting Type**: *system*), click **Select User Interface**.
9. In the **Select User Interface** page, select **Command operation mode**, and then click **OK**.

Showing previous data

This chapter describes how to show clients the previous files in shared directories.

- [Showing previous data on HCP](#)

Showing previous data on HCP

This section explains how to show clients previous data that was migrated to the HCP system.

GUI used for this operation

- [File Systems window on page C-33](#)
- [Edit File System dialog box on page C-44](#)

To show clients previous data migrated to the HCP system

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **File Systems**.
2. In the File Systems window, select the desired file system, and then click **Edit**.
3. In the **Namespace** tab of the **Edit File System** dialog box, select **Yes** for **Use file version restore**, and then specify how the previous data is to be kept.
4. Click **OK**.
5. Verify the information shown in the confirmation dialog box, and then click **Confirm**.
6. Verify that the processing results are correct, and then click **Close**.
7. Change the CIFS client settings for the shared directory so that all files and folders are displayed.

This allows CIFS clients to view to the `.history` folder in the shared directory in which previous data is shown.

Managing disk capacity

This chapter describes how to expand and limit capacity.

- [Expanding file system capacity](#)
- [Limiting the capacity used per file share](#)
- [Limiting the capacity used by a user or group](#)

Expanding file system capacity

This section explains how to expand the file system capacity for a shared directory.

GUI used for this operation

- [File Systems window on page C-33](#)
- [Expand File System dialog box on page C-52](#)

To expand the file system capacity

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **File Systems**.
2. In the File Systems window, select the desired file system, and then click **Expand**.
3. In the **Basic** tab of the **Expand File System** dialog box, specify an LU size or select existing LUs to be added.
4. View the **Advanced** tab and change the maximum percentage of space that can be used for an inode as necessary. The maximum capacity that can be used as an inode is 1 TB.
5. Click **OK**.
6. Verify the information shown in the confirmation dialog box, and then click **Confirm**.
7. Verify that the processing results are correct, and then click **Close**.

Limiting the capacity used per file share

This section explains how to limit the capacity used per file share directly below the mount point when quota is enabled.

GUI used for this operation

- [Shares window on page C-5](#)
- [Change Share Quota dialog box on page C-19](#)

To limit the capacity used per file shares

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Shares**.
2. In the Shares window, click the name of the desired file share, and then in the window that is shown, click **Change Share Quota**.
3. When limiting the capacity by specifying the capacity of the file share (the block capacity that can be used), select **Enable share quota** in the **Change Share Quota** dialog box, and then specify the capacity for the file share in **Total**.

When linking with the HCP system at the share level, and when limiting the capacity based on the hard quota of a migration-destination namespace, specify the hard quota to be allocated to the namespace in **Allocate quota**, and then select **Synchronize the file share capacity with the namespace quota**.

4. Click **OK**.
5. Verify the information shown in the confirmation dialog box, and then click **Confirm**.
6. Verify that the processing results are correct, and then click **Close**.

Limiting the capacity used by a user or group

This section explains how to limit the capacity used by a user or group when quota is enabled.

GUI used for this operation

- [File Systems window on page C-33](#)
- [Edit Quota dialog box on page C-55](#)

To limit the capacity used by a user or group

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **File Systems**.
2. In the File Systems window, click the name of the desired file system, and then in the window that is shown, click **Edit User/Group Quota**.
3. If you want to set a group quota, in the **List of Quota Information** page (for `User`) of the **Edit Quota** dialog box, select **Group** from the drop-down list, and then click **Display**.
4. In the **List of Quota Information** page, select one or more users or groups for which a quota is to be set, and then click **Quota Setup**.
5. In the **Quota Setup** page, specify the soft limits (warning threshold) and hard limits (maximum) for blocks and inodes, and then click **OK**.



Tip: You can set the default quota that is applied to users and groups for which quota is not specifically set (see [Default Quota Setup page on page C-62](#)).

You can set quota monitoring that notifies you when users or groups have exceeded the soft limit or grace period (see [Monitoring Setup page on page C-61](#)).

Protecting user data

This chapter describes how to set up virus scanning, and back up and restore user data.

- [Setting up virus scanning](#)
- [Backing up data to a tape device](#)
- [Restoring data from a tape device](#)

Setting up virus scanning

This section explains how to set up virus scanning that is performed when CIFS clients access files.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Virus Scan Server Configuration dialog box on page C-283](#)

To set up virus scanning

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the desired physical node, and then in the **Advanced** subtab of **Settings** tab in the window that is shown, click **Virus Scan Server Configuration**.
3. In the **List of Scanner Servers** page of the **Virus Scan Server Configuration** dialog box, click **Scanning Software**.
4. In the **Scanning Software** page, select the desired software, and then click **OK**.
5. In the **List of Scanner Servers** page, click **Add Server**.
6. In the **Add Scanner Server** page, specify the IP address, domain name, or host name of the scan server, and a port number of the scan server, and then click **Add**.
7. In the **List of Scanner Servers** page, click **Scan Conditions**.
8. View the **Scan Conditions** page, change settings as necessary, and click **OK**.
9. Repeat steps 2 to 8 for the other node in the cluster.



Note: Real-time scanning is not performed for the clients who are accessing the CIFS share before scanning is enabled. In this case, restart the CIFS service, or ask the clients to reconnect to the CIFS service.

Backing up data to a tape device

This section explains how to back up the data to a tape device.

Change the default password (`ndmp`) for connecting the backup server to the NDMP server to prevent unauthorized access, by using the `ndmppasswd` command.

If either of the following conditions is met, backup processing might end with an error:

- The total size of the length of the directory and file names to be backed up at the same time exceeds 1 GB.

- The total size of the length of the directory and file names in the directory immediately under the directories to be backed up at the same time exceeds 1 GB.

When calculating the sum, add 1 byte as the delimiter between each directory and file.

Make sure the total length of the names of the directories and files to be backed up does not exceed 1 GB by reducing the number of directories and files to be backed up, or by adjusting the hierarchy.

GUI used for this operation

- [Migration Task Wizard on page C-348](#)
- [Access Protocol Configuration dialog box on page C-217](#)
- [File Systems window on page C-33](#)
- [Migration Tasks dialog box on page C-336](#)
- [file-system window on page C-62](#)

To back up data to a tape device

1. If data is migrated to HCP, perform migration before backup.
You can save the amount of area used in the backup media by migrating some of the data to HCP.
2. Estimate the required backup media capacity from the amount of data to be backed up, and then prepare a tape device.
For details on how to estimate the backup media capacity, see the *Installation and Configuration Guide*.
3. If you want to back up data to a tape device connected to a node via a SAN, register tape drive information for the NDMP server.
For details on how to set up a tape device connected to a node via a SAN, see the *Installation and Configuration Guide*.
4. Set up the operating environment for the backup management software.
For details on how to set up an operating environment for the backup management software, see the supplementary Backup Restore documentation that is provided with HDI.



Note: Some backup management software products might not work correctly if the length of the path for data to be backed up is too long. Before starting formal operations, perform a test to verify that backup and restore operations are performed correctly.

If the interruption for an offline backup is configured so that backup processing continues even if a file is modified or deleted during the offline backup, go to step 8. You can use the `ndmpfsconfig` command to view and change the interruption settings.

5. On the node where the backup-source directories and files reside, stop the NFS, CIFS, FTP, SFTP, and TFTP services.

6. Back up the file share information by using the `cifsbackup` and `nfsbackup` commands as necessary.
7. Unmount and then remount the file system.
When mounting the file system, enable quota if you want to back up quota information.
8. Verify that the file system that you want to back up is mounted, and if not, mount it.
9. Restart the NDMP server if you performed any of the following operations after the last restart.
 - Set or change the fixed IP address, virtual IP address, or subnet mask of the node
 - Set or change the IP address or host name of the gateway
 - Add or change backup server information in the `/etc/hosts` file
10. Verify that the NDMP server is running normally.
11. Record the file system attributes such as the ACL type and the permissions and ACLs of all the directories above and for the directory used as the base point for the backup.
12. Use backup management software to perform the backup operation.
13. Restart the NFS, CIFS, FTP, SFTP, and TFTP services if you stopped them in step 5.

Restoring data from a tape device

This section explains how to restore data from a tape device.

When restoring files by specifying each file, if you specify more than 10,000 directories and files individually as restoration targets, restoration processing might end with an error. Make sure that the total number of directories and files does not exceed 10,000 by reducing the number of directories and files or by batch restoration of the data.

GUI used for this operation

- [Create File System dialog box on page C-126](#)
- [Access Protocol Configuration dialog box on page C-217](#)
- [File Systems window on page C-33](#)
- [Add Share dialog box on page C-38](#)

To restore data from a tape device

1. If you want to restore data from a tape device connected to a node via a SAN, register tape drive information for the NDMP server.
For details on how to set up a tape device connected to a node via a SAN, see the *Installation and Configuration Guide*.
2. Set up the operating environment for the backup management software.

For details on how to set up the operating environment for the backup management software, see the supplementary Backup Restore documentation that is provided with HDI.

3. Prepare the restore-destination file system.

For the restore-destination file system, a capacity that is 105% or more of the size of the restore data is required. Hitachi Data Systems recommends that you use the same ACL type as the one used when the data has been backed up. If you need to restore backup data of the Classic ACL type to a file system of the Advanced ACL type, consider the amount of space required for ACL conversion. For details, see the *Installation and Configuration Guide*.

For WORM file system data, restore the data to the original file system if you can use the file system without a problem.

The data of a file system that supported 64-bit inodes needs to be restored in a file system that supports 64-bit inodes. If you restore the data in a file system that does not support 64-bit inodes, the number of files might exceed the maximum number of files that can be created in a file system.

To restore data to a file system that is different from the backup source, create a new file system. If you restore data in an existing file system, the number of files might exceed the maximum number of files that can be created in a file system.

If data is migrated to HCP, use the `arcrestore` command to restore HCP data before restoring data from the backup media.

4. Prepare the restore-destination directory.

Create the same directory hierarchy from the mount point to the parent directory of the restoration target, and set the same permissions for all the directories in the hierarchy as in the backup data. If the same directory hierarchy does not exist, directories from the mount point to the parent directory will automatically be created during the restore operation but might be assigned different permissions or ACLs from those present when a backup is performed.

To restore data to a WORM file system, the structure of the directories and files in the file system must be the same as when the data was backed up.

If you created a new file system, go to step 6.

5. Stop the NFS, CIFS, FTP, SFTP, and TFTP services on the node that the restore-destination file system resides in.

6. Verify that the file system that you want to back up is mounted with the read and write permissions enabled, and with quota enabled if you want to restore quota information.

If the file system you want to backup is not mounted, mount it with the read and write permissions enabled, and with quota enabled if you want to restore quota information.

7. Restart the NDMP server if you performed any of the following operations after the last restart.

- o Set or change the fixed IP address, virtual IP address, or subnet mask of the node

- Set or change the IP address or host name of the gateway
 - Add or change backup server information in the `/etc/hosts` file
8. Use backup management software to perform the restore operation.
If data for multiple file systems exists in the data to be restored, restore the data for each file system. If multiple directories and files with the same relative paths exist within the selected data, the data might be restored to an unintended state.



Note: When the restore operation is performed for a file or directory without using the DAR function, the processing time increases depending on the amount of backup data, not depending on the amount of data to be restored.

For details about backed-up quota information and how to restore it, see [Appendix E, Backing up and restoring quota information on page E-1](#).

9. If you stopped the NFS, CIFS, FTP, SFTP, and TFTP services in step 5, restart the services.
10. Create a file share for the file system.

Backing up the system configuration

This chapter describes how to back up the system configuration manually and automatically.

- [Manually backing up system configuration](#)
- [Regularly backing up system configuration](#)

Manually backing up system configuration

This section explains how to manually back up the system configuration within the system and download the system configuration file to a disk outside of the system.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Backup Configuration dialog box on page C-171](#)

To manually back up the system configuration

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Backup Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **Save System Settings Menu** page of the **Backup Configuration** dialog box, click **Save All System Settings**.
4. In the **Save All System Settings** page, click **Save and Download** or **Batch Save and Download**.
5. Click **OK**.

Regularly backing up system configuration

This section explains how to regularly (automatically) back up system configuration.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Backup Configuration dialog box on page C-171](#)

To regularly back up system configuration

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Backup Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **Save System Settings Menu** page of the **Backup Configuration** dialog box, click **Save All System Settings**.
4. On the **Save All System Settings** page, click **Modify Schedule**.
5. In the **Schedule Settings for Saving All System Settings** page, specify the backup interval, backup time, and output setting.

Select **Transfer to HCP** or **Output directory** for the output setting. If you select **Output directory**, click **Select**, select the file system to which you want to back up the system configuration file on the **List of Mounted File Systems** page, and then click **OK**.

6. Click **OK**.

Changing the network configuration

This chapter describes how to change the network configuration.

Note: If there are any errors in the network settings of the management port (`mng0`), you cannot connect to the HDI system from the management console, and as a result, you will experience difficulties in system recovery as a system administrator. Therefore, make sure there are no errors in the network settings after you have changed them.

- [Changing the IP address of a node](#)
- [Changing the host name of a node](#)
- [Adding and deleting routing information](#)
- [Changing the negotiation mode](#)
- [Setting up redundant link configuration](#)
- [Setting up a VLAN](#)

Changing the IP address of a node

This section explains how to change the IP address of a node.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Cluster Management dialog box on page C-268](#)
- [processing-node window on page C-86](#)
- [Network & System Configuration dialog box on page C-178](#)

To change the IP address of a node

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node.
3. To change the `mng0` interface fixed IP address, go to the **Settings** tab and then the **Advanced** subtab, and click **Cluster Management**. To change the virtual interface IP address, proceed to step 8.
4. In the **Browse Cluster Status** page (for `Cluster / Node status`) of the **Cluster Management** dialog box, select **Resource group status** from the drop-down list, and then click **Display**.
5. In the **Browse Cluster Status** page (for `Resource group status`), stop both resource groups.
`Offline/No error` appears under **Resource group status**.
6. In the **Cluster Management** dialog box, go to the **Browse Cluster Status** page, select **Cluster / Node status** from the drop-down list, and click **Display**.
7. In the **Browse Cluster Status** page (**Cluster / Node status** view), stop the cluster.
INACTIVE appears under **Cluster status**.
8. In the **Advanced** subtab of **Settings** tab in the *physical-node-name* window that is shown by selecting the physical node in the object tree, click **Network & System Configuration**.
9. In the **System Setup Menu** page (**Setting Type**: `network`) of the **Network & System Configuration** dialog box, click **Interface Management**.
10. In the **List of Interfaces** page, select the protocol version for which you want to edit the information from the **Protocol version** drop-down list, and then click **Display**.
11. Select the interface for which you want to change the IP address, and then click **Edit**.
12. In the **Edit Interface** page, change the IP address, and then click **OK**.
13. If you stopped the cluster in step 7, start the cluster.
14. If you stopped the resource groups in step 5, restart them.

15. If you change the network address of `mng0` in step 13 for a configuration in which a BMC port is connected to an IP switch to which the management port is connected, set the same network address as `mng0` to the BMC port.

Use the `bmcctl` command to change the BMC port interface setting.

For details about how to set the BMC port interface, see the *CLI Administrator's Guide*.

Changing the host name of a node

This section explains how to change the host name of a node.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Backup Configuration dialog box on page C-171](#)
- [Cluster Management dialog box on page C-268](#)
- [processing-node window on page C-86](#)

To change the host name of a node

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Backup Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **Save System Settings Menu** page of the **Backup Configuration** dialog box, click **Save All System Settings**.
4. In the **Save All System Settings** page, click **Save and Download**.
5. Click **OK**.
6. In the **Advanced** subtab of **Settings** tab in the *physical-node-name* window, click **Cluster Management**.
7. In the **Browse Cluster Status** page (for `Cluster / Node status`) of the **Cluster Management** dialog box, select **Resource group status** from the drop-down list, and then click **Display**.
8. In the **Browse Cluster Status** page (for `Resource group status`), stop both resource groups.
9. In the **Browse Cluster Status** page (for `Resource group status`) of the **Cluster Management** dialog box, select **Cluster / Node Status** from the drop-down list, and then click **Display**.
10. In the **Browse Cluster Status** page (for `Cluster / Node status`), click **Stop** to stop the cluster.
11. Click **Modify Configuration**.
12. In the **Modify Cluster Configuration** page, click **Modify Host Name**.
13. Change the host name, and then click **OK**.

14. In a dialog box that confirms that you change the host name, click **OK**.
15. Start the cluster.
16. Start the resource groups.
17. In the *processing-node-name* window that is shown by selecting the processing node in the object tree, click **Refresh Processing Node**. The physical node names in the window display the new host names.

Adding and deleting routing information

This section explains how to add and delete routing information.

Adding routing information

This section describes how to add routing information.

If you perform the described operations on a physical node, the settings will be applied to both nodes in the cluster.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Network & System Configuration dialog box on page C-178](#)

To add routing information

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type**: *network*) of the **Network & System Configuration** dialog box, click **Routing Setup**.
4. In the **List of Routings** page, select the protocol version for which you want to add the information from the **Protocol version** drop-down list, and then click **Display**.
5. Click **Add**.
6. In the **Add Routing** page, enter the required information, and then click **OK**.

Deleting routing information

This section describes how to delete routing information.

If you perform the described operations on a physical node, the settings will be applied to both nodes in the cluster.

If the host name specified for the routing target or gateway cannot be resolved, you might not be able to delete the routing information correctly. If

a host name is specified for the routing target or gateway, make sure that the host name can be resolved before you delete routing information.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Network & System Configuration dialog box on page C-178](#)

To delete routing information

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type:** *network*) of the **Network & System Configuration** dialog box, click **Routing Setup**.
4. Select the protocol version for which you want to add the information from the **Protocol version** drop-down list, and then click **Display**.
5. Select the routing information you want to delete, and then click **Delete**.
6. Click **OK**.

If you delete the routing information of the management port, the database cache information on the management server might become inconsistent with that on the node, or it might become impossible to open dialog boxes from the **Settings** tab. Log on to the Hitachi File Services Manager from another management console in the same network as the nodes, and make necessary settings for the routing information.

Changing the negotiation mode

This section explains how to change the negotiation mode of network ports.

If cascaded trunking is not set up for the port, see [Changing the negotiation mode \(for a non-cascaded trunk port\) on page 9-5](#). If it is set up for the port, see [Changing the negotiation mode \(for a cascaded trunk port\) on page 9-6](#).

Changing the negotiation mode (for a non-cascaded trunk port)

This section describes how to change the negotiation mode of a non-cascaded trunk port.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Cluster Management dialog box on page C-268](#)
- [Network & System Configuration dialog box on page C-178](#)

To change the negotiation mode of a non-cascaded trunk port

1. Disable the monitoring of the resource group operating on the node.
In the object tree, select the node, and then click **Cluster Management** in the **Advanced** subtab of the **Settings** tab. Then, in the **Browse Cluster Status** page (for `Resource group status`) of the **Cluster Management** dialog box, select the resource group, and then click **Cancel Monitoring**.
2. Click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type:** `network`) of the **Network & System Configuration** dialog box, click **Data Port Setup**.
4. In the **List of Data Ports** page, select the port to change the negotiation mode, and then click **Negotiation Mode Setup**.
If link alternation is set up for the port, make sure beforehand that the port is in `standby` status. The status of a link alternation port can be confirmed on the **List of Trunking Configurations** page (see [List of Trunking Configurations page on page C-187](#)).
5. In the **Negotiation Mode Setup** page, change the negotiation mode, and then click **OK**.
After changing the setting on HDI, reconfigure the connected switch accordingly.



Note: When the connected switch is reconfigured, the port might temporarily link down with the KAQG01013-W message.

6. In the **List of Data Ports** page, confirm that the negotiation mode has been changed.
7. If trunking is set on the port where you changed the negotiation mode, repeat steps 4 through 6 so that all the ports included in the trunking are set to the same negotiation mode.
If link alternation is set, change the negotiation mode, wait about 10 seconds, alternate the link manually, and then repeat steps 4 through 6. For information about how to perform manual link alternation, see [Performing manual link alternation on page 9-10](#).
8. Close the **Network & System Configuration** dialog box.
9. Resume the monitoring of the resource group for which monitoring was disabled.
Click **Cluster Management** in the **Advanced** subtab of the **Settings** tab. Then, in the **Browse Cluster Status** page (for `Resource group status`) of the **Cluster Management** dialog box, click **Monitor**.
10. Repeat steps 1 to 9 for the other node in the cluster.

Changing the negotiation mode (for a cascaded trunk port)

This section describes how to change the negotiation mode of a cascaded trunk port.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Cluster Management dialog box on page C-268](#)
- [Network & System Configuration dialog box on page C-178](#)

To change the negotiation mode of a cascaded trunk port

1. Disable the monitoring of the resource group operating on the node.
In the object tree, select the node, and then click **Cluster Management** in the **Advanced** subtab of the **Settings** tab. Then, in the **Browse Cluster Status** page (for `Resource group status`) of the **Cluster Management** dialog box, select the resource group, and then click **Cancel Monitoring**.
2. Click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type:** `network`) of the **Network & System Configuration** dialog box, click **Data Port Setup**.
4. In the **List of Data Ports** page, select a port of the link aggregation that is in `Standby` status, and then click **Negotiation Mode Setup**.
The status of a link alternation port can be confirmed on the **List of Trunking Configurations** page (see [List of Trunking Configurations page on page C-187](#)).
5. In the **Negotiation Mode Setup** page, change the negotiation mode, and then click **OK**.
After changing the setting on HDI, reconfigure the connected switch accordingly.



Note: When the connected switch is reconfigured, the port might temporarily link down with the KAQG01013-W message.

6. In the **List of Data Ports** page, confirm that the negotiation mode has been changed.
7. Repeat steps 4 to 6 so that all ports of the link aggregation that is in `Standby` status have the same negotiation mode.
8. After changing the negotiation mode, wait 10 seconds or so, and then perform manual link alternation.
For information about how to perform manual link alternation, see [Performing manual link alternation on page 9-10](#).
9. Repeat steps 4 to 7 for each port of the link aggregation that is now in `Standby` status.
10. Close the **Network & System Configuration** dialog box.
11. Resume the monitoring of the resource group for which monitoring was disabled.
Click **Cluster Management** in the **Advanced** subtab of the **Settings** tab. Then, in the **Browse Cluster Status** page (for `Resource group status`) of the **Cluster Management** dialog box, click **Monitor**.

12. Repeat steps 1 to 11 for the other node in the cluster.

Setting up redundant link configuration

This section explains how set up redundant link configuration.

Setting link aggregation

GUI used for this operation

- [physical-node window on page C-91](#)
- [Network & System Configuration dialog box on page C-178](#)

To set link aggregation

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the node to set the link aggregation, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type**: *network*) of the **Network & System Configuration** dialog box, click **Trunking Setup**.
4. In the **List of Trunking Configurations** page, select the ports for which you want to set link aggregation, and then click **Create Link Aggregation**.
5. In the **Link Aggregation Setup** page, click **OK**.
6. Click **OK**.
After setting the link aggregation, modify the settings of the destination switch.



Note: From the **Add Interface** page of the **Network & System Configuration** dialog box, you must add interfaces for the ports for which link aggregation is set.

Setting link alternation

GUI used for this operation

- [physical-node window on page C-91](#)
- [Network & System Configuration dialog box on page C-178](#)

To set link alternation

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.

2. In the object tree, select the node to set the link alternation, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type:** *network*) of the **Network & System Configuration** dialog box, click **Trunking Setup**.
4. In the **List of Trunking Configurations** page, select two ports for which you want to set link alternation, and then click **Create Link Alternation**.
5. In the **Link Alternation Setup** page, select the default active port, and then click **OK**.
6. Click **OK**.
After setting the link alternation, modify the settings of the destination switch.



Note: From the **Add Interface** page of the **Network & System Configuration** dialog box, you must add interfaces for the ports for which link alternation is set.

Combining link aggregation and link alternation (cascaded trunking)

GUI used for this operation

- [physical-node window on page C-91](#)
- [Network & System Configuration dialog box on page C-178](#)

To combine link aggregation and link alternation

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the node to set the link aggregation and link alternation, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type:** *network*) of the **Network & System Configuration** dialog box, click **Trunking Setup**.
4. In the **List of Trunking Configurations** page, select the ports for which you want to set link aggregation, and then click **Create Link Aggregation**.
5. In the **Link Aggregation Setup** page, click **OK**.
6. Click **OK**.
7. In the **List of Trunking Configurations** page, select two ports for which you want to set link alternation, including a link aggregation port. Then, click **Create Link Alternation**.
8. In the **Link Alternation Setup** page, select the default active port, and then click **OK**.
9. Click **OK**.
After setting the cascaded trunking, modify the settings of the destination switch.



Note: If cascaded trunking is enabled for a port, always set up a tagged VLAN for that port in order to stabilize the communication between the client and the HDI system. For details about how to setup a VLAN, see [Setting up a VLAN on page 9-10](#).

Performing manual link alternation

GUI used for this operation

- [physical-node window on page C-91](#)
- [Network & System Configuration dialog box on page C-178](#)

To perform manual link alternation

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the node to alternate the link, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type:** *network*) of the **Network & System Configuration** dialog box, click **Trunking Setup**.
4. In the **List of Trunking Configurations** page, select a link alternation port, and then click **Change Active Port Status**.
5. Click **OK**.

Setting up a VLAN

To use a VLAN in an HDI system, a switch supporting an IEEE802.1Q tagged VLAN is required. When a VLAN is used, a virtual interface (a VLAN interface) is created for the data port. An identifier called a *VLAN ID* must be assigned to the VLAN interface.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Network & System Configuration dialog box on page C-178](#)

To set up a VLAN

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the node to set the VLAN, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type:** *network*) of the **Network & System Configuration** dialog box, click **Interface Management**.

4. In the **List of Interfaces** page, select the protocol version for which you want to set the information from the **Protocol version** drop-down list, and then click **Display**.
5. Click **Add**.
6. In the **Add Interface** page, select a port that uses VLAN, specify a VLAN ID from 1 to 4094, specify other information, and then click **OK**.
Hitachi Data Systems recommends that you specify the virtual IP addresses for both nodes to detect an error such as a link down in both nodes.
7. In the **System Setup Menu** page (**Setting Type:** `network`), click **Routing Setup**.
8. In the **List of Routings** page, select the protocol version for which you want to add the information from the **Protocol version** drop-down list, and then click **Display**.
9. Click **Add**.
10. In the **Add Routing** page, select the port and VLAN ID, specify other information, and then click **OK**.

Monitoring the system

This chapter describes how to use SNMPv2, v3, or email notifications to monitor the system.

If you use SNMPv2 or v3, the specifiable characters or settings that are described in this manual might be unusable depending on the SNMP manager. For details on the characters and settings that can be used for an SNMP manager, see the documentation of the SNMP manager.

- [Using SNMPv2](#)
- [Using SNMPv3](#)
- [Using error email notifications](#)

Using SNMPv2

This section explains how to use SNMPv2.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Network & System Configuration dialog box on page C-178](#)

To use SNMPv2

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type**: *network*) of the **Network & System Configuration** dialog box, select **System** from the **Setting Type** drop-down list, and then click **Display**.
4. In the **System Setup Menu** page (**Setting Type**: *system*) page, click **SNMP Setup**.
5. In the **List of SNMPs** page, click **Add**.
6. In the **Add SNMP** page, enter the required information, and then click **Add**.
7. In the **List of SNMPs** page, click **Back**.
8. In the **System Setup Menu** page (**Setting Type**: *system*) page, click **Edit System File**.
9. In the **Edit System File** page, from the **File type** drop-down list, select the `snmpd.conf` file, and then click **Display**.

10. To enable SNMP trap notification, append the following line to this file.

```
trap2sink SNMP-manager-host-name-or-IP-address [community-name
[port-number]]
```

Example: `trap2sink 10.213.76.194 stdDefComm1`

If you use IPv6, specify the host name or IP address and the port number of the SNMP manager as follows (The port number is required.):

```
udp6:host-name:port-number
```

```
udp6:[IP-address]:port-number
```

The default community name is `private`, and the default port number is 162.

11. Specify the server name of the SNMP manager that accesses MIBs.
By default, the settings are specified so that any network host can access MIBs. If you want to limit access, specify the name of the SNMP manager server that accesses MIBs. If you do not access MIBs, specify the local host.
If the protocol being used is IPv4, perform this task on the **List of SNMPs** page. To add the local host (`localhost`), temporarily delete all

entries, and then display the local host on the top of the **List of SNMPs** page.

If the protocol being used is IPv6, change the `source` setting of `com2sec6` in `Access Control` in the `snmpd.conf` file. If you removed the setting for `com2sec6` (for IPv6) or changed the setting into a comment by adding a hash mark (#) to the beginning of the line, `com2sec6` is reset to the default setting when you perform an update installation. Respecify the setting as necessary.

12. Click **OK**.
13. Confirm that the `cold start` trap is issued.
If the trap is not issued, verify the contents of the file. If you omit the community name for `trap2sink`, `public` is set for the community name of the `cold start` and `nsNotifyShutdown` traps that are issued when `snmpd` is started and stopped.
14. Repeat steps 2 to 13 for the other node in the cluster.



Tip: To stop error notifications, place a hash mark (#) at the beginning of each entry line in the `snmpd.conf` file.

Using SNMPv3

This section explains how to use SNMPv3.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Network & System Configuration dialog box on page C-178](#)

To use SNMPv3

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type:** `network`) page of the **Network & System Configuration** dialog box, select **System** from the **Setting Type** drop-down list, and then click **Display**.
4. In the **System Setup Menu** page (**Setting Type:** `system`) page, click **Edit System File**.
5. In the **Edit System File** page, from the **File type** drop-down list, select the `snmpd.conf` file, and then click **Display**.
6. Append the following two lines as SNMP management user information.

```
rouser user-name [security-level [OID]]
createUser user-name [authentication-type authentication-
password [encryption-type encryption-password]]
```

Example:

```
rouser user1 priv (rwuser can be specified instead of rouser.)
createUser user1 MD5 mypassphrase DES mypassword
```

7. To enable SNMP trap notification, append the following line to the file.

```
trapsess -v3 -u user-name [option] SNMP-manager-host-name-or-IP-
address[:port-number]
```

Example: trapsess -v3 -u user1 -l authPriv -a MD5 -A
mypassphrase -x DES -X mypassword 10.213.76.194

If you use IPv6, specify the host name or IP address and the port number of the SNMP manager as follows (The port number is required.):

```
udp6: host-name: port-number
```

```
udp6: [IP-address] : port-number
```

For details about the items to be specified when SNMPv3 is used, see [Table 10-1 Information specified in the snmpd.conf file when SNMPv3 is used on page 10-5](#).

Do not specify options that issue SNMPv2 traps usable by `net-snmp`.

8. Specify the server name of the SNMP manager that accesses MIBs.
By default, the settings are specified so that any network host can access MIBs. If you want to limit access, specify the name of the SNMP manager server that accesses MIBs. If you do not access MIBs, specify the local host.
If the protocol being used is IPv4, perform this task on the **List of SNMPs** page. To add the local host (`localhost`), temporarily delete all entries, and then display the local host on the top of the **List of SNMPs** page.
If the protocol being used is IPv6, change the `source` setting of `com2sec6` in `Access Control` in the `snmpd.conf` file. If you removed the setting for `com2sec6` (for IPv6) or changed the setting into a comment by adding a hash mark (`#`) to the beginning of the line, `com2sec6` is reset to the default setting when you perform an update installation. Respecify the setting as necessary.
9. Click **OK**.
10. Confirm that the `cold start trap` is issued after the `snmpd.conf` file is updated.
If the trap is not issued, verify the contents of the file.
11. Repeat steps 2 to 10 for the other node in the cluster.



Tip: To stop error notifications, place a hash mark (`#`) at the beginning of each entry line in the `snmpd.conf` file.

Table 10-1 Information specified in the snmpd.conf file when SNMPv3 is used

Configuration type	Configuration item	Description
rouser or rwuser#	User name	Specify a user name using no more than 32 characters. You can use the following ASCII characters: alphanumeric characters, hash mark (#), percent sign (%), hyphen (-), period (.), colon (:), equal sign (=), and underscore (_). A hash mark (#) cannot be used for the first character of a user name.
	Security level	Specify the security level for communication. noauth: Authentication is not used. auth: Authentication is used but encryption is not used. priv: Authentication and encryption are used. This item can be omitted.
	OID	When the security level is specified, specify the object ID that can be accessed by the user. This item can be omitted.
createUser	User name	Specify the user name that is used for SNMP communication. Use the user name specified for rouser or rwuser.
	Authentication type	If you specify auth or priv for the security level for rouser or rwuser, specify the type of user authentication. MD5: The HMAC-MD5-96 hash function is used. SHA: The HMAC-SHA1-96 hash function is used.
	Authentication password	When you specify an authentication type, specify an authentication password using at least 8 characters. You can use the following ASCII characters: alphanumeric characters, hash mark (#), percent sign (%), plus sign (+), hyphen (-), period (.), forward slash (/), colon (:), equal sign (=), at mark (@), and underscore (_). A hash mark (#) cannot be used for the first character of an authentication password.
	Encryption type	If you specify priv for the security level for rouser or rwuser, specify the encryption type for the common key. DES: CBC-DES is used. AES: CFB-AES-128 is used.
	Encryption password	When you specify an encryption type, specify a password required for encryption by using at least 8 characters.

Configuration type	Configuration item	Description
		<p>You can use the following ASCII characters: alphanumeric characters, hash mark (#), percent sign (%), plus sign (+), hyphen (-), period (.), forward slash (/), colon (:), equal sign (=), at mark (@), and underscore (_).</p> <p>A hash mark (#) cannot be used for the first character of a password for encryption.</p>
trapsess -v3	-u User name	Specify the user name that is used for trap notification. Use the user name specified for <code>rouser</code> or <code>rwuser</code> .
	-l Security level	<p>If you specify the security level for <code>rouser</code> or <code>rwuser</code>, specify the same security level here. However, the specified strings are different from the ones specified for <code>rouser</code> or <code>rwuser</code>.</p> <p><code>noAuthNoPriv</code>: Authentication is not used.</p> <p><code>authNoPriv</code>: Authentication is used but encryption is not used.</p> <p><code>authPriv</code>: Authentication and encryption are used.</p>
	-a Authentication type	If you specify the authentication type for <code>createUser</code> , specify the same authentication type (MD5 or SHA).
	-A Authentication password	Specify the authentication password that is specified for <code>createUser</code> .
	-x Encryption type	If you specify the encryption type for <code>createUser</code> , specify the same encryption type (DES or AES).
	-X Encryption password	Specify the password for encryption that is specified for <code>createUser</code> .
	Host name or IP address of the SNMP manager	Specify the host name or IP address of the SNMP manager to which trap notification is sent.
	Port number	<p>Specify the port number that is used for trap notification in the following format:</p> <p><i>SNMP-manager-host-name-or-IP-address:port-number</i></p> <p>You can skip this setting for SNMP manager using IPv4. If you skip this setting, the allocated port number is 162.</p> <p>You cannot skip this setting for SNMP manager using IPv6.</p>
<p>#: <code>rwuser</code> is the setting when reading and writing of a MIB object are permitted; however, HDI does not support writing to MIB objects.</p>		

Using error email notifications

This section explains how to use email for the notification of error information.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Network & System Configuration dialog box on page C-178](#)
- [List of RAS Information page on page C-164](#)

To use email notifications

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab.
3. In the **System Setup Menu** page (**Setting Type:** *network*) page of the **Network & System Configuration** dialog box, select **System** from the **Setting Type** drop-down list, and then click **Display**.
4. In the **System Setup Menu** page (**Setting Type:** *system*) page, click **Edit System File**.
5. In the **Edit System File** page, from the **File type** drop-down list, select the `email_alert.conf` file, and then click **Display**.
6. Append the mail server information and the recipient and sender email addresses to this file.
7. Click **OK**.
8. Confirm that the test email is received.

A test email is sent with the title `HDI Alert (node-host-name KAQM09112-I)`.

If you do not receive the test email within five minutes after clicking **OK** at the specified recipient email address, verify the following and take action as appropriate:

- The definitions in the `email_alert.conf` file are valid.
- The mail server settings are correct.
- The system message `KAQM09113-E` is not output to the **List of RAS Information** page (for `List of messages`).

Error information emails are sent with the title `HDI Alert (node-host-name message-ID)`.

9. Repeat steps 2 to 8 for the other node in the cluster.



Note: If you are unable to receive error email notifications after enabling them, verify the following and take action as appropriate:

- The system messages KAQM09113-E, KAQM09114-E, KAQM09115-E, KAQM09116-E, and KAQM09117-E are not output to the **List of RAS Information** page (for List of messages).
 - The definitions in the `email_alert.conf` file are valid.
 - The mail server settings have not changed.
-
-



Tip: To stop error notifications, place a hash mark (#) at the beginning of each entry line in the `email_alert.conf` file.

Controlling a node and OS

This chapter describes how to start and stop a node, and how to shut down and restart the OS on a node.

For details about how to control a node and OS by using commands, see the *CLI Administrator's Guide*.

- [Stopping or starting a node](#)
- [Shutting down and restarting the OS on a node](#)

Stopping or starting a node

This section describes how to start and stop a node.

Stopping a node

This section describes how to stop a node.

Before stopping a node

Stopping a node causes the resource group operating on that node to fail over to the other node. To prevent failover, before you stop a node, move operation of the resource group to the other node.

Do not stop and start a node repeatedly. If you perform these operations repeatedly, the KAQM06018-E message might be output when you stop the node. In this case, forcibly stop the node.

GUI used by this operation

- [physical-node window on page C-91](#)
- [Cluster Management dialog box on page C-268](#)

To stop a node

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the node that you want to stop.
3. Click **Cluster Management** in the **Advanced** subtab of the **Settings** tab.
4. In the **Browse Cluster Status** page (for `Cluster / Node status`) of the **Cluster Management** dialog box, check whether the **Node status** of the other node in the cluster is `UP`.
If the **Node status** of the other node is not `UP`, start the other node. For details about how to start a node, see [Starting a node on page 11-3](#).
5. In the **Browse Cluster Status** page, select **Resource group status** from the drop-down list, and then click **Display**.
6. In the **Browse Cluster Status** page (for `Resource group status`), confirm that **Resource group status** of the resource group running on the node to be stopped is `Online / No error` or `Online Maintenance / No error`.
7. Use a radio button to select the resource group that is running on the node to be stopped, and then click **Change Execution Node**.
The selected resource group moves (fails over) to the other node in the cluster. Movement might take 10 to 20 minutes or more, depending on the usage conditions of the node on which the resource group is currently running. (These conditions include the number of file systems, whether the volume manager is used, and the number of NFS shares.)

8. In the **Browse Cluster Status** page (for `Resource group status`), check **Resource group status** for any error information, and then confirm that the operation has been completed normally.
If error information is displayed, you need to perform recovery for failures that occurred during the operation. For details on how to fix failures, see the *Cluster Troubleshooting Guide*.
9. In the **Browse Cluster Status** page (for `Resource group status`), select **Cluster / Node Status** from the drop-down list, and then click **Display**.
10. In the **Browse Cluster Status** page (for `Cluster / Node status`) of the **Cluster Management** dialog box, click **Stop** for the node.
Stop and **Perform Forced Stop** are displayed if the node is running.



Tip: If a failure occurs (preventing you from continuing processing) before you stop the node, you can forcibly stop the node.

When you click **Perform Forced Stop** for a node, the system ignores any errors that occurred during processing, performs a forced stop for the node, and begins failover for the resource group active on the node.

Some services might remain running after a forced stop 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 might start. Therefore, after performing a forced stop for a cluster, reboot the OS on both nodes before starting the cluster. Also, if the resource group has not been moved to the other node when one node is forcibly stopped, reboot the OS before you start the node.

-
11. In the **Browse Cluster Status** page (for `Cluster / Node status`), check **Node status** for any error information, and then confirm that the operation has been completed normally.
If error information is displayed, you need to perform recovery for failures that occurred during the operation. For details on how to fix failures, see the *Cluster Troubleshooting Guide*.

Starting a node

This section describes how to start a node.

Before starting the node

When a node is started while a resource group is in the `Online Ready/No error` status, the resource group is automatically started. After processing finishes, it might take a while before you can perform resource group related operations (until the `Online/No error` status is reached).

The system administrator needs to make sure that no partial blockage has occurred in a resource group during the resource group startup process. On the **List of RAS Information** page (for `List of messages`) of the **Check for Errors** dialog box, check whether the message KAQG72006-E or

KAQM35001-E has been output to the system messages. For the action to take if the message has been output, see the *Error Codes* manual.

Do not stop and start a node repeatedly. If you perform these operations repeatedly, the KAQM06018-E message might be output when you stop the node.

GUI used by this operation

- [physical-node window on page C-91](#)
- [Cluster Management dialog box on page C-268](#)

To start a node

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the node that you want to start.
3. Click **Cluster Management** in the **Advanced** subtab of the **Settings** tab.
4. In the **Browse Cluster Status** page (for `Cluster / Node status`) of the **Cluster Management** dialog box, click **Start** for the node.
Start is displayed if the node is not running.
If you click **Start**, the node starts, and makes the resource group available for starting.
5. In the **Browse Cluster Status** page (for `Cluster / Node status`), check **Node status** for any error information, and then confirm that the operation has been completed normally.
If error information is displayed, you need to perform recovery for failures that occurred during the operation. For details on how to fix failures, see the *Cluster Troubleshooting Guide*.
6. If the resource group have been moved to the other node in the cluster as a result of a failover, fail them back to the node that you started.
For details about how to move a resource group between nodes in the cluster, see steps 4 to 8 in [Stopping a node on page 11-2](#).

Shutting down and restarting the OS on a node

This section describes how to shut down and restart the OS on a node.

Shutting down the OS on a node

This section describes how to shut down the OS on a node.

Before shutting down the OS on a node

Before the OS is shut down, the node must be stopped. In the **Browse Cluster Status** page (for `Cluster / Node status`) of the **Cluster Management** dialog box, verify that the node at which the OS is to be shut

down is inactive. For details about how to stop the node, see [Stopping a node on page 11-2](#).



Tip:

- To start the OS, press the power switch on the node chassis.
 - For details about how to shut down both OSs on the processing node at the same time, see [Shutting down the OSs on both nodes on page 11-6](#).
-

GUI used by this operation

- [physical-node window on page C-91](#)
- [Cluster Management dialog box on page C-268](#)

To shut down the OS on a node

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the OS that you want to shut down.
3. Click **Cluster Management** in the **Advanced** subtab of the **Settings** tab.
4. In the **Browse Cluster Status** page (for `Cluster / Node status`) of the **Cluster Management** dialog box, click **Shutdown**.
5. When the dialog box notifying you that the OS was shut down appears, click **OK**.
6. Click **Close**.

Restarting the OS on a node

This section describes how to restart the OS on a node.

Normally, the system administrator needs to reboot the OS for the following operations:

- Setting new information for the LDAP server for user authentication, or deleting all information for the LDAP server for user authentication
- Setting, changing, or deleting information for the NIS server
- Setting or changing the NTP server or the time zone
- Changing the node time

If the OS needs to be rebooted for any other reason, contact maintenance personnel first.

Before restarting the OS on a node

Before the OS is rebooted, the node must be stopped. In the **Browse Cluster Status** page (for `Cluster / Node status`) of the **Cluster Management** dialog box, verify that the node at which the OS is to be

rebooted is inactive. For details about how to stop the node, see [Stopping a node on page 11-2](#).

If you are using encryption, note that if system settings are saved in the HCP system, before you restart the OS, make sure the HCP system is normally operating and that the HDI and HCP systems can communicate normally.

If the host name specified for the routing target or gateway cannot be resolved, the routing information might not be restored after rebooting the OS. If a host name is specified for the routing target or gateway, make sure that the host name can be resolved before rebooting the OS. If the routing information cannot be restored, see the *Cluster Troubleshooting Guide*, and take appropriate action.

GUI used by this operation

- [physical-node window on page C-91](#)
- [Cluster Management dialog box on page C-268](#)

To restart the OS on a node

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the node on which you want to restart the OS.
3. Click **Cluster Management** in the **Advanced** subtab of the **Settings** tab.
4. In the **Browse Cluster Status** page (for `Cluster / Node status`) of the **Cluster Management** dialog box, click **Reboot**.
5. Select **Start the node after a reboot** or **Do not start the node after a reboot**.
If you select **Start the node after a reboot**, specify whether you start the resource group (and fail back if the resource group is failed over).
6. Click **Reboot**.
7. When the dialog box notifying you that the OS was restarted appears, click **OK**.
8. Click **Close**.
9. If you selected **Do not start the node after a reboot** in step 5, restart the OS, and then wait about five minutes. In the **Cluster Management** dialog box, display the **Browse Cluster Status** page, start the node, and then perform a failback of the resource group.
10. If you selected **Start the node after a reboot** in step 5, and specified not to perform a failback of the resource group after the node is started, in the **Cluster Management** dialog box, display the **Browse Cluster Status** page, and then perform a failback of the resource group.

Shutting down the OSs on both nodes

This section describes how to stop a processing node and both OSs at the same time.

The system administrator can stop a processing node when stopping the HDI system through a planned outage. When a processing node is stopped in this manner, both OSs are forcibly stopped and the nodes are powered off, regardless of service activity and any I/O operations being performed on the file system.

GUI used by this operation

- [Processing Nodes window on page C-78](#)

To shut down the OSs on both nodes at the same time

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the Processing Nodes window, open the **File Servers** tab. Then, select the check box of the processing node that you want to stop, and then click **Shutdown Node**.
3. Verify the information shown in the confirmation dialog box, select the check box, and then click **Confirm**.
4. Verify that the processing results are correct, and then click **Close**.

Starting the OSs of both nodes at the same time

This section describes how to start a processing node to start both OSs at the same time.

Before starting the OSs of both nodes

Starts a processing node in an environment where the management server can communicate with the BMC of the processing node by way of IPv4.

If you are using encryption, and the system settings are saved to the HCP system, confirm that the HCP system is operating normally and that the HDI and HCP systems can communicate normally, before starting a processing node.

GUI used by this operation

- [Processing Nodes window on page C-78](#)

To start the OSs on both nodes at the same time

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the Processing Nodes window, open the **File Servers** tab. Then, select the check box of the processing node that you want to start, and then click **Start Node**.
3. Verify the information shown in the confirmation dialog box, and then click **Confirm**.
4. Verify that the processing results are correct, and then click **Close**.

Changing the connection between nodes and storage systems

This chapter describes how to change the connection between nodes and storage systems.

- [Changing the ports assigned to an LU](#)
- [Reconfiguring an LU path](#)
- [Reconfiguring an FC path](#)
- [Replacing FC switches](#)
- [Connecting an additional storage system](#)
- [Detaching a storage system](#)

Changing the ports assigned to an LU

If access performance from CIFS or NFS clients deteriorates (even though the CPU usage of the node is low), it might be because the processing load is concentrated on a particular port on the storage system. In such situations, re-assigning the LUs making up the file system to a different port might improve performance.

The following figure provides a conceptual image of changing storage system ports assigned to an LU.

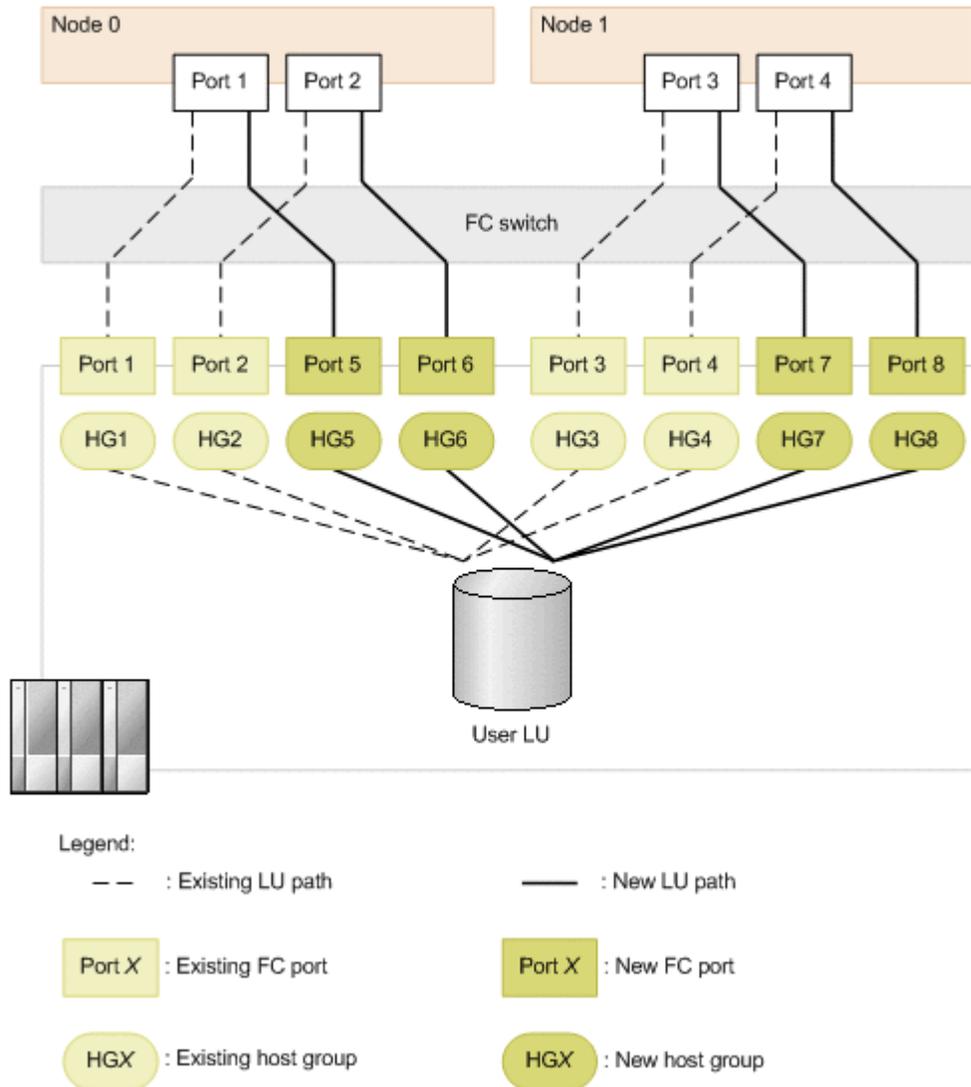


Figure 12-1 Conceptual image of changing the ports assigned to an LU

This section describes how to change ports assigned to an LU on the condition that Fibre Channel cards have been added on nodes and host groups have been added in the storage system.

The procedure to change storage system ports might differ depending on whether to add an FC path when changing ports. The system administrator,

working with the SAN administrator and maintenance personnel, must perform the following procedure.

GUI used by this operation

- [Cluster Management dialog box on page C-268](#)

To change the port assignments

1. Verify the assignment settings for the target LU.
Identify the LDEV number assigned to the LU.
For details about how to view LDEV numbers and assignment settings for user LUNs, see the *CLI Administrator's Guide*.
2. Manually fail over the resource group operating on the node.
3. Stop the failover-source node.
4. If you want to add an FC path, ask the SAN administrator to set up the hardware and the SAN.
5. Ask the SAN administrator to delete the existing LU path from the stopped node, and to add LUs to the host group after the change.
6. Reboot the OS on the stopped (failover-source) node.
7. Start the failover-source node.
8. Fail back the resource group to the original node.
9. Repeat steps 2 to 8 for the other node in the cluster.

Reconfiguring an LU path

The system administrator can add, delete, or change an LU path. The system administrator performs these operations by working with the SAN administrator. Before any of these operations are performed, setup or reconfiguration of the FC path must be completed.



Note: Observe the following note.

- Do not change or delete the LU path for the command device unless you added, deleted, or changed the path by mistake. If you add or change the LU path for the command device, you must restart the OS afterwards. You can use Hitachi Storage Navigator Modular 2 or Storage Navigator to verify the command device information.
 - Before adding, deleting, or changing an LU path, make sure that the mapping guard for the system LU is enabled to avoid an error in system LUs that is caused by improper mapping operations. If the mapping guard is not enabled for the system LUs, enable the guard. The mapping guard can be set up from Hitachi Storage Navigator Modular 2 or Storage Navigator. Make sure that the version of Hitachi Storage Navigator Modular 2 that you use is 6.5 or later.
-

Adding an LU path

GUI used by this operation

- [processing-node window on page C-86](#)
- [physical-node window on page C-91](#)

To add an LU path

1. Ask the SAN administrator to add the LU path.
2. Refresh the processing node.
3. Make sure that the target LU is shown correctly.

If the target LU is not shown in the **LU**s tab in the *physical-node-name* window, you might have added the LU path for the command device by mistake. In this case, delete the LU path for the command device, and then perform the procedure to add an LU path again.

Deleting an LU path

GUI used by this operation

- [physical-node window on page C-91](#)
- [processing-node window on page C-86](#)

To delete an LU path

1. Stop the use of the target LU if it is being used.
If a file system is using the target LU, delete the file system.
2. Ask the SAN administrator to delete the LU path.
3. Refresh the processing node.
If you want to use a command, run the `fpstatus` command on both of the nodes, instead of refreshing the processing node.

4. Make sure that the target LU has been deleted correctly.
If the target LU is shown in the **LU**s tab in the *physical-node-name* window, you might have deleted the LU path for the command device by mistake. In this case, add the LU path for the command device, and then perform the procedure to delete an LU path again.

If the GUI is refreshed or the `fpstatus` command is run after the LU path is deleted, the `KAQK40000-E` message or the `KAQK40001-E` message might be output as a system message. If the FC path status is `Online`, ignore the output message.

Changing an LU path

GUI used by this operation

- [physical-node window on page C-91](#)
- [processing-node window on page C-86](#)

To change an LU path

1. Stop the use of the target LU if it is being used.
If a file system is using the target LU, delete the file system.
2. Ask the SAN administrator to change the LU path.
3. Refresh the processing node.
If you want to use a command, run the `fpstatus` command on both of the nodes, instead of refreshing the processing node.
4. Make sure that the target LU is shown correctly.
If the target LU is not shown in the **LU**s tab in the *physical-node-name* window, you might have changed the LU path for the command device by mistake. In this case, delete the LU path for the command device, and then perform the procedure to change an LU path again.

If the GUI is refreshed or the `fpstatus` command is run after the LU path is changed, the `KAQK40000-E` message or the `KAQK40001-E` message might be output as a system message. If the FC path status is `Online`, ignore the output message.

Reconfiguring an FC path

By working with the SAN administrator and maintenance personnel, you can reconfigure an FC path between a node and a storage system.

Stop the NDMP server before changing the FC switches or zoning. After configuring FC switches, start the NDMP server, and then enable the backup management software to use the tape drive.

Adding an FC path

GUI used by this operation

- [processing-node window on page C-86](#)
- [Health Monitor window on page C-137](#)
- [physical-node window on page C-91](#)

To add an FC path

1. Ask the SAN administrator to set up the hardware and the SAN.
2. Refresh the processing node.

3. Verify the FC path configuration after the change.
For the reconfigured node, verify the following items in the **FC Path** subtab in the Health Monitor window, and then make sure that the target FC path has been correctly added:
 - Model of the storage system
 - Serial number of the storage system
 - FC ports on the node
 - FC ports on the storage systemIn addition, verify the following items in the **LUs** tab in the *physical-node-name* window, and then make sure that the LUs for the added FC path are correct:
 - Model of the storage system
 - Serial number of the storage system
 - LDEV number
4. Repeat steps 1 to 3 for the other node in the cluster.

Changing or deleting an FC path

GUI used by this operation

- [Cluster Management dialog box on page C-268](#)
- [processing-node window on page C-86](#)
- [Health Monitor window on page C-137](#)
- [physical-node window on page C-91](#)

To change or delete an FC path

1. Manually fail over the resource group operating on the node.
2. Stop the failover-source node.
3. Ask the SAN administrator to set up the hardware and the SAN.
4. Reboot the OS on the stopped (failover-source) node.
5. Refresh the processing node.
6. Verify the FC path configuration after the change.
For the reconfigured node, verify the following items in the **FC Path** subtab in the Health Monitor window, and then make sure that the target FC path is correctly changed or is not shown:
 - Model of the storage system
 - Serial number of the storage system
 - FC ports on the node
 - FC ports on the storage system

In addition, verify the following items in the **LU**s tab in the *physical-node-name* window, and then make sure that the LUs for the changed FC path are correct, or the LUs for the deleted FC path are not shown:

- o Model of the storage system
 - o Serial number of the storage system
 - o LDEV number
7. Start the failover-source node.
 8. Fail back the resource group to the original node.
 9. Repeat steps 1 to 8 for the other node in the cluster.

Replacing FC switches

By working with the SAN administrator and maintenance personnel, you can replace FC switches between a node and a storage system.



Note: Do not change an LU configuration that is in a storage system in which FC paths are in the *Offline* status.

To replace FC switches

1. Use the `fpstatus` command to view the statuses of the FC paths connected to the target FC switch.
2. Use the `fpoffline` command to place all the FC paths connected to the target FC switch *Offline*.
3. Repeat steps 1 to 2 for the other node in the cluster.
4. Ask the SAN administrator to replace the FC switch.
5. Use the `fponline` command to place the FC paths that were placed *Offline* in step 2 back *Online*.
6. Verify the statuses of the FC paths connected to the target FC switch. Verify that the FC paths are in the *Online* status.

Connecting an additional storage system

To connect an additional storage system while the HDI system is in operation, you need to reconfigure the FC paths. By working with the SAN administrator and maintenance personnel, you can connect an additional storage system.

Before connecting an additional storage system

Before connecting an additional storage system, the system administrator must design the SAN in terms of how to connect the additional storage system to the node via Fibre Channel. To determine the design, you can create a table like the following.

Table 12-1 Sample notes on SAN design

Zone of FC switch	Port on node	Port on additional storage system
zone1	Node0-fc0	0A
zone2	Node1-fc0	0B
zone3	Node0-fc2	1A
zone4	Node1-fc2	1B
zone5	--	N/A
zone6	--	N/A
zone7	--	N/A
zone8	--	N/A

Note: N/A = Not applicable.

Connecting an additional storage system

GUI used by this operation

- [processing-node window on page C-86](#)
- [Health Monitor window on page C-137](#)
- [physical-node window on page C-91](#)

To connect a storage system to nodes

1. Set the host groups for the storage system ports.
2. Ask the SAN administrator to set up the hardware and the SAN according to the predetermined SAN design.
For details about what to consider for SAN design, see [Before connecting an additional storage system on page 12-7](#).
After you finish setting up the hardware or SAN, use an FC cable to connect the storage system to the node.
3. Refresh the processing node.
4. Make sure that the FC paths are correctly set up.
For the reconfigured node, verify the following items in the **FC Paths** subtab in the **Network** tab of the Health Monitor window, and then make sure that the relevant FC paths are correctly added:
 - Model of the storage system
 - Serial number of the storage system
 - FC ports on the node
 - FC ports on the storage system

In addition, verify the following items in the **LU**s tab in the *physical-node-name* window, and then make sure that the LUs for the added FC paths are correct:

- Serial number of the storage system
- LDEV number

5. Repeat steps 2 to 4 for the other node in the cluster.

Notes:

If you use an FC cable to connect the node to the storage system before specifying a host group for the storage system port, you will be unable to use the LU on the added storage system. In this case, perform one of the following actions:

- Disconnect and then reconnect the FC cable that connects the node and the storage system.
- Disable and then re-enable the port connected to the storage system on the FC switch located between the node and the storage system.
- Restart the node.

Detaching a storage system

To detach a storage system managed by nodes while the HDI system is in operation, you need to reconfigure the FC paths. By working with the SAN administrator and maintenance personnel, you can detach a storage system.

GUI used by this operation

- [Cluster Management dialog box on page C-268](#)
- [processing-node window on page C-86](#)
- [Health Monitor window on page C-137](#)
- [physical-node window on page C-91](#)

To detach a storage system from the nodes

1. Make sure that the LUs in the target storage system are not being used by the HDI system.
2. Manually fail over the resource group operating on the node.
3. Stop the failover-source node.
4. Ask the SAN administrator to set up the hardware and the SAN.
5. Reboot the OS on the stopped node (failover-source).
6. Refresh the processing node.
7. Verify the FC path configuration after the change.

For the reconfigured node, verify the following items in the **FC Paths** subtab in the **Network** tab of the Health Monitor window, and then make sure that the relevant FC paths are not shown:

- o Model of the storage system
- o Serial number of the storage system
- o FC ports on the node
- o FC ports on the storage system

In addition, verify the following items in the **LUs** tab in the *physical-node-name* window, and then make sure that the LUs for the deleted FC paths are not shown:

- o Serial number of the storage system
 - o LDEV number
8. Start the failover-source node.
 9. Fail back the resource group to the original node.
 10. Repeat steps 1 to 9 for the other node in the cluster.

Setting up an environment for command and GUI operations

This chapter describes how to set up an environment for command and GUI operations.

- [Setting up the SSH environment to use commands](#)
- [Setting up a public key certificate](#)

Setting up the SSH environment to use commands

This section explains how to register a public key to use commands.

Prerequisites for registering a public key

SSH2 is supported in HDI systems. Use a key creation tool to create the private key and public key that are used in the SSH authentication. Create the public key in OpenSSH format. For details about 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 log on password. You can omit a passphrase.

Store the public key in the computer where you can use the Hitachi File Services Manager GUI.

GUI used for this operation

- [physical-node window on page C-91](#)
- [Access Protocol Configuration dialog box on page C-217](#)

To register a public key to use commands

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Access Protocol Configuration** in the **Advanced** subtab of **Settings** tab.
3. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **SSH**, and then click **Modify Configuration**.
4. In the **Public Key List** page, click **Add**.
5. In the **Add Public Key** page, specify the public key file, and then click **Add**.

The public key is registered for the SSH account `nasroot`.

For details about how to use commands, see the *CLI Administrator's Guide*.

6. Repeat steps 2 to 5 for the other node in the cluster.

Setting up a public key certificate

This section describes how to set up a public key certificate issued by a certification authority (CA) for a node.

A self-signed certificate has been set up in the node using the default setting because communication between a node and GUI is based on SSL. To use a public key certificate issued by a certificate authority, obtain a certificate from a certificate authority and set the certificate up for a node.

Public key certificates and intermediate certificate authority certificates can be set for nodes. Cross certificates cannot be applied.

The execution of commands is required for this operation. See [Setting up the SSH environment to use commands on page 13-2](#) to set up a proper environment. For details about how to use commands, see the *CLI Administrator's Guide*.

To set up a public key certificate issued by a certificate authority for a node

1. Execute the `certctl` command by using the `--create-cert` option to create a certificate signing request (CSR) and private key.

```
certctl --create-cert --dest-key private-key-file-name --dest-csr CSR-file-name --key-passwd private-key-password [--country country-name] [--state-province state-or-province-name] [--locality locality-name] [--organization company-or-organization-name] [--unit organization-or-department-unit-name] [--common-name host-name-of-node] [--email E-mail-address] [--challenge-passwd challenge-password] [--optional-company other-company-or-organization-name]
```

The certificate signing request and private key file will be output to the SSH account home directory (`/home/nasroot`).

2. Use the `scp` command or any other method to transfer the CSR file to the local disk of the management console or any other appropriate location.
3. Send the certificate signing request to a certificate authority to obtain a public key certificate.
4. Use the `scp` command or any other method to transfer the public key certificate file obtained from the certificate authority to the HDI. Transfer the file to the home directory for the SSH account (`/home/nasroot`).
5. Execute the `certctl` command by using the `--create-pkcs` option to create a keystore in PKCS #12 format.

```
certctl --create-pkcs --key private-key-file-name --cert public-key-certificate-file-name [--intermediate-cert intermediate-certificate-authority-certificate-file-name] --dest-keystore keystore-file-name --passwd keystore-password --key-passwd private-key-password
```

The keystore file in PKCS #12 format will be output to the SSH account home directory (`/home/nasroot`).

6. Use the `scp` command or any other method to transfer the keystore file in PKCS #12 format to the local disk of a machine that has Oracle JDK 6 or later installed.
7. Import the keystore in PKCS #12 format to a keystore in JKS format. To do this, the machine you are using must have Oracle JDK6 or later installed.

Here is an example of creating a keystore file on a Windows machine.

```
keytool.exe -alias certificate -importkeystore -srckeystore path-of-keystore-in-PKCS-#12-format -destkeystore path-of-keystore-in-JKS-format -
```

```
srcstoretype pkcs12 -deststoretype jks -destalias alias-name-of-your-choice -destkeypass changeit
```

If you are prompted to enter the password for the destination keystore, enter the `changeit`. If you are prompted to enter a password for the source keystore, enter the password that you specified when you created the keystore in PKCS #12 format.

8. Use the `scp` command or any other method to transfer the keystore file in JKS format to the HDI.

Transfer the file to the home directory for the SSH account (`/home/nasroot`).

9. Execute the `certctl` command by using the `--set-cert` option to set up the following for the node: the certificate obtained from the certificate authority, the created private key, and the keystore in JKS format.

```
certctl --set-cert --key private-key-file-name --cert public-key-certificate-file-name [--intermediate-cert intermediate-certificate-authority-certificate-file-name] --keystore keystore-file-name --key-passwd private-key-password [-y]
```

10. Repeat steps 1 to 9 for the other node in the cluster.
11. Use the `scp` command or any other method to transfer the certificate file obtained from the certificate authority to the local disk of the management server.
12. Execute the following command to import the certificate obtained from a certificate authority to the keystore of the management server.

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmdskeytool -import -trustcacerts -alias alias-name-of-your-choice -file path-of-certificate-obtained-from-CA -keystore Hitachi-Command-Suite-Common-Component-installation-folder\jdk\jre\lib\security\jssecacerts
```

After executing the command, you will be prompted to enter the password. Enter the keystore password for the management server.

If you have also obtained an intermediate CA certificate from a certificate authority, also execute the command to import the intermediate CA certificate.

13. Stop and then restart Hitachi File Services Manager and Hitachi Command Suite Common Component.

For details on how to stop and start Hitachi File Services Manager and Hitachi Command Suite Common Component, see the *Installation and Configuration Guide*.



Tip: To initialize the setting of a public key certificate set up in a node, execute the `certctl` command by using the `--reset` option.

Performing an update installation

This chapter describes how to perform an update installation for software.

Note that the software version of Hitachi File Services Manager and the nodes might be different. Hitachi File Services Manager can manage nodes whose software version is the same as or earlier than the version of Hitachi File Services Manager. For example, if the Hitachi File Services Manager version is 4.2.0-xx, nodes whose software version is 4.2.0-xx or earlier can be managed (xx indicates that the version is not dependent on the version number after the hyphen (-)). To update the software of nodes, check the version of Hitachi File Services Manager in advance. If Hitachi File Services Manager needs to be upgraded, upgrade Hitachi File Services Manager first, and then update the software on the nodes.

- [Performing an upgrade or overwrite installation of Hitachi File Services Manager](#)
- [Updating software](#)

Performing an upgrade or overwrite installation of Hitachi File Services Manager

This section describes how to perform an upgrade or overwrite installation of Hitachi File Services Manager on the management server that is not in cluster configuration.

Before updating the software version on the nodes, be sure to perform an upgrade installation of Hitachi File Services Manager.

If Hitachi File Services Manager configuration files have become corrupted due to a failure or a mistake by the system administrator, you can restore the files by installing the same version of Hitachi File Services Manager as an overwrite installation.



Note: You cannot perform an overwrite installation of Hitachi File Services Manager whose version is older than the version of Hitachi File Services Manager currently installed on the management server. If you want to use an older version of Hitachi File Services Manager, uninstall the currently installed Hitachi File Services Manager, and then install the older version as a new installation.

To perform an upgrade or overwrite installation of Hitachi File Services Manager

1. Insert the installation media for Hitachi File Services Manager, and then run `HFSMinst.exe` in the media.
2. Read the terms, and then click **Yes**.
The Welcome to the **Installation of Hitachi File Services Manager (Upgrade)** dialog box or the **Welcome to the Installation of Hitachi File Services Manager (Overwrite)** dialog box appears. The following shows an example of the dialog box displayed when an overwrite installation is performed.



Note: When you click **Next**, the installer stops the services of Hitachi Command Suite Common Component and other Hitachi Command Suite products.

3. Verify the information displayed in the dialog box, and then click **Next**.
The **Confirmation of the Setup Status of the Hitachi Command Suite Common Component Database** dialog box appears.
This dialog box indicates how the installed Hitachi Command Suite products have been configured.
4. Verify the configuration, and then click **Next**.
The **Confirmation Before Installation** dialog box is shown.
If the management server does not contain the Hitachi File Services Manager database, the **Specify the Storage Destination for Database Files of Hitachi File Services Manager** dialog box appears before the **Confirmation Before Installation** dialog box. If this dialog box appears, specify the database file storage folder, and then click **Next** to continue installation.

Specify the folder for storing database files based on the following rules:

- Specify an absolute path, using no more than 90 bytes.
 - For the path, you can use alphanumeric characters, left parentheses ((), right parentheses ()), periods (.), underscores (_), and space characters. However, you cannot specify a period (.) at the beginning or end of the path. Also, you cannot specify a space character at the beginning or end of the path, nor can you specify consecutive space characters.
 - You can use backslashes (\) as path delimiters. However, the path cannot end with a backslash.
5. Verify that the specified information is correct, and then click the **Install**. Installation starts and a series of dialog boxes indicating the processing status appear. If the installation is successful, the **Installation Complete** dialog box appears.

If an upgrade or overwrite installation is performed, the existing Hitachi File Services Manager database is not initialized.

If an upgrade installation is performed when a communication error exists between the management server and the node, the database cache information on the management server and the information on the node might not match. If a mismatch occurs, eliminate the communication error, and then perform refresh processing.



Note: If the password for the management server keystore file (`jssecacerts`) has been set, an error dialog box appears before the **Installation Complete** dialog box is displayed. Verify the information displayed in the dialog box, and then click **OK**. After the installation is complete, import the SSL certificate to the management server. For details on how to import the SSL certificate to the management server, see the *Installation and Configuration Guide*.

6. Click **Finish** to complete the installation.

Updating software

This section describes how to perform an update installation for the software that runs on a node from the management console.

When updating the software, perform the operation from the management console located on the management LAN.

Ensure that at least 2 GB of free space is available on the management server where Hitachi File Services Manager is to be installed. The versions of the software products installed on the nodes in a cluster must be the same. A system administrator must keep the versions of installed software products consistent across the nodes in the same cluster. Before updating the software on nodes, be sure to check the version of Hitachi File Services Manager, and then upgrade Hitachi File Services Manager in advance if necessary. For details about how to upgrade Hitachi File Services Manager, see [Performing an upgrade or overwrite installation of Hitachi File Services Manager on page 14-2](#).

You can install software when the status of the nodes and resource groups is as follows:

When installing software on both nodes:

- The statuses of the nodes are either both `UP` or both `INACTIVE`.
- The statuses of the resource groups on both nodes are either `Online` or `Offline`. The statuses of the resource groups do not need to be the same.

When installing software on only one of the nodes:

- The statuses of the nodes are `UP`, or the status of the node on which you want to install the software is `INACTIVE`.
- The statuses of the resource groups on the nodes are either `Online` or `Offline`. The statuses of the resource groups do not need to be the same.

If you install the software from installation media, place the installation media in the management console's optical drive in advance.

Note the following points during a software update:

- Do not use the GUI or a command to execute other operations.
- If periodic saving of system configuration information is performed, the processing might end with an error. Therefore, review the start time of the processing beforehand so that the processing is not performed during a software update.

Updating the software on a node

This section describes how to update the software on a node.

GUI used for this operation

- [physical-node window on page C-91](#)
- [System Software window on page C-147](#)
- [System Software Installation Wizard on page C-148](#)
- [Backup Configuration dialog box on page C-171](#)

To update the software on a node

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node, and in the window that is shown, click **Software Update** in the **Basic** subtab of **Settings** tab.
3. In the System Software window, click **Update Software**.
4. Verify the contents displayed in the **1. Introduction** page of the System Software Installation Wizard, and then click **Next >**.

5. In the **2. Create a backup of the system settings** page, save the system configuration information, select the check box, and then click **Next >**.
Clicking **Backup Configuration** displays the **Save System Settings Menu** page in the **Backup Configuration** dialog box. Save the system configuration information.
6. On the **3. Select the installation source** page, specify an installation file, and then click **Next >**.
If you want to specify an installation file on the management console, select the **Install from a local file** option, and then specify the `install_files.tar.gz` file on the installation media. If you want to specify a file name by browsing through the files, click **Browse**.
If you want to use an installation file that has already been transferred to a node, confirm the displayed product information, and then select the **Install from the transferred file** option.
If you specified an installation file on the management console, click **Next >** to start transferring the file to a node. After the file is transferred, go to the next step.
7. In the **4. Select the installation destination** page, select the target physical node as the installation destination, and then click **Next >**.
If you install the software on both physical nodes, select the **Both physical nodes** option. If you install the software on only one of the physical nodes, select the **Only on *target-physical-node-name*** option for that node.
8. In the **5. Select the installation method** page, specify an installation method, and then click **Next >**.
To perform all the installation steps together, select the **Automatically perform all installation steps** check box. If you do not select this check box, you have to manually start the next step after each step is completed.
9. Confirm the information displayed in the **6. Confirm** page, select the check box, and then click **Confirm**.
The **7. Installation** page is displayed and installation processing starts. If you are performing a manual installation, after each step is completed, click **Start Next Step** to start the next step.
You can change the installation method during installation. While you are performing an automatic installation, if you click **Change Installation Method**, the installation method is changed to a manual installation. While you are performing a manual installation, after the current step is completed, if you select the **Automatically perform the remaining installation steps.** check box, and then click **Start Next Step**, the installation method is changed to an automatic installation.
10. In the **8. Finish** page, verify that the processing results are correct, and then click **Close**.

If you set up linking with an HCP system for a version earlier than 3.2.0-00 and then updated the software, you must configure the settings so that HCP tenants can be managed from Hitachi File Services Manager. Perform the

setup according to [When the software is updated after setting up linking with an HCP system for a version earlier than 3.2.0-00 on page 14-6](#).

When the software is updated after setting up linking with an HCP system for a version earlier than 3.2.0-00

This section describes the necessary procedure when the node software is updated after setting up linking with HCP for a version earlier than 3.2.0-00.

You must change settings in either of the following ways so that you can manage HCP tenants from Hitachi File Services Manager:

- Creating a user account with the same name as the data access account (see [Creating a user account with the same name as the data access account on page 14-6](#))
- Setting up a user account for a tenant administrator in Hitachi File Services Manager (see [Setting up a user account for a tenant administrator in Hitachi File Services Manager on page 14-7](#))



Note: Hitachi Data Systems recommends that you use the first method because the second method temporarily stops the HDI service.

You can use HCP Tenant Management Console and Hitachi File Services Manager to perform the setup. For details about how to use Tenant Management Console, see the HCP manuals.

Creating a user account with the same name as the data access account

Create a tenant administrator user account with the same name as the data access account set in the HDI system, and then verify the connection with HCP.

GUI used for this operation

- [processing-node window on page C-86](#)
- [Configuration Wizard on page C-317](#)

To create a tenant administrator user account with the same name as the data access account, and then verify the connection with HCP

1. Use the user name and password for the tenant administrator user account to log on to HCP Tenant Management Console.
2. Create a tenant administrator user account with the same name as the data access account set in the HDI system.
Specify the following settings:
 - Give the roles `Monitor`, `Administrator`, `Compliance`, and `Security` to the created tenant administrator user account.
 - Enable the HCP management API (MAPI) for the tenant.

3. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
4. In the object tree, select the processing node, and in the window that is shown, click **Reconfigure Processing Node**.
5. In the Configuration Wizard, specify the necessary information.
In the **6. Optional settings** page, select **Custom settings**, and then specify **HCP settings**.
6. In the **6-3. HCP settings** page, click **Test Connection**.
If you verify the connection with HCP, the procedure is complete. Cancel the rest of the steps in the Configuration Wizard. If the connection test fails, take action according to the message.

Setting up a user account for a tenant administrator in Hitachi File Services Manager

If you cannot create a tenant administrator user account with the same name as the data access account, create a new tenant administrator user account, and then set up the created user account in Hitachi File Services Manager.

GUI used for this operation

- [processing-node window on page C-86](#)
- [Configuration Wizard on page C-317](#)

To create a new tenant administrator user account, and then set up the created user account in Hitachi File Services Manager

1. Use the user name and password for the tenant administrator user account to log on to HCP Tenant Management Console.
2. Create a tenant administrator user account.
You can use any user name and password. Specify the following settings:
 - Give the roles *Monitor, Administrator, Compliance, and Security* to the created tenant administrator user account.
 - Enable the HCP management API (MAPI) for the tenant.
3. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
4. In the object tree, select the processing node, and in the window that is shown, click **Reconfigure Processing Node**.
5. In the Configuration Wizard, specify the necessary information.
In the **6. Optional settings** page, select **Custom settings**, and then specify **HCP settings**.
6. In the **6-3. HCP settings** page, specify the user account information for the created tenant administrator, and then click **Test Connection**.
If the connection test fails, take action according to the message.
7. Verify the information that is shown in the **7. Confirmation** page, and then click **Confirm**.

The **9. Completion** page is shown when the setup finishes.



A

Operations provided by the GUI

This appendix describes the GUI operations.

- [GUI operations](#)

GUI operations

The following table lists the operations that can be performed by using the GUI.

Table A-1 Operations provided by the GUI

Operation target	Operation	See
Log on security	Setting the system administrator password requirements	Password dialog box on page C-310
	Setting automatic locking of system administrator accounts	Account Lock dialog box on page C-312
	Setting the message to be shown as a warning banner in the login window	Edit Message dialog box on page C-314
System administrator accounts	Adding a system administrator	Add User dialog box on page C-300
	Deleting a system administrator	Table C-248 Operations that can be performed from the Users window on page C-299
	Editing the profile of a system administrator	Edit Profile dialog box on page C-303
	Changing the password of a system administrator	Change Password dialog box on page C-304
	Changing the permissions of a system administrator	Change Permission dialog box on page C-305
	Locking a system administrator account manually	Table C-248 Operations that can be performed from the Users window on page C-299
	Unlocking a system administrator account	Table C-248 Operations that can be performed from the Users window on page C-299
	Changing the system administrator authentication method	Change Authentication Method dialog box on page C-301
Processing nodes	Registering a processing node	Add Processing Node dialog box on page C-82
	Deleting a processing node	Table C-58 Operations that can be performed on a processing node from

Operation target	Operation	See
		the File Servers tab in the Processing Nodes window on page C-80
	Editing processing node information	Edit Node dialog box on page C-85
	Refreshing processing node information	Table C-67 Operation that can be performed on a processing node from the processing-node window on page C-87
	Starting a processing node	Table C-58 Operations that can be performed on a processing node from the File Servers tab in the Processing Nodes window on page C-80
	Stopping a processing node	Table C-58 Operations that can be performed on a processing node from the File Servers tab in the Processing Nodes window on page C-80
	Specifying settings for a physical node	Settings tab on page C-102
HCP	Registering an HCP system	Add Processing Node dialog box on page C-82
	Deleting an HCP system	Table C-60 HCP operations that can be performed from the Content Platform tab in the Processing Nodes window on page C-82
File systems	Creating a file system	Create File System dialog box on page C-126
	Deleting a file system	Table C-24 File system operations that can be performed from the File System tab in the File Systems window on page C-37

Operation target	Operation	See
		Table C-76 File system operations that can be performed for a file system from the File System subtab of the File Systems tab in the physical-node window on page C-98
	Expanding a file system	Expand File System dialog box on page C-52
	Unmounting a file system	Table C-24 File system operations that can be performed from the File System tab in the File Systems window on page C-37 Table C-43 File system operations that can be performed from the file-system window on page C-63 Table C-76 File system operations that can be performed for a file system from the File System subtab of the File Systems tab in the physical-node window on page C-98
	Mounting a file system	Mount File System dialog box on page C-54
	Editing the file system settings	Edit File System dialog box on page C-44
Quotas	Setting a user quota or group quota for each file system	Quota Setup page on page C-59
	Setting a default quota for a file system	Default Quota Setup page on page C-62
	Setting a quota grace period for a file system	Grace Period Setup page on page C-60
	Setting a quota monitoring method for a file system	Monitoring Setup page on page C-61

Operation target	Operation	See
File shares	Creating a file system and a file share at the same time	Create and Share File System dialog box on page C-103
	Adding a file share	Add Share dialog box on page C-38
	Releasing a file share	Table C-3 File share operations that can be performed from the Shares window on page C-7
		Table C-48 File share operations that can be performed from the Shares tab in the file-system window on page C-69 Table C-74 File share operations that can be performed from the Shares tab in the physical-node window on page C-94
	Changing the capacity of a file share	Change Share Quota dialog box on page C-19
	Editing the attributes of a file share	Edit Share dialog box on page C-7
Migration	Setting a migration task	Migration Task Wizard on page C-348
	Managing migration tasks	Migration Tasks dialog box on page C-336
Cluster, nodes, and resource groups	Defining a cluster configuration	Cluster Management dialog box on page C-268
	Changing the cluster configuration definition	Modify Cluster Configuration page on page C-276
	Viewing the cluster node status	Browse Cluster Status page (for Cluster / Node status) on page C-271
	Stopping or starting the cluster	Table C-227 Cluster and node information shown in the Browse Cluster Status page (for Cluster / Node

Operation target	Operation	See
		status) on page C-273
	Stopping or starting a node	Table C-227 Cluster and node information shown in the Browse Cluster Status page (for Cluster / Node status) on page C-273
	Forcibly stopping a cluster node	Table C-227 Cluster and node information shown in the Browse Cluster Status page (for Cluster / Node status) on page C-273
	Viewing the status of a resource group	Browse Cluster Status page (for Resource group status) on page C-278
	Stopping or starting a resource group	Table C-233 Operations that can be performed from the Browse Cluster Status page (for Resource group status) on page C-280
	Forcibly stopping a resource group	Table C-233 Operations that can be performed from the Browse Cluster Status page (for Resource group status) on page C-280
	Excluding a resource group as a monitored object or restarting monitoring of a resource group	Table C-233 Operations that can be performed from the Browse Cluster Status page (for Resource group status) on page C-280
	Changing the resource group execution node (failover and failback)	Table C-233 Operations that can be performed from the Browse Cluster Status page (for Resource group

Operation target	Operation	See
		status) on page C-280
	Restarting the OS (system administrator)# ¹	Table C-227 Cluster and node information shown in the Browse Cluster Status page (for Cluster / Node status) on page C-273
	Shutting down the OS (system administrator)# ¹	Table C-227 Cluster and node information shown in the Browse Cluster Status page (for Cluster / Node status) on page C-273
	Changing the host name of a node	Modify Host Name page on page C-277
Services	Controlling a service# ¹	Table C-191 Operations that can be performed from the List of Services page on page C-219
	Changing the configuration definition of the NFS service# ¹	NFS Service Management page on page C-248
	Changing the configuration definition of the CIFS service# ¹	CIFS Service Management page on page C-222
	Maintaining the CIFS service# ¹	CIFS Service Maintenance page on page C-258
	Changing the configuration definition of the SSH service# ¹	Public Key List page on page C-256
	Changing the configuration definition of the FTP service# ¹	FTP Service Management page on page C-242
	Changing the configuration definition of the SFTP service# ¹	SFTP Service Management page on page C-251
Network and system	Setting up ports# ¹	List of Data Ports page on page C-181
	Setting up and releasing trunking# ²	List of Trunking Configurations page on page C-187
	Setting up an interface and setting network information	List of Interfaces page on page C-192

Operation target	Operation	See
	Setting information for the DNS server, the NIS server, and the LDAP server for user authentication	DNS, NIS, LDAP Setup page on page C-197
	Setting routing information	List of Routings page on page C-200
	Specifying time-related settings	Time Setup page on page C-203
	Setting the destination for transferring system log data ^{#1}	Syslog Setup page on page C-204
	Setting the log file size ^{#1}	Log File Capacity Setup page on page C-206
	Setting the data retention period for core files ^{#1}	Core File Auto. Deletion Setup page on page C-208
	Directly editing system files ^{#2}	Edit System File page on page C-209
	Tuning system performance ^{#1}	Performance Tuning page on page C-213
	Setting up SNMP ^{#1}	List of SNMPs page on page C-214
	Selecting the user interface mode	Select User Interface page on page C-216
Proxy server	Setting proxy server information	Proxy Server Settings window on page C-281
Anti-virus	Setting up scan software ^{#1}	Scanning Software page on page C-293
	Registering a scan server ^{#1}	Add Scanner Server page on page C-287
	Changing the settings of a registered scan server ^{#1}	Edit Scanner Server page on page C-286
	Deleting a registered scan server ^{#1}	Table C-238 Operations that can be performed from the List of Scanner Servers page on page C-286
	Setting scan conditions ^{#1}	Scan Conditions page on page C-287
	Enabling or disabling real-time scanning ^{#1}	Table C-238 Operations that can be performed from the List of Scanner Servers page on page C-286

Operation target	Operation	See
Local users and groups	Managing local users	Local Users dialog box on page C-150
	Managing local groups	Local Users dialog box on page C-150
Hardware information	Viewing hardware information	Health Monitor window on page C-137
	Refreshing hardware information	Table C-104 Operations that can be performed from the Health Monitor window on page C-137
Software	Viewing software information	System Software window on page C-147
	Installing software	System Software Installation Wizard on page C-148
Linkage to Device Manager	Viewing Device Manager information	HDvM Connection Management dialog box on page C-334
	Editing Device Manager information	Edit HDvM Settings dialog box on page C-335
System configuration	Saving system settings	Save All System Settings page on page C-173
	Downloading or uploading system settings files	Upload Saved Data page on page C-176
	Setting periodic saving of the system settings	Schedule Settings for Saving All System Settings page on page C-177
Error information	Managing system messages ^{#1}	List of RAS Information page (for List of messages) on page C-165
	Managing system logs ^{#1}	List of RAS Information page (for List of system logs) on page C-167
	Managing other log files ^{#1}	List of RAS Information page (for List of other log files) on page C-167

Operation target	Operation	See
	Downloading or deleting all log files simultaneously ^{#1}	List of RAS Information page (for Batch-download) on page C-168
	Managing core and dump files ^{#1}	List of RAS Information page (for List of core files) on page C-169
	Viewing the status of the connections with external servers ^{#1}	List of RAS Information page (for Server check) on page C-170
<p>#1: Perform the operation for each node in the cluster.</p> <p>#2: Certain settings must be specified for each node in the cluster. For details, see the references.</p>		

Basic GUI operations

This appendix describes basic operations for the GUI.

- [Notes on using the GUI](#)
- [Hitachi File Services Manager main window](#)
- [Operation dialog boxes](#)
- [Confirmation dialog boxes](#)
- [Results dialog boxes](#)

Notes on using the GUI

Note the following when using the GUI:

- If you want to start and use multiple main windows on one management console, do not perform dialog operations for the same processing node simultaneously. Also, do not share a session in multiple main windows.
- If you want to update the contents shown in the GUI to the latest information, click **Refresh Processing Node**.
- If your mouse has a scroll wheel, do not use the scroll wheel while pressing the **Shift** key. Doing so can cause your Web browser to jump between pages, interrupting operations that are in progress. If this problem occurs, click **Close** to close the browser window.

If **Close** is not shown, click the **X** in the title bar to close the dialog box, and then show it again.

- You can perform the following operations only by using the menu (or shortcut keys) of the Web browser:

- Text size change
- Copy
- Paste

If you perform operations other than these, the GUI behavior might be affected.

- Click **Cancel** or **Close** to close dialog boxes that are no longer needed.
- If you use a dialog box while the network load is temporarily high, some information in the dialog box might not be shown. If this happens, close and re-open the dialog box, verify the status, and then start using it.
- If a window is closed while a page is loading, an error sometimes occurs the next time a window is opened, and no operations can be performed. If this happens, close all open Web browsers, and then start over from the beginning.
- You can use multi-byte Unicode (UTF-8) characters for the following items:
 - Path names
 - CIFS share names
 - Comments for CIFS shares
 - Comments for server names shown in the CIFS client
 - User names or group names that have been assigned by user mapping
- If some of the GUI items take a long time to appear and you cannot determine the cause, there might be a problem in the FC cable connections between the HDI node and the storage system. Verify the connections, and if you cannot locate the problem, view the system messages and log files to verify whether a failure occurred.

Note the following then using Internet Explorer:

- If the name of the execution result file obtained during user batch registration contains characters other than alphanumeric, the file name might be converted to corrupted characters (for example, %2d) at download time. This will not affect the contents of the file. If necessary, change the file name.
- When a file is downloaded, save it before viewing it. If **Open** is clicked in the download dialog box of the Web browser, the following might occur:
 - File information is shown in the download dialog box of Hitachi File Services Manager.
 - Even if the window showing download information is closed, the animation in the top of the dialog box will not stop and operation becomes impossible.

If a window becomes inoperable, click the **X** on the title bar to close the window.

- When a file has been downloaded and you attempt to close the download dialog box of Hitachi File Services Manager, the animation in the top of the dialog box might not stop and operation might become impossible. If a window becomes inoperable, click the **X** on the title bar to close the window.
- To upload a file, specify the path to the file. If you specify the file name only, the animation in the top of the dialog box might not stop and the window might become inoperative. If a window becomes inoperable, click the **X** on the title bar to close the window.

Hitachi File Services Manager main window

This section describes the basic layout of the Hitachi File Services Manager main window, and the items in each window.

The following figure shows the basic layout of the Hitachi File Services Manager main window:

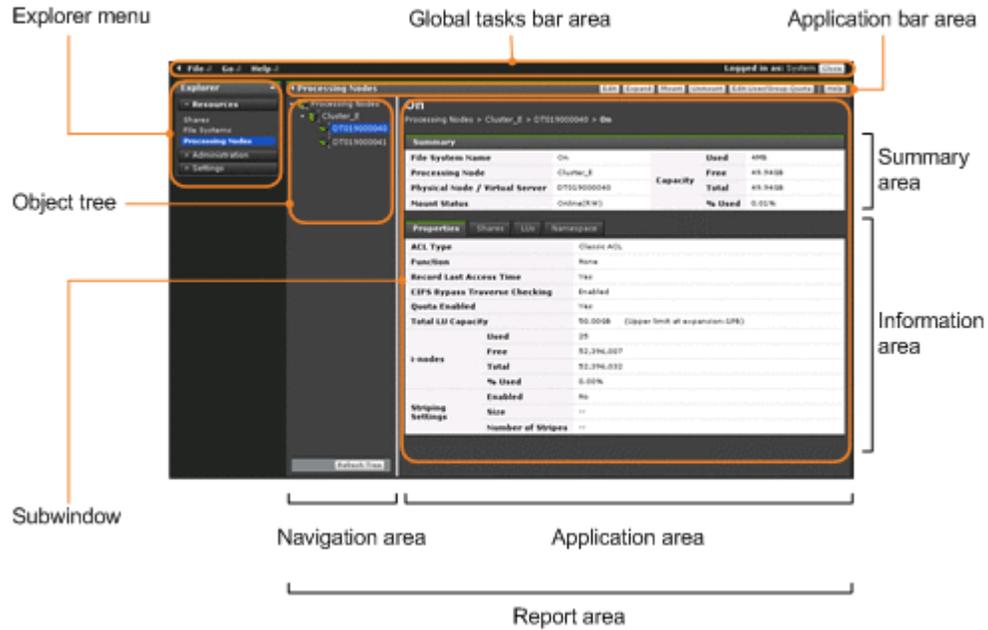


Figure B-1 Hitachi File Services Manager main window

Global tasks bar area

The global tasks bar area allows you to perform operations such as accessing Help or logging off the GUI.

You can show or hide the area that contains the **Explorer** menu by clicking the triangular icon at the far left of the global tasks bar area.

Table B-1 Global tasks bar area

Item	Description
File	Select this menu to finish using Hitachi File Services Manager. Close Logs you off of Hitachi File Services Manager and closes the window.
Go	The following items are shown: Configuration Wizard Select this to use the Configuration Wizard to perform a new HDI setup (see Configuration Wizard on page C-317). To change the configuration of a registered HDI system, click Reconfigure Processing Node in the <i>processing-node</i> window or <i>physical-node</i> window (see processing-node window on page C-86 or physical-node window on page C-91). HDvM Connection Management Select this to link Hitachi File Services Manager to Device Manager (see HDvM Connection Management dialog box on page C-334). Migration Tasks

Item	Description
	Select this to manage migration tasks (see Migration Tasks dialog box on page C-336).
Help	Select this menu to show Help or the version information. Online manual... Shows Help. About... Shows the Hitachi File Services Manager version. For details about how to verify the version information of the software running on a node, see System Software window on page C-147 .
Logged in as	Shows a maximum of 30 characters of the full name of the system administrator who is currently logged on. When the full name has been omitted, the user ID is shown.
Close	Logs you off of Hitachi File Services Manager and closes the window.

Explorer menu

The **Explorer** menu allows you to select an operation available in the Hitachi File Services Manager GUI. When you select an item from the **Explorer** menu, the appropriate information is shown in the navigation area and application area.

You can show or hide the **Explorer** menu by clicking the triangular icon at the far right of the **Explorer** menu bar.

Table B-2 Explorer menu

Item	Description
Resources	Shows the following menu items for managing objects such as file shares or file systems. This menu is shown only when a system administrator who has Admin permission for Hitachi File Services Manager is logged on. <ul style="list-style-type: none"> • Shares • File Systems • Processing Nodes
Administration	Shows the menu items listed below for managing users of Hitachi File Services Manager. This menu is shown only when a system administrator who has the Admin (user management) permission is logged on. <ul style="list-style-type: none"> • Users and Permissions • Security
Settings	Shows the following menu item for managing the profile of a system administrator: <ul style="list-style-type: none"> • User Profile

Navigation area

When the operation target selected in the **Explorer** menu is in a tree structure, the object tree appropriate to the item is shown in the navigation area.

You can show or hide the navigation area by clicking the triangular icon at the far left of the application bar area.

Table B-3 Navigation area

Item	Description
Object tree	Shows, in tree format, the objects for the item selected in the Explorer menu.
Refresh Tree	Refreshes the information in the object tree.

Application bar area

The application bar area shows buttons that are relevant to the information shown in the application area. Use these buttons to add or delete objects, or to change the settings for objects shown in the application area.

Click **Help** to show Help.

Application area (window)

The application area shows information relevant to the objects selected in the **Explorer** menu and object tree. The application area is a window.

Table B-4 Application area (window)

Item	Description
Summary area	Shows summary information about the objects selected in the Explorer menu and the object tree.
Information area	Shows information about the objects under the objects selected in the Explorer menu and the object tree. You can use the tabs and sub-tabs to change what information is shown.
Sort function	When you click a column title of a sortable table, the table is sorted according to that column. When the table has been sorted, an icon indicating whether the sorting is in ascending or descending order appears to the right of the column title used as the sort key.
Paging function	Lists objects on a page basis. You can select the number of lines in one page. You can perform the following operations with the paging function: Specifying the number of lines per page: From a drop-down list, you can select the number of lines to show on one page. The default is 25. Navigating pages:

Item	Description
	<p>You can navigate to the first page, the previous page, the next page, or the last page.</p> <p>Page text box:</p> <p>The current page number and the total number of pages. You can navigate to a specific page by entering the page number in the text box and then pressing the Enter key.</p> <p>Note that when you run the sort function, the display returns to the first page, regardless of which page is currently shown.</p>
Filtering function	<p>Allows you to extract, from the list of objects shown in the sortable table, information about objects that match specified conditions.</p> <p>When you specify a filtering condition in the Filter dialog box and then click OK, only information about the objects that match the filtering condition appears in the application area. When you click Apply, the Filter dialog box reappears after the filtering was performed, enabling you to continue setting filtering conditions.</p>

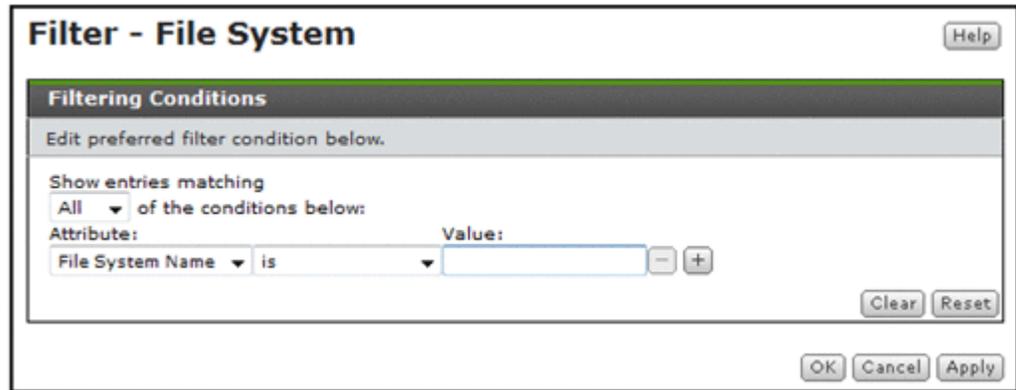


Figure B-2 Filter dialog box

Click **Filter Off** in the application area to remove the filtering conditions.

Operation dialog boxes

The following figure shows the operation dialog box launched from a window.

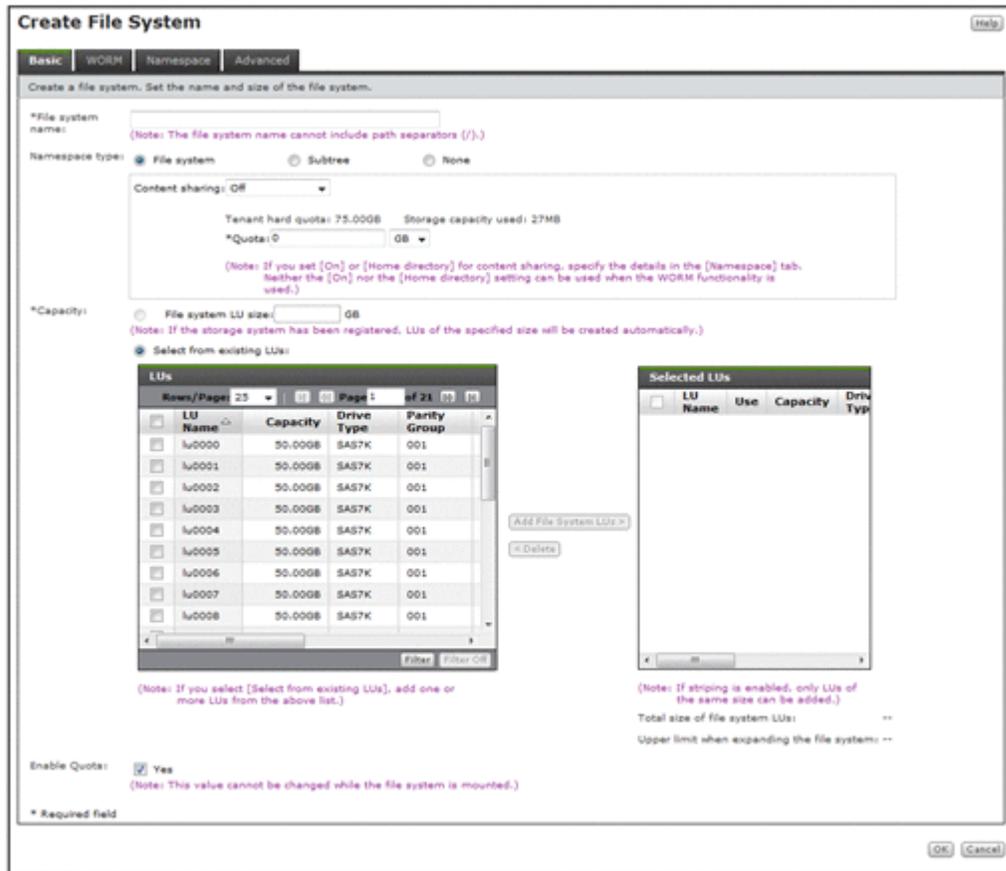


Figure B-3 Operation dialog box (launched from a window)

Table B-5 Operation dialog box (launched from a window)

Item	Description
Help	Shows Help.
OK	Begins the operation according to the specified information.
Cancel	Cancels the operation.

The following figure shows the operation dialog box launched from the **Settings** tab.

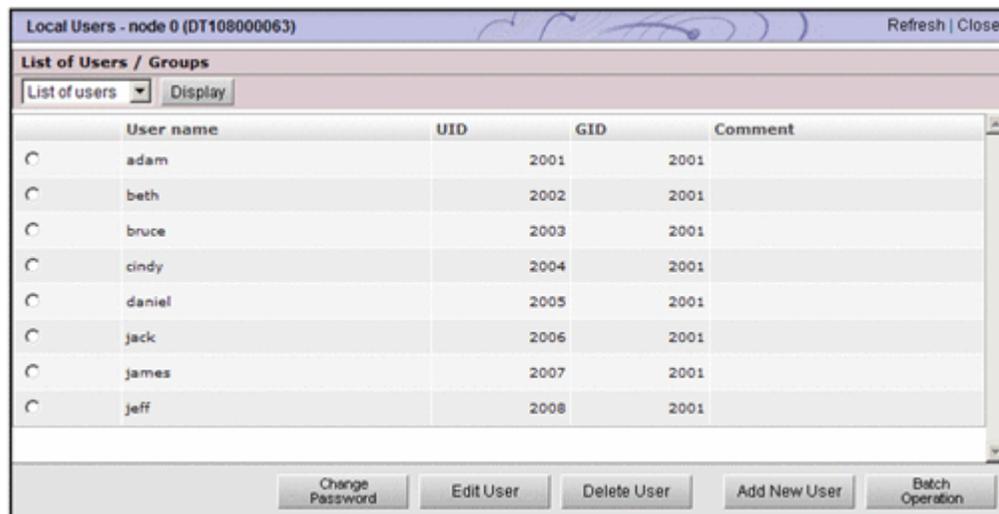


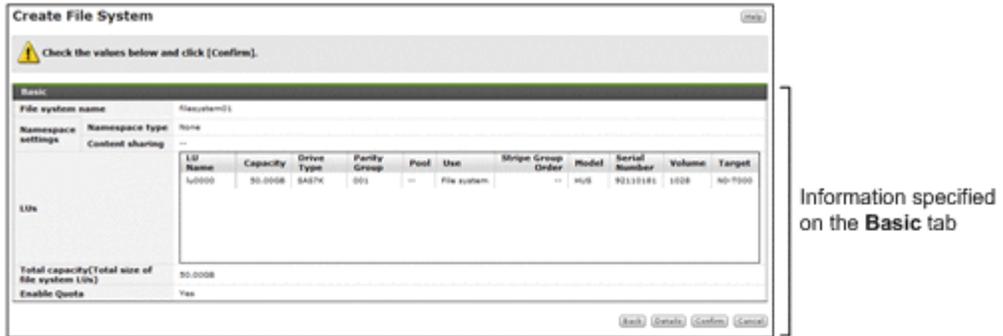
Figure B-4 Operation dialog box (launched from the Settings tab)

Table B-6 Operation dialog box (launched from the Settings tab)

Item	Description
Refresh	Updates the lists or object statuses in the page to the latest information. Although Refresh also appears in other pages, clicking it has no effect.
Close	Closes the dialog box.

Confirmation dialog boxes

The following figure shows the confirmation dialog boxes.



Click the **Details** button.

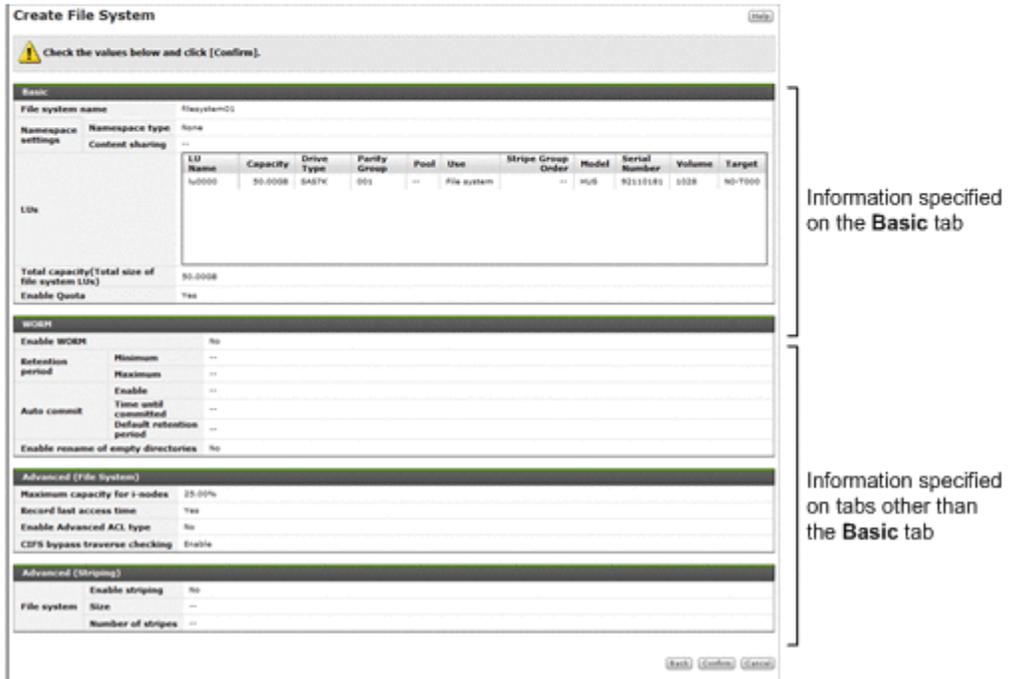


Figure B-5 Confirmation dialog box

Table B-7 Confirmation dialog boxes

Item	Description
Help	Shows Help.
Yes, confirmation-message check box	Select this check box to confirm that the information in the dialog box is correct and that processing can begin.
Back	Click Back to return to the operation dialog box. Some dialog boxes do not show Back .
Details	The information specified in the operation dialog box. When you click Details , detailed information for the operation appears below the Basic area. Some dialog boxes do not show Details .
Confirm	Begins processing according to the information shown in the confirmation dialog box.

Item	Description
Cancel	Cancels the operation.

Results dialog boxes

The following figure shows the results dialog box when an operation ends normally.



Figure B-6 Results dialog box when an operation ends normally

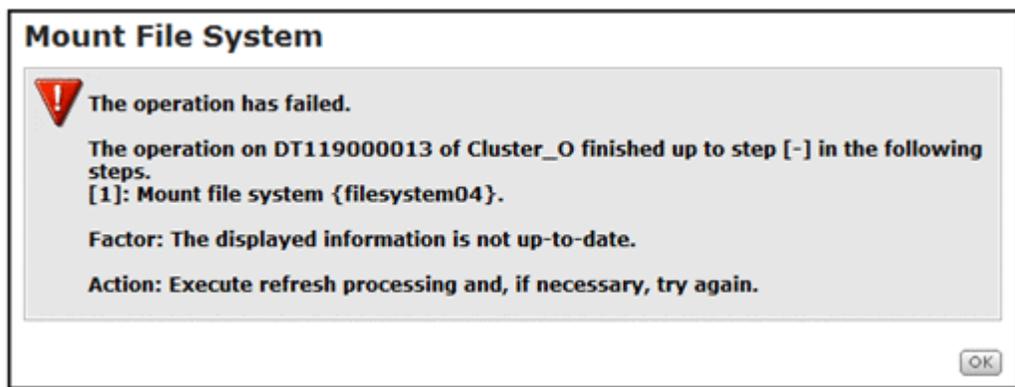


Figure B-7 Results dialog box when an operation ends in an error

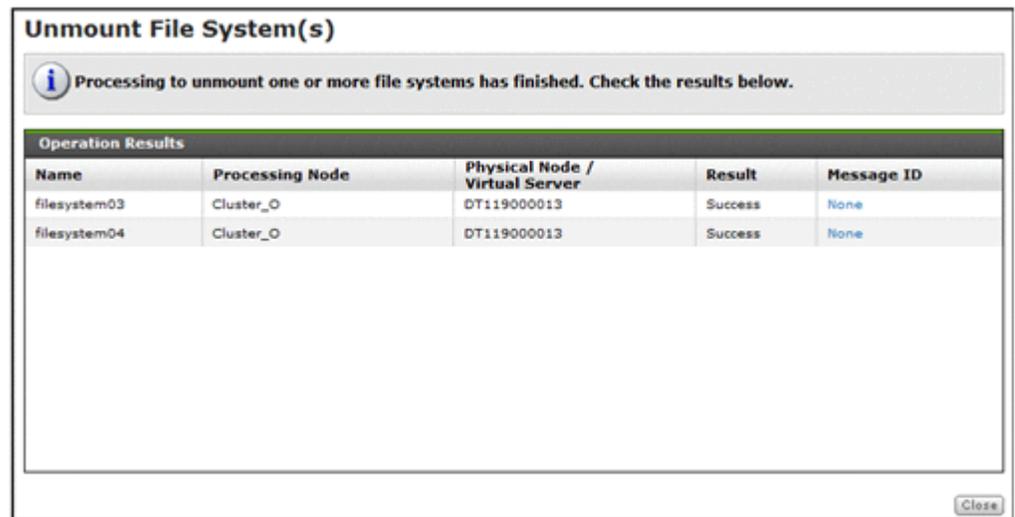


Figure B-8 Results dialog box when more than one object is specified in the operation dialog box

The following table shows the icons that appear in results dialog boxes

Table B-8 Icons that appear in results dialog boxes

Icon	Severity level	Description
	Information	Indicates that the operation finished normally. If you specified multiple virtual objects, this icon appears even if the operation has failed on some of the objects.
	Warning	Indicates that the processing of the operation finished, but there is a warning or point to confirm.
	Error	Indicates that an error occurred during processing of the operation.

When you specify more than one object in the operation dialog box, you can check information about each object in **Operation Results** of the results dialog box. The following table lists the information shown in **Operation Results**.

Table B-9 Operation Results

Item	Description
Name	The object name.
Result	The operation result. <i>Success</i> The operation ended successfully <i>Error</i> The operation ended with an error
Message ID	The linked content according to the operation result. <i>None</i> The operation ended successfully. When you click the link, the results dialog box for the successful operation is shown. <i>message-ID</i> When the operation ended with an error, a message ID corresponding to the error is shown. When you click the link, the results dialog box for the operation that ended with an error is shown.

In addition to the information in the previous table, some results dialog boxes show other related information.

Help

The Help.

OK and Close

Click either **OK** or **Help** to close the dialog box.

If the operation ends in an error, follow the instructions in the message that appears, and then try the operation again. For details about messages, see

the *Error Codes* manual. Check the output message ID and verify the cause of the error and the action to take.

GUI reference

This appendix describes the following items and how to use each window.

- [Shares window](#)
- [Edit Share dialog box](#)
- [Change Share Quota dialog box](#)
- [share window](#)
- [File Systems window](#)
- [Add Share dialog box](#)
- [Edit File System dialog box](#)
- [Expand File System dialog box](#)
- [Mount File System dialog box](#)
- [Edit Quota dialog box](#)
- [file-system window](#)
- [Processing Nodes window](#)
- [Add Processing Node dialog box](#)
- [Edit Node dialog box](#)
- [processing-node window](#)

- [physical-node window](#)
- [Create and Share File System dialog box](#)
- [Create File System dialog box](#)
- [Health Monitor window](#)
- [System Software window](#)
- [System Software Installation Wizard](#)
- [Local Users dialog box](#)
- [Check for Errors dialog box](#)
- [Backup Configuration dialog box](#)
- [Network & System Configuration dialog box](#)
- [Access Protocol Configuration dialog box](#)
- [Cluster Management dialog box](#)
- [Proxy Server Settings window](#)
- [Configure Proxy Server dialog box](#)
- [Virus Scan Server Configuration dialog box](#)
- [Activate License dialog box](#)
- [HCP-name window](#)
- [storage-system-name window](#)
- [Users and Permissions window](#)
- [Users window](#)
- [Add User dialog box](#)
- [Change Authentication Method dialog box](#)

- [user-ID window](#)
- [Edit Profile dialog box](#)
- [Change Password dialog box](#)
- [Change Permission dialog box](#)
- [Permissions window](#)
- [application window](#)
- [Security window](#)
- [Password window](#)
- [Password dialog box](#)
- [Account Lock window](#)
- [Account Lock dialog box](#)
- [Warning Banner window](#)
- [Edit Message dialog box](#)
- [User Profile window](#)
- [Configuration Wizard](#)
- [HDvM Connection Management dialog box](#)
- [Edit HDvM Settings dialog box](#)
- [Migration Tasks dialog box](#)
- [Download Report dialog box](#)
- [Failed dialog box](#)
- [Policy Information dialog box](#)
- [Migration Task Wizard](#)

- [File Systems dialog box](#)
- [Stop Task dialog box](#)
- [Migrate Immediately dialog box](#)
- [Enable Task dialog box](#)
- [Disable Task dialog box](#)
- [Delete Task dialog box](#)

Shares window

You can use the Shares window to view information about the file shares on processing nodes as a list.

To open the Shares window, in the **Explorer** menu of the Hitachi File Services Manager main window ([Explorer menu on page B-5](#)), select **Resources**, and then **Shares**.

Shares						
Summary						
Total Number of CIFS Shares	2					
Total Number of NFS Shares	1					
Total Number of Shares	2					
Shares						
Share Name	Protocol	Processing Node	Physical Node / Virtual Server	Use Namespace	Content Sharing	CIFS Share Name
filesystem04	CIFS, NFS	Cluster_O	DT119000013	--	--	filesystem04
filesystem04/share04	CIFS	Cluster_O	DT119000013	--	--	share04

Table C-1 Information shown in the Summary of the Shares window

Item	Description
Total Number of CIFS Shares	The number of CIFS shares on processing nodes.
Total Number of NFS Shares	The number of NFS shares on processing nodes.
Total Number of Shares	The number of file shares on processing nodes.

Table C-2 Information shown in the Shares of the Shares window

Item	Description
Share Name	The name of the share.
Protocol	The names of the protocols used by the file share. CIFS The CIFS protocol is used. NFS The NFS protocol is used.

Item	Description
	CIFS, NFS The CIFS and NFS protocols are used.
Processing Node	The name of the processing node (cluster) in which the file share is created.
Physical Node/Virtual Server	The name of the physical node on which the file share is currently operating.
Use Namespace	Displays whether the HCP namespace is allocated to the share. Yes Displayed when the HCP namespace is allocated to the share. No Displayed when the HCP namespace is not allocated to the share. If a file system is not linked to the HCP system at the share level, two hyphens (--) are displayed.
Content Sharing	Displays how data is shared with other HDI systems via the linked HCP. Off Displayed if data is not synchronized with other HDI systems On (Read-Only) Displayed if other HDI data is referenced as read-only If a file system is not linked to the HCP system at the share level, two hyphens (--) are displayed.
CIFS Share Name	The name of the CIFS share when the CIFS protocol is used in the file share. This item is left as blank if the CIFS protocol is not used.
Capacity ^{#1}	The usage of the file system. If the capacity of the file share is managed, the usage of the file share is shown. ^{#2} Used The used capacity of the file system or file share. Free The remaining capacity of the file system or file share. Total The total capacity of the file system or file share. % Used The percentage of the file system or file share capacity in use. 0 is shown in all items if the file system has not been mounted correctly.
Capacity Management Directory	The directory subject to capacity management is shown. If the capacity of the file share is not managed, the file system name is shown.

Item	Description
#1:	The values shown are calculated from the block capacity of the file system. Capacities shown in MB are rounded to the nearest ones place. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.
#2:	When the capacity of the file share is limited based on the hard quota of the migration-destination namespace, it will be displayed as follows. <ul style="list-style-type: none"> When it is a Shares window: "--" will be displayed. When it is a <i>share</i> window: The current usage status of the namespace quota will be displayed, not the block capacity of the file share. However, "--" will be displayed if the information cannot be obtained from the HCP system.

Table C-3 File share operations that can be performed from the Shares window

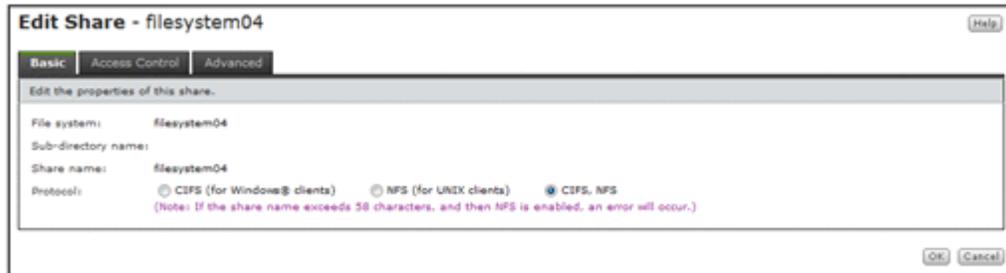
Button	Function	See
Release Share	Release an unnecessary file share. Notes: <ul style="list-style-type: none"> The shared directory is not deleted even after the file share is released. When the CIFS protocol and NFS protocol are being used, both are released. Edit the file share attributes if you want to release only one protocol. For details about editing file share attributes, see Basic tab on page C-8. If the CIFS service configuration definition settings do not allow the CIFS share settings to be automatically reloaded and you released a CIFS share during degenerated operation, to enable the CIFS share settings, perform a failback operation, and then restart the CIFS services on both nodes. For details about how to carry out perform a failback operation, see Browse Cluster Status page on page C-271. For details about how to restart a CIFS service, see List of Services page on page C-218. 	N/A
Edit Share	Edit file share attributes such as the protocol and access permissions.	Edit Share dialog box on page C-7
Change Share Quota	Change the quota for the file share immediately under the mount point.	Change Share Quota dialog box on page C-19
Note: N/A = Not applicable.		

Edit Share dialog box

You can use the **Edit Share** dialog box to edit file share attributes. The current settings are applied to any information that is not changed.

To set the ACL for a created shared directory, use the `dirsetacl` command.

To open the **Edit Share** dialog box, select the target share name on the **Shares** tab in the *file-system* window ([file-system window on page C-62](#)), and then click **Edit Share**.



Basic tab

You can use the **Basic** tab to edit the file share properties.

Table C-4 Information specified in the Basic tab in the Edit Share dialog box

Item	Description
Protocol	<p>Select the protocol to be used in the file share.</p> <p>CIFS (for Windows® clients) Select this option to use the CIFS protocol.</p> <p>NFS (for UNIX clients) Select this option to use the NFS protocol.</p> <p>CIFS, NFS Select this option to use the CIFS protocol and the NFS protocol. However, if the file share was created in a file system that supports home-directory-roaming, you cannot change the CIFS (for Windows® clients) setting.</p>
Use namespace	<p>Select Yes to allocate HCP namespaces to the share.</p> <p>If Off is specified for Content sharing, specify the following items:</p> <ul style="list-style-type: none"> • Namespace name Specify a migration-destination namespace name of no more than six characters that you want to add to the end of the file share name. You can use alphanumeric characters and hyphens (-). You cannot, however, use a hyphen (-) as the last character. • Quota Specify the hard quota that you want to allocate to the namespace. Specify a value smaller than the Tenant hard quota value. • Synchronize the file share capacity with the namespace quota To limit the usage capacity per share based on the hard quota of the migration-destination namespace, select the Yes check box. When the Yes check box is selected, the value specified in Quota becomes the maximum value that can be used in the share.

Access Control tab

You can use the **Access Control** tab to specify attributes related to file share access permissions.

CIFS subtab

You can use the **CIFS** subtab to specify attributes related to CIFS share access permissions.

Table C-5 Information specified in the CIFS subtab of the Access Control tab in the Edit Share dialog box

Item	Description
Enable ACL ^{#1}	Select this check box to reference or set the ACL from the client. Note that you cannot set the ACL for the guest account (<i>nobody</i>). If you specify this setting, you cannot cancel it later.
Read only	Select this check box to allow access for the CIFS share in read-only mode. If a file system containing a file share is mounted as read-only, the CIFS share is shared as read-only, even if this check box is cleared. Note that if the file system supports home-directory-roaming, you cannot share CIFS shares as read-only, so you cannot select this item.
Special permitted users/groups	To set permissions for a specific user or group separately from file share permissions, select the target user or group from the Users or Groups tab. Add RW > Click this button to permit read-write access. Add RO > Click this button to permit read-only access. < Delete Click this button to delete users or groups from Special Permitted Users or Special Permitted Groups . Refresh Users and Groups Click this button to refresh information about users and groups. If you select the user or group whose permission has already been set and click Add RW > or Add RO > , the new permission will be applied. The total number of users and groups whose access permissions are set in Special permitted users/groups is limited to 100 or fewer per file share. Note that the following equation must be satisfied (the number of users is <i>u</i> , the number of groups is <i>g</i> , the total number of characters for user names is <i>n</i> , and the total number of characters for group names is <i>m</i>): $u + 2g + n + m \leq 1024$ (\leq : Less than or equal to)

Item	Description
	Note that users and groups registered by using the user mapping functionality cannot be specified in the GUI.
Host/network based access restriction	<p>To limit the CIFS clients that can access the CIFS share, specify, in the text box, the host name^{#2} or IP address of each CIFS client that is to be allowed access to the CIFS share. Alternatively, specify the network address^{#3} of the network to which each CIFS client belongs. To specify multiple CIFS clients, delimit clients by using commas (,). Note that you can specify no more than 5,631 characters in total. To allow all CIFS clients access to the CIFS share, do not specify anything in the text box.</p> <p>You must also select an option to specify whether the specified CIFS clients are to be allowed or denied access to the CIFS share.</p> <p>Notes:</p> <ul style="list-style-type: none"> - If hosts or networks with limited access are set in the CIFS service configuration definition (CIFS Service Management page of the Access Protocol Configuration dialog box), the setting applies to all file shares. To set hosts or networks with limited access for each CIFS share, do not set hosts or networks with limited access in the CIFS service configuration definition. - To specify the host name, edit the <code>/etc/hosts</code> file to add all the specified host names and IP addresses. If you do not add host names in the <code>/etc/hosts</code> file, the specified information might not take effect. Also, if any of the host names you specify for an IP address has been added as an alias after the first host name, file share access might not behave as specified. For details about how to edit the <code>/etc/hosts</code> file, see Edit System File page on page C-209. - Even if you permit access to the CIFS share, user authentication is carried out for the CIFS client.
Browsable share	Select this option to list the CIFS share names in the CIFS client environment.
Allow guest account access^{#4}	<p>Select whether you permit access for guest accounts.</p> <p>Yes</p> <p>Allow access for guest accounts.</p> <p>No</p> <p>Do not allow access for guest accounts.</p> <p>Inherit CIFS service default</p> <p>Use the CIFS service configuration definitions.</p> <p>A guest account is handled as <code>nobody</code> (user-ID: 65534) regardless of CIFS service authentication modes. Therefore, for a CIFS share that is accessible with a guest account, set the access permissions taking into consideration that the CIFS share can be accessed by <code>nobody</code>. You cannot set the ACL for a guest account (<code>nobody</code>). However, if access with a guest account is not permitted at all in the CIFS service settings, the settings for individual CIFS shares do not apply.</p> <p>Note that if the file system supports home-directory-roaming, guest accounts are denied access by default. You cannot change this setting.</p>

Item	Description
Set access permissions only for the owner	In an Advanced-ACL-type file system, if only Owner has read or write permissions, select the Yes check box. Access permissions are not set for Group or Other (all users and groups).
Access permissions for new files	<p>When sharing a CIFS share in read-write mode, set access permissions to Owner, Group, and Other (in the case of the Advanced ACL type, all users and groups) for creating files.</p> <p>RW Select this option to permit read-write access.</p> <p>RO Select this option to permit read-only access.</p> <p>None Select this option to not permit read or write access.</p> <p>If RO or None is specified for Owner, even the owner will not be able to write to new files.</p> <p>If RO is set for Group, set RO or None for Other. To set None for Group, also set None for Other. If you set access permissions other than these for Other, Group access permissions set for files might be deleted when the files are updated.</p>
Access permissions for new directories	<p>To permit access to the CIFS share in read-write mode, set access permissions for Owner, Group, and Other (in the case of the Advanced ACL type, all users and groups) when a new directory is created.</p> <p>RW Select this option to permit read-write access.</p> <p>RO Select this option to permit read-only access.</p> <p>None Select this option to not permit read or write access. Only searching is permitted.</p> <p>If you specify RO or None for Owner, even the owner will not be able to write to new directories.</p> <p>If you set RO for Group, set RO or None for Other as well. If you set None for Group, set None for Other as well. If you set access permissions other than these for Other, Group access permissions set for directories might be deleted when the directories are updated.</p>
<p>#1: Specify this item when editing attributes of a file share in a file system of the Classic ACL type.</p> <p>#2: You cannot specify the following names as the host name:</p> <ul style="list-style-type: none"> • ALL • FAIL • EXCEPT <p>#3: Specify the network address in the format below: <i>network-address/netmask</i> (example: 10.203.15.0/255.255.255.0) Specify a prefix length for the netmask for IPv6.</p>	

Item	Description
	#4: When the CIFS share settings and the CIFS service configuration definitions are different from each other, the CIFS share settings are applied. If Inherit CIFS service default is selected for the item, the settings specified in the CIFS service configuration definition are applied. In addition, after settings in the CIFS service configuration definition are changed, the new settings will be automatically applied.

NFS subtab

You can use the **NFS** subtab to specify attributes related to NFS share access permissions.

Table C-6 Information specified in the NFS subtab of the Access Control tab in the Edit Share dialog box

Item	Description				
Hosts	<p>Specify the hosts allowed to access the NFS share, access permission, and a target to be mapped as an anonymous user. You can specify multiple hosts to access the NFS share.</p> <p>Add RW > Click this button to permit read-write access to the NFS share for the specified hosts by using the specified anonymous mapping setting.</p> <p>Add RO > Click this button to permit read-only access to the NFS share for the specified hosts by using the specified anonymous mapping setting.</p> <p>< Delete Click this button to delete a host from Selected Hosts.</p> <p>Note that the total length (specified length + 5 bytes) of the specified host names or network addresses must be less than 1,258 bytes.</p> <table border="1" data-bbox="542 1207 1399 1848"> <thead> <tr> <th data-bbox="542 1207 750 1249">Host/network</th> <th data-bbox="750 1207 1399 1249"></th> </tr> </thead> <tbody> <tr> <td data-bbox="542 1249 750 1848"></td> <td data-bbox="750 1249 1399 1848"> <p>Specify 255 characters or fewer. Specify a host name beginning with an alphabetic character and consisting of alphanumeric characters, hyphens (-), and underscores (_). If you specify a host alias, the official host name also must be 255 characters or fewer. In addition to the host name and the IP address, you can use the following formats:</p> <p>Netgroup Specify an NIS netgroup. For example, for @group, only the host segment is extracted from the netgroup members.</p> <p>IP network To permit all hosts in the subnetwork to access the NFS share, specify the IP address and the netmask in the following format: <i>address/netmask</i> The netmask can be specified in dotted decimal format or as a prefix length (Specify a prefix length for IPv6).</p> </td> </tr> </tbody> </table>	Host/network			<p>Specify 255 characters or fewer. Specify a host name beginning with an alphabetic character and consisting of alphanumeric characters, hyphens (-), and underscores (_). If you specify a host alias, the official host name also must be 255 characters or fewer. In addition to the host name and the IP address, you can use the following formats:</p> <p>Netgroup Specify an NIS netgroup. For example, for @group, only the host segment is extracted from the netgroup members.</p> <p>IP network To permit all hosts in the subnetwork to access the NFS share, specify the IP address and the netmask in the following format: <i>address/netmask</i> The netmask can be specified in dotted decimal format or as a prefix length (Specify a prefix length for IPv6).</p>
Host/network					
	<p>Specify 255 characters or fewer. Specify a host name beginning with an alphabetic character and consisting of alphanumeric characters, hyphens (-), and underscores (_). If you specify a host alias, the official host name also must be 255 characters or fewer. In addition to the host name and the IP address, you can use the following formats:</p> <p>Netgroup Specify an NIS netgroup. For example, for @group, only the host segment is extracted from the netgroup members.</p> <p>IP network To permit all hosts in the subnetwork to access the NFS share, specify the IP address and the netmask in the following format: <i>address/netmask</i> The netmask can be specified in dotted decimal format or as a prefix length (Specify a prefix length for IPv6).</p>				

Item	Description
	<p>DNS domain</p> <p>Specify the name of the DNS domain to which NFS clients belong, with a period (.) added at the beginning of the name.</p> <p>Example: <code>.example.com</code></p> <p>Wild card</p> <p>To specify all hosts, use an asterisk (*) as a wild card.</p> <p>When the NFS client machine has multiple network interfaces communicating with the HDI system, specify the hosts and networks allowed to access the NFS share in one of the following formats:</p> <ul style="list-style-type: none"> • Use a wild card (*). • Specify the IP addresses of all network interfaces used on the NFS client side. • Specify the host names for all network interfaces used on the NFS client side. • Specify an IP network that contains the IP addresses of all network interfaces used on the NFS client side. • Specify a netgroup that contains the host names for all network interfaces used on the NFS client side. • Specify a DNS domain that contains the host names for all network interfaces used on the NFS client side.
	<p>Security flavor</p> <p>Specify a security flavor.</p> <p>Use the default settings^{#1}</p> <p>Select this to use the NFS service configuration definitions.</p> <p>Use the original settings</p> <p>Select this to specify different settings from the NFS service configuration definitions.</p> <p>Select one or more of the following check boxes:</p> <ul style="list-style-type: none"> - sys <p>Select this to use the UNIX (AUTH_SYS) authentication.</p> <ul style="list-style-type: none"> - krb5 <p>Select this to use the Kerberos authentication.</p> <ul style="list-style-type: none"> - krb5i <p>Select this to use the data integrity function in addition to the Kerberos authentication.</p> <ul style="list-style-type: none"> - krb5p <p>Select this to use the data integrity function and the privacy function in addition to the Kerberos authentication.</p>

Item	Description
	<p>Anonymous mapping^{#2}</p> <p>Select users who can access the HDI system from the hosts allowed to access the NFS share specified in the Host/network and those you want to map as anonymous users.</p> <p>Not applied</p> <p>Select this option to disable anonymous user mapping.</p> <p>For root user</p> <p>Select this option to map only the root user as an anonymous user.</p> <p>For anyone</p> <p>Select this option to map every user as an anonymous user.</p>
UID for anonymous mapping	Specify the user ID for accessing as an anonymous user. Specify a value in the range from 0 to 65535.
GID for anonymous mapping	Specify the group ID for accessing as an anonymous user. Specify a value in the range from 0 to 65535.
<p>#1: The NFS service configuration definitions at the time a file share is created will be used. Even if you create a file share, and then change the settings of the NFS service configuration definitions, the changes will not be applied to the existing file shares.</p> <p>#2: If you specify For root user, UID for anonymous mapping and GID for anonymous mapping will be used only for the root users after user mapping in the NFS service is performed. If you specify For anyone, UID for anonymous mapping and GID for anonymous mapping will supersede the user mapping settings in the NFS service.</p>	

Namespace tab

You can use the **Namespace** tab to specify information about the namespace to be allocated to shares. The information to be specified depends on the usage of the namespace.

Table C-7 Information specified in the Namespace tab in the Edit Share dialog box (when Content sharing is set to Off)

Item	Description
Namespace-access account	Select Create and specify a password to create an account for accessing the namespace from another HDI system.

Table C-8 Information specified in the Namespace tab in the Edit Share dialog box (when Content sharing is set to On (Read-Only))

Item	Description
Namespace FQDN	If Yes is specified for Use namespace on the Basic tab, specify the fully qualified domain name of the namespace that is used for referencing other HDI data as read-only via the linked HCP.
External HCP host name	If the HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the HCP system.
Namespace-access account	Specify the user name and password for the account for accessing the namespace. If you click the Test Connection for Primary button after specifying information, you can check the connection with the HCP system.
Replica	If you are using the HCP replication functionality, select the Use check box. System name Specify the replica HCP system name to Fully Qualified Domain Name. External Replica HCP host name If the replica HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the replica HCP system. After specifying the information, click the Test Connection for Replica button to check whether you can connect to the replica HCP system.

Advanced tab

You can use the **Advanced** tab to specify attributes of the file share as required.



Note: Observe the following notes:

- You can use commands to set even more detailed attributes for the file share.
- If the CIFS service configuration definition settings do not allow the CIFS share settings to be automatically reloaded and you added a CIFS share during degenerated operation, to enable the CIFS share settings, perform a failback operation, and then restart the CIFS services on both nodes. For details about how to perform a failback operation, see [Browse Cluster Status page on page C-271](#). For details about how to restart a CIFS service, see [List of Services page on page C-218](#).

CIFS subtab

You can use the **CIFS** subtab to specify the attributes of the CIFS share.

Table C-9 Information specified in the CIFS subtab of the Advanced tab in the Edit Share dialog box

Item	Description
CIFS share name	<p>Specify the CIFS share name.</p> <p>Specify 80 characters or fewer.</p> <p>You can use any alphanumeric character, exclamation mark (!), hash mark (#), dollar sign (\$), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), plus sign (+), comma (,), hyphen (-), period (.), semicolon (;), equal sign (=), at mark (@), left square bracket ([), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), right curly bracket (}), tilde (~), or space. You can also specify multi-byte characters. However, the string cannot contain only a dollar sign or periods (e.g., \$, ., or ..) and cannot end with a period (e.g., Abc.). If the string ends with a dollar sign, you cannot specify a period just before that dollar sign (e.g., Abc.\$). The space specified at the end of the string will be removed.</p> <p>If you use a percent sign (%) in the CIFS share name, make sure the percent sign is not used in any of the following combinations:</p> <p>%D, %G, %H, %I, %L, %M, %N, %P, %R, %S, %T, %U, %V, %a, %d, %g, %h, %i, %m, %p, %u, %v, %w, %\$</p> <p>In addition, the CIFS share name cannot be <code>global</code>, <code>homes</code>, <code>printers</code>, <code>admin\$</code>, <code>c\$</code>, <code>global\$</code>, <code>homes\$</code>, <code>ipc\$</code>, or <code>printers\$</code>.</p> <p>Windows does not distinguish between uppercase and lowercase alphabetic characters. Specify a unique name on the physical node regardless of uppercase and lowercase alphabetic characters.</p> <p>If omitted, the share name of the file system is used as a CIFS share name.</p>
Comment shown to CIFS clients	<p>Specify the CIFS share comment, using 256 characters or fewer.</p> <p>You can use any alphanumeric character, exclamation mark (!), hash mark (#), dollar sign (\$), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), forward slash (/), colon (:), left angle bracket (<), right angle bracket (>), question mark (?), at mark (@), left square bracket ([], backslash (\), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({ }, vertical bar (), right curly bracket (}), and tilde (~). In addition, you can specify multi-byte characters. You can also specify a space, but a string cannot start or end with a space. Also, a string cannot end with a backslash (\).</p>
Enable auto creation of home directory	<p>Select this option to use the function for automatically creating a home directory in the CIFS share.</p>

Item	Description
	<p>However, if the file share was created in a home-directory-roaming file system, the function for automatically creating a home directory is enabled by default. To disable the function, use the <code>cifsedit</code> command.</p>
<p>Users allowed to change file time stamp^{#1#2}</p>	<p>Select the users who can update the time-stamps of files in the CIFS share. To share files using only the CIFS protocol, select Write permitted users.</p> <p>Write permitted users</p> <p>Enable all users allowed to write files to update the time-stamps.</p> <p>Owner only</p> <p>Enable only the file owner to update the time-stamps.</p> <p>Inherit CIFS service default</p> <p>Use the CIFS service configuration definitions.</p>
<p>Disk synchronization policy^{#2}</p>	<p>Specify the operations for write requests from CIFS clients to the CIFS share.</p> <p>At write and close</p> <p>Select this to write synchronously with a write request or a close request.</p> <p>At close</p> <p>Select this to write synchronously with a close request.</p> <p>Routine disk flush only</p> <p>Select this to write at a fixed interval, regardless of when write requests and close requests are made.</p> <p>Inherit CIFS service default</p> <p>Use the CIFS service configuration definitions.</p> <p>For details about how the system works for each setting, see the notes in Table C-202 Information specified in the CIFS Service Management page (Setting Type: Performance) on page C-236.</p>
<p>Windows® client access policy^{#2}</p>	<p>Select the method for processing accesses from Windows clients.</p> <p>Parallel</p> <p>Process accesses in parallel.</p> <p>Serial</p> <p>Process accesses serially.</p> <p>Inherit CIFS service default</p> <p>Use the CIFS service configuration definitions.</p>
<p>Allow CIFS client cache^{#2}</p>	<p>Specify whether the updated data of the file in the CIFS share is cached to the client.</p> <p>Specify No for read-write-content-sharing file systems. If the updated data of the file in the CIFS share is cached on the client, the update date might not be reflected properly on other sites.</p> <p>Yes</p>

Item	Description
	<p>Cache data. The performance can be improved by caching the updated data for files in a CIFS share to the client. However, data reliability might be degraded if a failure occurs in the CIFS client or network.</p> <p>For the file systems listed below, we recommend also setting Allow read-only client cache for access conflicts values to Yes, because there is a risk that the client cache will fail to validate.</p> <ul style="list-style-type: none"> - File systems that migrate data to an HCP system <p>No</p> <p>Do not cache data.</p> <p>Inherit CIFS service default</p> <p>Use the CIFS service configuration definitions.</p>
<p>Allow read-only client cache for access conflicts^{#2}</p>	<p>Specify whether to use a read-only client cache when multiple CIFS clients simultaneously attempt to access a file.</p> <p>Yes</p> <p>Select this to use a read-only client cache. This improves system performance because data is cached on the client PC when a CIFS client opens a file. The caching of data improves system performance. This item can be selected if Yes is selected under Allow CIFS client cache. In addition, this item can be selected if Inherit CIFS service default is selected under Allow CIFS client cache when the CIFS service configuration definitions are set to cache updates to the files in CIFS shares.</p> <p>No</p> <p>Select this to not use a read-only client cache.</p> <p>Inherit CIFS service default</p> <p>Select this if the CIFS service configuration definitions determine whether a read-only client cache is used.</p> <p>Note that we recommend that you do not use the read-only client cache if you also want to use the NFS protocol to access the file shares because changes might not be applied. If you need to use the read-only client cache, we recommend implementing file sharing individually for each protocol to ensure that the NFS protocol is not used to access the share.</p>
<p>Allow Access Based Enumeration^{#2}</p>	<p>Specify whether to enable access-based enumeration.</p> <p>Yes</p> <p>Select this to enable access-based enumeration.</p> <p>No</p> <p>Select this to disable access-based enumeration.</p> <p>Inherit CIFS service default</p> <p>Select this if the CIFS service configuration definitions determine whether access-based enumeration is enabled.</p>
<p>Use Volume Shadow Copy Service</p>	<p>This item is not supported.</p>

Item	Description
SMB encryption ^{#2#3}	<p>Specify whether communication with the CIFS client is to be encrypted.</p> <p>The setting for this item is only valid if you select SMB 3.0 for the SMB protocol in CIFS Service Management page (Setting Type: Basic) of the Access Protocol Configuration dialog box. If you select an option other than SMB 3.0 for the SMB protocol, select Disable or set communication with the CIFS client not to be encrypted in the configuration definition of the CIFS service, and then select the Inherit CIFS service default.</p> <p>Auto</p> <p>Select this option if communication with the client is to be encrypted only when the client supports encryption.</p> <p>Mandatory</p> <p>Select this option if communication with the client is always to be encrypted.</p> <p>Only clients that support SMB 3.0 or later can access a CIFS share. Note that clients cannot access a CIFS share by using guest accounts.</p> <p>Disable</p> <p>Select this option if communication with the client is not to be encrypted.</p> <p>Inherit CIFS service default</p> <p>Use the CIFS service configuration definitions.</p>
<p>#1: Specify when creating a file system of the Classic ACL type.</p> <p>#2: When the CIFS share settings and the CIFS service configuration definitions are different from each other, the CIFS share settings are applied. If Inherit CIFS service default is selected for the item, the settings specified in the CIFS service configuration definition are applied. In addition, after settings in the CIFS service configuration definition are changed, the new settings will be automatically applied.</p> <p>#3: If Mandatory is selected in SMB encryption for some CIFS shares and Disable is selected for others, select Auto. Note that when Disable is selected in SMB encryption for the CIFS share, if you select Mandatory, the CIFS share will become inaccessible. If Mandatory or Disable is selected in SMB encryption in the CIFS service configuration definitions, select Inherit CIFS service default.</p>	

Change Share Quota dialog box

The system administrator can change the quota for the file share immediately under the mount point in a file system with the quota functionality enabled.

Before setting or changing the quota for shares, update the processing node information. Also ask clients not to access the directory until the setting is completed.

To open the **Change Share Quota** dialog box, select the target share name on the **Shares** tab in the *file-system* window ([file-system window on page C-62](#)), and then click **Change Share Quota**.

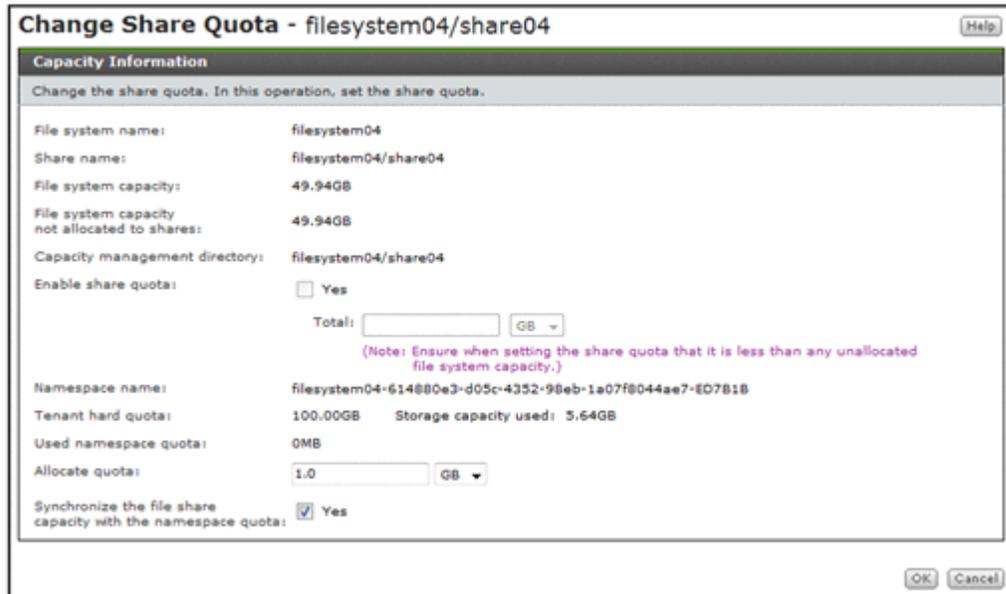


Table C-10 Information specified in the Change Share Quota dialog box

Item	Description
Enable share quota #	<p>Select the Yes check box when managing the share capacity (setting the subtree quota) by specifying the capacity of the file share (the block capacity that can be used). This check box can be selected if the quota functionality for the file system is enabled.</p> <p>Total</p> <p>If the Yes check box for Enable share quota is selected, the quota for the file share can be specified. A value larger than the Used value and smaller than File system capacity not allocated to shares can be specified. If MB is selected as the unit, specify an integer. If a unit other than MB is selected, you can specify a value with a maximum of two decimal places.</p>
Allocate quota	<p>Specify the hard quota to be allocated to the migration-destination namespace when data is migrated to the HCP system at the share level. Specify a value that is greater than the Used namespace quota value and smaller than the Tenant hard quota value. Select GB, TB, or PB for the unit.</p>
Synchronize the file share capacity with the namespace quota #	<p>To limit the usage capacity per share based on the hard quota of the migration-destination namespace when data is migrated to the HCP system at the share level, select the Yes check box. This check box can be selected if the quota functionality for the file system is enabled.</p> <p>When the Yes check box is selected, the value specified in Allocate quota becomes the maximum value that can be used in the share.</p>
<p>#: You cannot select Enable share quota and Synchronize the file share capacity with the namespace quota at the same time.</p>	

If the directory for which capacity management is to be set contains many files, the setting process might take time (about 34 seconds for 50,000 files). If there are 2,640,000 or more files, it is likely that a timeout will occur. If a timeout occurs, because the setting processing continues, check the processing status from system messages that have been output. If the KAQM04136-I system message has been output, then processing has ended normally. If the message has not been output, check the status of the network.

If the KAQM04137-I message has been output as a system message, the processing has been completed successfully. If the KAQM04138-E message has been output, the processing has failed. In this case, use the File Services Manager log (`management.log`) to check the failure details, remove the cause of the failure, and then use the `stquotaset` command to restore the capacity management settings. If the failure occurred while capacity management was being set, remove the quota settings of the directory. If the failure occurred while the capacity management setting was being removed, specify the quota settings again. After the settings have been restored, try the operation again.

After the capacity of a share has been set, the usage shown of the share might be larger than the usage of the file system. If this occurs, update the processing node information.

share window

You can use the *share* window to view detailed information about a specific file share.

To open the *share* window, click the desired *share* link in one of the following windows:

- Shares window (see [Shares window on page C-5](#))
- **Shares** tab in the *physical-node* window (see [Shares tab on page C-93](#))
- **Shares** tab in the *file-system* window (see [Shares tab on page C-68](#))

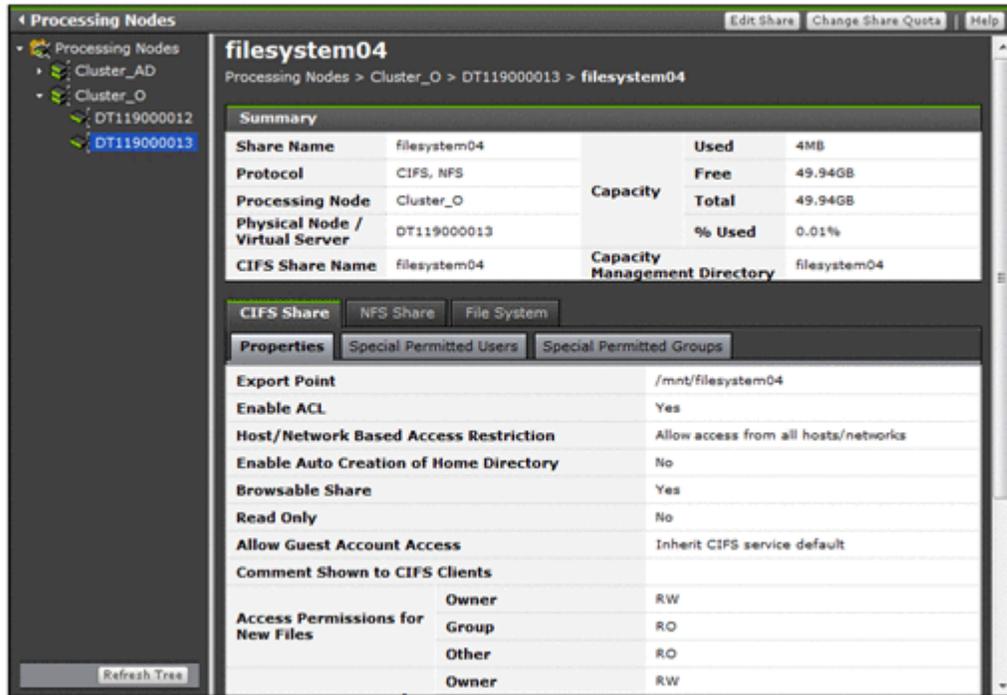


Table C-11 File share operations that can be performed from the share window

Button	Function	See
Edit Share	Edit file share attributes such as the protocol and access permissions.	Edit Share dialog box on page C-7
Change Share Quota	Change the quota for the file share immediately under the mount point.	Change Share Quota dialog box on page C-19

Table C-12 Information shown in the share window

Item	Description	See					
Summary	Information about the file share.	Table C-2 Information shown in the Shares of the Shares window on page C-5					
CIFS Share	Information about the CIFS share when the CIFS protocol is used.	N/A					
	<table border="1"> <tr> <td>Properties</td> <td>The attributes of the CIFS share.</td> <td>Properties subtab on page C-23</td> </tr> <tr> <td>Special Permitted Users</td> <td>For a CIFS share, information about users who have access permissions that are different from the permissions of other users.</td> <td>Special Permitted Users subtab on page C-27</td> </tr> </table>	Properties	The attributes of the CIFS share.	Properties subtab on page C-23	Special Permitted Users	For a CIFS share, information about users who have access permissions that are different from the permissions of other users.	Special Permitted Users subtab on page C-27
Properties	The attributes of the CIFS share.	Properties subtab on page C-23					
Special Permitted Users	For a CIFS share, information about users who have access permissions that are different from the permissions of other users.	Special Permitted Users subtab on page C-27					

Item	Description		See
	Special Permitted Groups	For a CIFS share, information about groups that have access permissions that are different from the permissions of other groups.	Special Permitted Groups subtab on page C-27
NFS Share	Information about the NFS share when the NFS protocol is used.		N/A
	Properties	The attributes of the NFS share.	Properties subtab on page C-28
	Hosts	Information about the hosts allowed to access the NFS share.	Hosts subtab on page C-28
File System	Information about the file system in which the file share was created.		File System tab on page C-29
Namespace	Information about the namespace allocated to the shares.		Namespace tab on page C-31
Note: N/A = Not applicable.			

CIFS Share tab

You can use the **CIFS Share** tab to view information about the CIFS share when the CIFS protocol is used.

Properties subtab

You can use the **Properties** subtab to view the attributes of the CIFS share.

Table C-13 Information shown on the Properties subtab of the CIFS Share tab in the share window

Item	Description
Export Point	The absolute path of the shared directory.
Enable ACL	Indicates whether CIFS clients are allowed to view and set the ACL. Yes CIFS clients are allowed to view and set the ACL. No CIFS clients are not allowed to view and set the ACL.
Host/Network Based Access Restriction	The access restriction for the CIFS share. Allow access from all hosts/networks Shown when access is allowed from all hosts and networks. Allow access from Shown with the specific hosts and networks that are explicitly allowed access.

Item	Description
	<p>Disallow access from</p> <p>Shown with the specific hosts and networks that are explicitly denied access.</p>
<p>Enable Auto Creation of Home Directory</p>	<p>Indicates whether the function for automatically creating a home directory is enabled or disabled.</p> <p>Yes</p> <p>The function for automatically creating a home directory is enabled.</p> <p>No</p> <p>The function for automatically creating a home directory is disabled.</p>
<p>Browsable Share</p>	<p>Indicates whether CIFS share names are listed in the CIFS client environment.</p> <p>Yes</p> <p>CIFS share names are listed.</p> <p>No</p> <p>CIFS share names are not listed.</p>
<p>Read Only</p>	<p>Indicates whether read-only access to the CIFS share is allowed.</p> <p>Yes</p> <p>Read-only access is allowed.</p> <p>No</p> <p>Read-write access is allowed.</p>
<p>Allow Guest Account Access[#]</p>	<p>Indicates whether to allow a guest account access to the CIFS share.</p> <p>Yes</p> <p>Guest account access is allowed.</p> <p>No</p> <p>Guest account access is not allowed.</p> <p>Inherit CIFS service default</p> <p>The CIFS service configuration definitions are used.</p>
<p>Comment Shown to CIFS Clients</p>	<p>Shows the comment for the CIFS share.</p>
<p>Access Permissions for New Files</p>	<p>Displays access permissions for creating files in a write-permitted CIFS share for Owner, Group, and Other (in Advanced-ACL-type file systems, this means all users and groups).</p> <p>--</p> <p>Yes is specified for the Set access permissions only for the owner setting for creating or editing CIFS shares.</p> <p>RW</p> <p>Read-write access is allowed.</p> <p>RO</p> <p>Read-only access is allowed.</p>

Item	Description
	<p>None Neither read nor write access is allowed.</p> <p>Unknown The ACL type of the file system could not be obtained.</p>
<p>Access Permissions for New Directories</p>	<p>Displays access permissions for creating directories in a write-permitted CIFS share for Owner, Group, and Other (in Advanced-ACL-type file systems, this means all users and groups).</p> <p>-- Yes is specified for the Set access permissions only for the owner setting for creating or editing CIFS shares.</p> <p>RW Read-write access is allowed.</p> <p>RO Read-only access is allowed.</p> <p>None Neither read nor write access is allowed.</p> <p>Unknown The ACL type of the file system could not be obtained.</p>
<p>Users Allowed to Change File Time Stamp[#]</p>	<p>Shows the users who can update the time-stamps of files in the CIFS share.</p> <p>-- The file system is the Advanced ACL type. For a file system of the Advanced ACL type, only the users who have write permission can update the time-stamps.</p> <p>Write permitted users All users who are allowed to write to files can update the time-stamps.</p> <p>Owner only Only the file owner can update the time-stamps.</p> <p>Inherit CIFS service default The file system in which the CIFS share was created is the Classic ACL type, and the CIFS service configuration definitions are used. The CIFS service configuration definitions are used.</p> <p>Unknown The ACL type of the file system could not be obtained.</p>
<p>Disk Synchronization Policy[#]</p>	<p>Shows operational settings for write requests from CIFS clients to the CIFS share.</p> <p>At write and close Writing is performed synchronously with a write request or a close request.</p> <p>At close Writing is performed synchronously with a close request.</p> <p>Routine disk flush only</p>

Item	Description
	<p>Writing is performed at a fixed interval, regardless of when write requests and close requests are made.</p> <p>Inherit CIFS service default</p> <p>The CIFS service configuration definitions are used.</p> <p>For details about how the system works for each setting, see the notes in Table C-202 Information specified in the CIFS Service Management page (Setting Type: Performance) on page C-236.</p>
Windows® Client Access Policy#	<p>Indicates the method for processing accesses from Windows clients.</p> <p>Parallel</p> <p>Accesses are processed in parallel.</p> <p>Serial</p> <p>Accesses are processed serially.</p> <p>Inherit CIFS service default</p> <p>The CIFS service configuration definitions are used.</p>
Allow CIFS Client Cache#	<p>Indicates whether updated data files in the CIFS share are cached to clients.</p> <p>Yes</p> <p>The client caching is enabled.</p> <p>No</p> <p>The client caching is disabled.</p> <p>Inherit CIFS service default</p> <p>The CIFS service configuration definitions are used.</p>
Allow Read-only Client Cache for Access Conflicts#	<p>Indicates whether a read-only client cache is used when multiple CIFS clients simultaneously attempt to access a file.</p> <p>Yes</p> <p>The read-only client cache is used.</p> <p>No</p> <p>The read-only client cache is not used.</p> <p>Inherit CIFS service default</p> <p>The CIFS service configuration definitions are used.</p>
Allow Access Based Enumeration#	<p>Indicates whether access-based enumeration is used.</p> <p>Yes</p> <p>Access-based enumeration is used.</p> <p>No</p> <p>Access-based enumeration is not used.</p> <p>Inherit CIFS service default</p> <p>The CIFS service configuration definitions are used.</p>
Use Volume Shadow Copy Service	<p>Shows Inherit CIFS service default.</p>
SMB Encryption#	<p>Displays whether the communication with the CIFS client is to be encrypted when you use SMB 3.0.</p>

Item	Description
	Auto Communication with the client is to be encrypted only when the client supports encryption. Mandatory Communication with the client is always to be encrypted. Disabled Communication with the client is not to be encrypted. Inherit CIFS service default The CIFS service configuration definitions are used.
#: When the CIFS share settings and the CIFS service configuration definitions are different from each other, the CIFS share settings are applied. If <code>Inherit CIFS service default</code> is displayed for the item, the settings specified in the CIFS service configuration definition are applied. In addition, after settings in the CIFS service configuration definition are changed, the new settings will be automatically applied.	

Special Permitted Users subtab

You can use the **Special Permitted Users** subtab to view, for a CIFS share, information about users who have access permissions that are different from the permissions of other users.

Table C-14 Information shown on the Special Permitted Users subtab of the CIFS Share tab in the share window

Item	Description
User Name	The names of any users who have special access permissions for the file share.
Permission	The access permission. RW Read-write access is allowed. RO Read-only access is allowed.

Special Permitted Groups subtab

You can use the **Special Permitted Groups** subtab to view, for a CIFS share, information about groups that have access permissions that are different from the permissions of other groups.

Table C-15 Information shown on the Special Permitted Groups subtab of the CIFS Share tab in the share window

Item	Description
Group Name	The names of any groups that have special access permissions for the file share.

Item	Description
Permission	The access permission. RW Shown when read-write access is allowed. RO Shown when read-only access is allowed.

NFS Share tab

You can use the **NFS Share** tab to view information about the NFS share when the NFS protocol is used.

Properties subtab

You can use the **Properties** subtab to view the attributes of the NFS share.

Table C-16 Information shown on the Properties subtab of the NFS Share tab in the share window

Item	Description
Export Point	The absolute path of the shared directory.
UID for Anonymous Mapping	The user ID for access as an anonymous user.
GID for Anonymous Mapping	The group ID for access as an anonymous user.

Hosts subtab

The **Hosts** subtab shows information about the hosts allowed to access the NFS share.

Table C-17 Information shown on the Hosts subtab of the NFS Share tab in the share window

Item	Description
Host/Network	The name of the host or network from which access is allowed to the NFS share.
Permission	The access permissions for the NFS share. RW Read-write access is allowed. RO Read-only access is allowed.
Security Flavor	The security flavor that is being used. If multiple security flavors are being used, the security flavors are shown separated by commas.

Item	Description
	<p>sys The UNIX (AUTH_SYS) authentication is being used.</p> <p>krb5 The Kerberos authentication is being used.</p> <p>krb5i The Kerberos authentication as well as the data integrity function are being used.</p> <p>krb5p The data integrity function and the privacy function in addition to the Kerberos authentication are being used.</p>
Anonymous Mapping	<p>The users mapped as anonymous users.</p> <p>Not applied Anonymous user mapping is disabled.</p> <p>For root user Only the root user is mapped as an anonymous user.</p> <p>For anyone All users are mapped as an anonymous user.</p>

File System tab

You can use the **File System** tab to view information about the file system in which the file share was created.

Table C-18 Information specified in the File System tab in the share window

Item	Description
File System Name	The name of the file system.
Mount Status	<p>Shows the status of the file system.</p> <p>Online (RW) The file system is mounted with both read and write operations permitted.</p> <p>Online (RO) The file system is mounted as read-only.</p> <p>Unmounted The file system is unmounted.</p> <p>Expanding The file system is being expanded or an error occurred during expansion processing. Wait a while, and then refresh the processing node information. If the status does not change, an error might have occurred during processing. Obtain all the log data, and then inform maintenance personnel.</p> <p>Reclaiming</p>

Item	Description
	<p>The unused area of the virtual LUs that are used for the file system is being released.</p> <p>Data corrupted</p> <p>The file system is blocked because of an error in the OS or a pool capacity shortage.</p> <p>Take corrective action by referring to the <i>Cluster Troubleshooting Guide</i>.</p> <p>Device error</p> <p>The file system is blocked because of an error in the LU (multiple drive failure).</p> <p>Take corrective action by referring to the <i>Cluster Troubleshooting Guide</i>.</p>
ACL Type	<p>The ACL type of the file system.</p> <p>Advanced ACL</p> <p>The file system is the Advanced ACL type.</p> <p>Classic ACL</p> <p>The file system is the Classic ACL type.</p> <p>Unknown</p> <p>Shown when ACL type information cannot be obtained.</p>
Function	<p>The name of the function that is using the file system.</p> <p>None</p> <p>The file system is not being used by another function.</p> <p>Active Migration</p> <p>The file system is used by a function of Active File Migration.</p> <p>WORM</p> <p>Shown for a WORM file system.</p>
Quota Enabled	<p>Shows whether the quota function is enabled for the file system.</p> <p>Yes</p> <p>The quota function is enabled.</p> <p>No</p> <p>The quota function is disabled.</p> <p>If the LU or the file system is blocked, the status in effect before the failure occurred is shown. Additionally, <i>No</i> is shown after a failure under one of the following conditions:</p> <ul style="list-style-type: none"> • The quota setting was disabled before the failure occurred. • The quota setting was enabled before the failure occurred. However, the status was changed when, for example, an unmount operation was performed after the failure.
Total LU Capacity	<p>The total capacity of the LUs that make up the file system.</p> <p>Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.</p> <p>The upper limit for expansion of the file system capacity is also displayed. If the initial capacity of a created file system is less</p>

Item	Description
	than 32 GB + 16 MB, the maximum capacity after expansion will be less than the displayed value. For details about the initial capacity of a created file system and the maximum capacity after expansion, see the <i>CLI Administrator's Guide</i> .
Capacity[#]	<p>The usage of the file system.</p> <p>Used The used capacity of the file system.</p> <p>Free The remaining capacity of the file system.</p> <p>Total The total capacity of the file system.</p> <p>% Used The percentage of the file system capacity in use.</p> <p>If the file system has not been mounted correctly, 0 is shown in all items.</p>
i-nodes	<p>The inode usage.</p> <p>Used The used inode capacity.</p> <p>Free The free inode capacity.</p> <p>Total The total inode capacity.</p> <p>% Used The percentage of inode capacity in use.</p> <p>If the file system has not been mounted correctly, 0 is shown in all items.</p>
Striping Settings	<p>The striping information.</p> <p>Enabled Yes if the file system is in a striping configuration. No if the file system is not in a striping configuration.</p> <p>Size The stripe size. If the file system is not in a striping configuration, -- is shown.</p> <p>Number of Stripes The number of stripes. If the file system is not in a striping configuration, -- is shown.</p>
<p>[#]: The values shown are calculated from the block capacity of the file system. Capacities shown in MB are rounded to the nearest ones place. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.</p>	

Namespace tab

You can use the **Namespace** tab to view information about the HCP namespace. The information shown depends on the content sharing settings.

Table C-19 Information shown in the Namespace tab in the share window (when content sharing is set to Off)

Item	Description
Use Namespace	<p>Displays whether the HCP namespace is allocated to the share.</p> <p>Yes Displayed when the HCP namespace is allocated to the share.</p> <p>No Displayed when the HCP namespace is not allocated to the share.</p> <p>If No is specified, Target Namespace and Namespace-access Account are not displayed.</p>
Content Sharing	Shows <i>Off</i> .
Target Namespace	The HCP namespace to which data is migrated.
Namespace-access Account	The user name of the account for accessing the namespace from another HDI system.
Synchronize the File Share Capacity with the Namespace Quota	<p>Displays whether the usage capacity is limited per share based on the hard quota of the migration-destination namespace.</p> <p>Yes Usage capacity is limited.</p> <p>No Usage capacity is not limited.</p>

Table C-20 Information shown in the Namespace tab in the share window (when content sharing is set to On (Read-Only))

Item	Description
Use Namespace	<p>Displays whether the HCP namespace is allocated to the share.</p> <p>Yes Displayed when the HCP namespace is allocated to the share.</p> <p>No Displayed when the HCP namespace is not allocated to the share.</p> <p>If No is specified, Target Namespace and Namespace-access Account are not displayed.</p>
Content Sharing	Shows <i>On (Read-Only)</i> .
Target Namespace	The namespace that is used for referencing other HDI data as read-only via the linked HCP.
External HCP Host Name	The host name or IP address that has been made external and is used to connect to the HCP system is displayed.
Namespace-access Account	<p>The user name of the account for accessing the namespace.</p> <p>If you click the Test Connection for Primary button after specifying information, you can check the connection to the HCP system.</p>

Item	Description
Replica System Name	If you are using the HCP replication functionality, the system name is displayed.
External Replica HCP Host Name	The host name or IP address that has been made external and is used to connect to the replica HCP system is displayed.

File Systems window

In the File Systems window, you can view the operating status and usage of each file system.

To open the File Systems window, in the **Explorer** menu of the Hitachi File Services Manager main window ([Explorer menu on page B-5](#)), select **Resources**, and then **File Systems**.

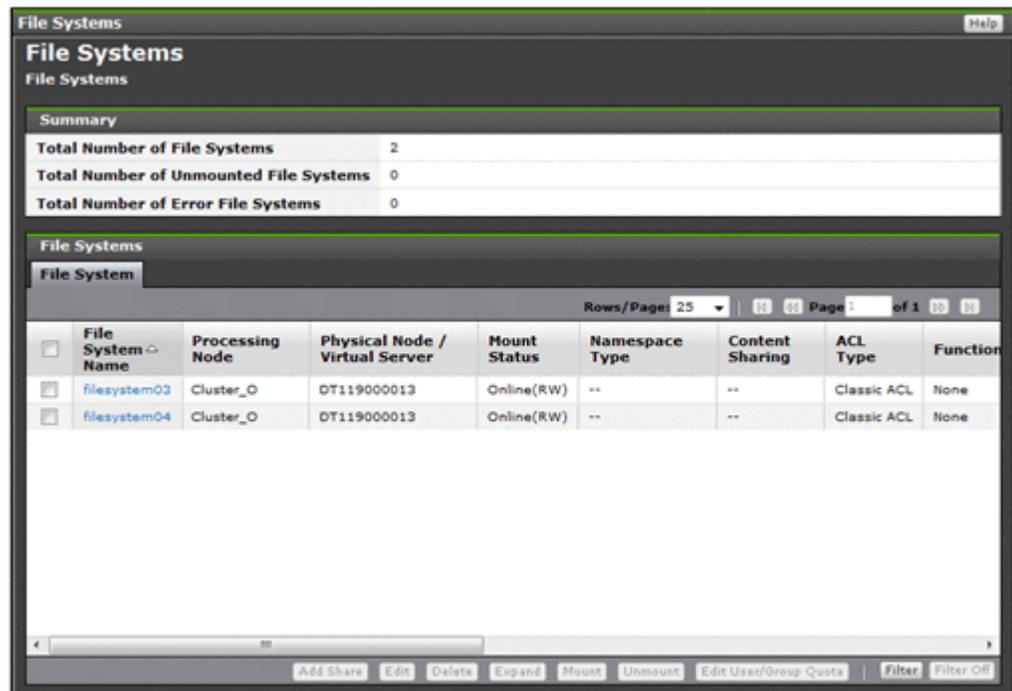


Table C-21 Information shown in the Summary of the File Systems window

Item	Description
Total Number of File Systems	The number of file systems on processing nodes.
Total Number of Unmounted File Systems	The number of unmounted file systems among the file systems on processing nodes.
Total Number of Error File Systems	The number of file systems where an error has occurred among the file systems on processing nodes.

Table C-22 Information shown in the File Systems of the File Systems window

Item	Description	See
File System	Information about file systems is shown.	File System tab on page C-34

File System tab

You can use the **File System** tab to view information about file systems.

Table C-23 Information shown in the File System tab in the File Systems window

Item	Description
File System Name	The name of the file system.
Processing Node	The name of the processing node (cluster) on which the file system was created.
Physical Node/ Virtual Server	The name of the physical node on which the file system is currently running.
Mount Status	<p>The status of the file system.</p> <p>Online (RW) The file system is mounted with both read and write operations permitted.</p> <p>Online (RO) The file system is mounted as read-only.</p> <p>Unmounted The file system is unmounted.</p> <p>Expanding The file system is being expanded or an error occurred during expansion processing. Wait a while, and then refresh the processing node information. If the status does not change, an error might have occurred during processing. Obtain all the log data, and then inform maintenance personnel.</p> <p>Reclaiming The unused area of the virtual LUs that are used for the file system is being released.</p> <p>Data corrupted The file system is blocked because of an error in the OS or a pool capacity shortage. Take corrective action by referring to the <i>Cluster Troubleshooting Guide</i>.</p> <p>Device error</p>

Item	Description
	<p>The file system is blocked because of an error in the LU (multiple drive failure).</p> <p>Take corrective action by referring to the <i>Cluster Troubleshooting Guide</i>.</p>
Namespace Type	<p>Displays how the file system is linked to the HCP system.</p> <p>File System</p> <p>The file system is linked to the HCP system at the file system level.</p> <p>Subtree</p> <p>The file system is linked to the HCP system at the share level.</p> <p>-- is shown when a namespace is not used.</p>
Content Sharing	<p>Displays how data is shared with other HDI systems via the linked HCP.</p> <p>Off</p> <p>Displayed if data is not synchronized with other HDI systems</p> <p>On (Read-Only)</p> <p>Displayed if other HDI data is referenced as read-only</p> <p>On (Read/Write)</p> <p>Displayed if the read-write-content-sharing functionality is used to share data among HDI systems (read-write-content-sharing file system)</p> <p>Home directory</p> <p>Displayed if roaming among HDI systems is enabled for home directory data created for each end user (home-directory-roaming file system)</p> <p>-- is shown when a namespace is not used.</p>
ACL Type	<p>The ACL type of the file system.</p> <p>Advanced ACL</p> <p>The file system is the Advanced ACL type.</p> <p>Classic ACL</p> <p>The file system is the Classic ACL type.</p> <p>Unknown</p> <p>The ACL type information cannot be obtained.</p>
Function	<p>Shows the name of the function that is using the file system.</p> <p>None</p> <p>The file system is not being used by another function.</p> <p>Active Migration</p> <p>The file system is used by a function of Active File Migration.</p> <p>WORM</p> <p>A WORM file system.</p>

Item	Description
Quota Enabled	<p>Shows whether the quota function is enabled for the file system.</p> <p>Yes The quota function is enabled.</p> <p>No The quota function is disabled.</p> <p>If the LU or the file system is blocked, the status in effect before the failure occurred is shown. Additionally, No is shown after a failure under one of the following conditions:</p> <ul style="list-style-type: none"> • The quota setting was disabled before the failure occurred. • The quota setting was enabled before the failure occurred. However, the status was changed when, for example, an unmount operation was performed after the failure.
Total LU Capacity	<p>The total capacity of the LUs that make up the file system. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.</p>
Capacity[#]	<p>The usage of the file system.</p> <p>Used The used capacity of the file system.</p> <p>Free The remaining capacity of the file system.</p> <p>Total The total capacity of the file system.</p> <p>% Used The percentage of the file system capacity in use.</p> <p>If the file system has not been mounted correctly, 0 is shown in all items.</p>
i-nodes	<p>The inode usage.</p> <p>Used The used inode capacity.</p> <p>Free The free inode capacity.</p> <p>Total The total inode capacity.</p> <p>% Used The percentage of inode capacity in use.</p> <p>If the file system has not been mounted correctly, 0 is shown in all items.</p>
<p>[#]: The values shown are calculated from the block capacity of the file system. Capacities shown in MB are rounded to the nearest ones place. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.</p>	

Table C-24 File system operations that can be performed from the File System tab in the File Systems window

Button	Function	See
Add Share	Add a file share in the file system. Note that a file share cannot be added if the read-write-content-sharing file system or home-directory-roaming file system and a file share has already been created.	Add Share dialog box on page C-38
Edit	Edit the file system settings.	Edit File System dialog box on page C-44
Delete	Delete a file system that is no longer required. This operation can be performed when the nodes and the resource group satisfy the following conditions: <ul style="list-style-type: none"> • The status of both nodes is <code>UP</code>. • The status of the resource group is <code>Online/No error</code> or <code>Offline</code>. Perform the following operations in advance: <ul style="list-style-type: none"> • Release all file shares in the target file system. Notes: <ul style="list-style-type: none"> • If the target file system has been mounted, it is unmounted automatically. • A file system cannot be deleted if it contains a file whose retention period has not expired. • If a file system whose data has been migrated to an HCP is deleted, the data on the HCP is not deleted. • After the file system is deleted, the LUs used for the file system can be used for other purposes. • When the status of the resource group is <code>Offline</code> and a file system for which file shares have been created is deleted, its NFS shares are automatically released but its CIFS shares are not. After starting the resource group, use the appropriate commands to release the file shares. 	N/A
Expand	Expand the capacity of a file system as needed.	Expand File System dialog box on page C-52

Button	Function	See
Mount	Mount a file system.	Mount File System dialog box on page C-54
Unmount	Unmount a file system when maintenance of the HDI system is required or to change the file system attributes.	N/A
Edit User/Group Quota	<p>Manage quota information for each file system.</p> <p>By clicking this button, you can open the Edit Quota dialog box for a specific file system. You can show up to 10 Edit Quota dialog boxes for a physical node at the same time. To close unnecessary Edit Quota dialog boxes, click Close. If the Edit Quota dialog box cannot be opened, quit all Web browsers, and then log on again.</p>	Edit Quota dialog box on page C-55
Note: N/A = Not applicable.		

Add Share dialog box

In the **Add Share** dialog box, the system administrator can add a file share to the mount point directory or any directory in the existing file system. The advanced attribute of the file share can be set for each protocol.

A maximum of 1,024 NFS shares can be created per cluster. Access control when an NFS share is created in a file system of the Advanced ACL type follows the set ACL, not the permissions that can be referenced from the client side. Therefore, when only NFS shares are to be used, Hitachi Data Systems recommends a file system of the Classic ACL type. For the same reason, even if you are using an Advanced ACL file system, Hitachi Data Systems recommends that you do not set ACE (access control entry) inheritance for directories in which NFS shares will be created.

The maximum number of CIFS shares per cluster depends on whether the setting in the CIFS service configuration definitions specifies that the CIFS share settings are to be automatically applied to the CIFS client environment. For details about the maximum number of CIFS shares, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

To open the **Add Share** dialog box, select the target file system in the File Systems window ([File Systems window on page C-33](#)), and then click **Add Share**.

Table C-25 Information shown in the Add Share dialog box

Item	Description	See	
Basic	Specify basic attributes related to the file share.	Basic tab on page C-40	
Access Control	Specify attributes related to file share access permissions. The Directory subtab does not appear if you select Use existing directory as is under Export point owner on the Basic tab or if you want to reference other HDI data as read-only at the share level.	Access Control tab on page C-108	
	CIFS	Specify attributes related to CIFS share access permissions.	CIFS subtab on page C-108#
	NFS	Specify attributes related to NFS share access permissions.	NFS subtab on page C-111#
	Directory	For the Advanced ACL type, set the ACL for the shared directory. For the Classic ACL type, set access permissions for the shared directory.	Directory subtab (A file system of the Advanced ACL type) on page C-114# Directory subtab (A file system of the Classic ACL type) on page C-115#
Namespace	Specify namespace information if you are allocating HCP namespaces to the share.	Namespace tab on page C-43	

Item	Description	See
Advanced	Specify attributes of the file share as required.	Advanced tab on page C-121
	CIFS	Specify attributes of the CIFS share.

#: See the information shown in the **Create and Share File System** dialog box.

Basic tab

You can use the **Basic** tab to specify the basic attributes related to the file share.

Table C-26 Information specified in the Basic tab in the Add Share dialog box

Item	Description
Share directory name	<p>Specify the path of the directory to which a file share is to be added. Directory paths that can be specified depend on the protocol that is used.</p> <p>When the CIFS protocol is used</p> <p>You can use any alphanumeric character, exclamation mark (!), hash mark (#), dollar sign (\$), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), plus sign (+), comma (,), hyphen (-), period (.), forward slash (/), semicolon (;), equal sign (=), at mark (@), left square bracket ([), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), right curly bracket (}), tilde (~), or space. You can also specify multi-byte characters. The total number of characters for the directory path, including the file system name, must be no more than 251.</p> <p>If you use a percent sign (%) in the shared directory name, make sure the percent sign is not used in any of the following combinations:</p> <p>%D, %G, %H, %I, %L, %M, %N, %P, %R, %S, %T, %U, %V, %a, %d, %g, %h, %i, %m, %p, %u, %v, %w, %\$</p> <p>Note that if the directory name at the end of the shared directory satisfies one of the following conditions, you need to specify the CIFS share name of the Advanced tab:</p> <ul style="list-style-type: none"> - When there are more than 80 characters. - When the name is <code>global</code>, <code>homes</code>, or <code>printers</code>. - When the directory name conflicts with an existing CIFS share name. <p>When the NFS protocol is used</p> <p>You can use any alphanumeric character, hyphen (-), period (.), forward slash (/), and underscore (_). You cannot specify multi-byte characters. The total number of characters for the directory path, including the file system name, must be no more than 58.</p>

Item	Description
	<p>For example, to create a file share in the <code>/mnt/filesystem01/share01</code> directory of the <code>filesystem01</code> file system, specify <code>share01</code>. The path cannot contain symbolic links.</p> <p>You can leave the path blank to make the <code>/mnt/filesystem01</code> file system itself a file share.</p> <p>The shared directory must be unique in the cluster. Note that the directory names <code>.conflict</code>, <code>.conflict_longpath</code>, <code>.snaps</code>, <code>.history</code> and <code>.lost+found</code> cannot be specified, and the directory names <code>.arc</code>, <code>.system_gi</code>, <code>.system_reorganize</code>, <code>.backupupdates</code>, <code>.temp_backupupdates</code>, and <code>lost+found</code> cannot be specified directly under a file system. The path cannot contain symbolic links. A forward slash or space specified at the end of the string will be removed.</p> <p>This item is not displayed if you create a read-write-content-sharing file system or home-directory-roaming file system. The mount point is automatically specified as the shared directory.</p>
Protocol	<p>Select the protocol to be used in the file share.</p> <p>CIFS (for Windows® clients) Select this option to use the CIFS protocol.</p> <p>NFS (for UNIX clients) Select this option to use the NFS protocol.</p> <p>CIFS, NFS Select this option to use the CIFS protocol and the NFS protocol.</p> <p>If you create a file share in a home-directory-roaming file system, you cannot change CIFS (for Windows® clients), which is selected by default.</p>
Enable share quota ^{#1}	<p>Select the Yes check box when managing the share capacity (setting the subtree quota) by specifying the capacity of the file share (the block capacity that can be used). This check box can be selected if the quota functionality for the file system is enabled.</p> <p>Use existing quota Select this option if the current capacity settings are to be used.</p> <p>Set/overwrite quota Select this option if the capacity is to be specified. In the Total text box, specify a value that is larger than the Used value and is smaller than the File system capacity not allocated to shares value. If MB is selected as the unit, specify an integer. If a unit other than MB is selected, you can specify a value with a maximum of two decimal places.</p> <p>For notes on setting this item and the action to be taken if the setting fails, see Change Share Quota dialog box on page C-19.</p> <p>This item is not displayed if you create a read-write-content-sharing file system or home-directory-roaming file system.</p>

Item	Description
<p>Use namespace</p>	<p>Select Yes to add a file share to a directory directly below the mount point of the file system, and then allocate the HCP namespace to the added share.</p> <p>If Off is specified for Content sharing, specify the following items:</p> <ul style="list-style-type: none"> • Namespace name Specify a migration-destination namespace name of no more than six characters that you want to add to the end of the file share name. You can use alphanumeric characters and hyphens (-). You cannot, however, use a hyphen (-) as the last character. • Quota Specify the hard quota that you want to allocate to the namespace. Specify a value smaller than the Tenant hard quota value. • Synchronize the file share capacity with the namespace quota^{#1} To limit the usage capacity per share based on the hard quota of the migration-destination namespace, select the Yes check box. This check box can be selected if the quota functionality for the file system is enabled. When the Yes check box is selected, the value specified in Quota becomes the maximum value that can be used in the share.
<p>Export point owner</p>	<p>Specify the permission of the shared directory. The owner and owner group of the mount point are set to <code>root</code>.</p> <p>Use existing directory as is Select this option to use an existing directory and the permissions inherited from the existing directory for the shared directory.</p> <p>Create directory / change directory owner Select this option to use a newly created directory for the shared directory, or use an existing directory and modify the permissions. When the file system to which you are adding the file share is the Advanced ACL type, and ACLs are already set for the shared directory, the existing ACL settings are deleted.</p> <p>- Export point owner user^{#2} Specify the owner of the shared directory. To specify a user registered in user mapping, use the following format: <i>domain-name^{#3}\user-name</i></p> <p>- Export point owner group^{#2} Specify the owner group for the shared directory. To specify a group registered in user mapping, use the following format: <i>domain-name^{#3}\group-name</i></p>

Item	Description
	<p>If you want to reference other HDI data as read-only at the share level, you cannot specify Export point owner user or Export point owner group.</p> <p>This item is not displayed if you create a home-directory-roaming file system.</p>
	<p>#1: You cannot select Enable share quota and Synchronize the file share capacity with the namespace quota at the same time.</p> <p>#2: You cannot specify a Windows domain built-in user or group.</p> <p>#3: If you use the CIFS protocol and Active Directory authentication as the CIFS service authentication mode, specify the value set in Domain name (NetBIOS) in the Active Directory Authentication page of the Access Protocol Configuration dialog box for the domain name in Export point owner user and Export point owner group.</p>

Namespace tab

You can use the **Namespace** tab to specify information about the namespace to be allocated to shares. The information you can specify depends on how HCP data is shared.

Table C-27 Information specified in the Namespace tab in the Add Share dialog box (when content sharing is set to Off)

Item	Description
Namespace-access account	Select Create and specify a password to create an account for accessing the namespace from another HDI system.

Table C-28 Information specified in the Namespace tab in the Add Share dialog box (when content sharing is set to On (Read-Only))

Item	Description
Namespace FQDN	Specify the fully qualified domain name of the namespace that is used for referencing other HDI data as read-only via the linked HCP.
External HCP host name	If the HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the HCP system.
Namespace-access account	<p>Specify the user name and password for the account for accessing the namespace.</p> <p>If you click the Test Connection for Primary button after specifying information, you can check the connection with the HCP system.</p>
Replica	<p>If you are using the HCP replication functionality, select the Use check box.</p> <p>System name</p> <p>Specify the replica HCP system name to Fully Qualified Domain Name.</p>

Item	Description
	<p>External Replica HCP host name</p> <p>If the replica HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the replica HCP system.</p> <p>After specifying the information, click the Test Connection for Replica button to check whether you can connect to the replica HCP system.</p>

Edit File System dialog box

You can edit the file system settings.

To open the **Edit File System** dialog box, select a file system and then click **Edit** from the File Systems window ([File Systems window on page C-33](#)).

Edit File System - filesystem01 [Help]

WORM | Namespace | Advanced

Specify the WORM settings.

*Retention period:

Minimum : Infinite
(Note: If the minimum retention period is [Infinite], then the retention period for files will be infinite.)

day(s) hour(s) minute(s)

Maximum : Infinite
(Note: If the maximum retention period is [Infinite], then the retention period for files can be set to any value equal to or greater than the minimum retention period.)

day(s) hour(s) minute(s)

Auto commit:

Enable: Yes
(Note: Once you enable the auto-commit function, you will no longer be able to disable it.)

Commit mode : Manual Auto

Time until committed : day(s) hour(s) minute(s)
(Note: Once you set the time until committed, you will no longer be able to change it. If you use a namespace and the specified time until committed is longer than the migration execution interval, migration might take a long time.)

Default retention period : Infinite
(Note: If the [Default retention period] is [Infinite], then the automatically committed retention period for files will be infinite.)

day(s) hour(s) minute(s)

Enable rename of empty directories: Yes

* Required field

[OK] [Cancel]

WORM tab

You can use the **WORM** tab to specify a file system's WORM setting. To edit a file system's WORM settings, the file system must be mounted.

Table C-29 Information specified in the WORM tab in the Edit File System dialog box

Item	Description
<p>Retention period</p>	<p>Specify the minimum and maximum retention periods.</p> <p>Minimum</p> <p>Specify the minimum retention period. Specify a value from 0 minutes to 36,500 days in the day(s), hour(s), and minute(s) text boxes. To set an indefinite time period for the minimum, select the Infinite check box.</p> <p>If autocommit is enabled, the value must be equal to or less than the Default retention period in Auto commit. If the Infinite check box is not selected for Default retention period, the Infinite check box cannot be selected for this item.</p> <p>Maximum</p> <p>Specify the maximum retention period. Specify a value from 1 minute to 36,500 days in the day(s), hour(s), and minute(s) text boxes. The value must be no less than Minimum.</p> <p>To set an indefinite time period for the maximum, select the Infinite check box. If the Infinite check box is selected for Minimum, the Infinite check box is automatically selected for this item as well.</p> <p>If autocommit is enabled, the value must be no less than the Default retention period in Auto commit. If the Infinite check box is selected for Default retention period, you cannot change the Maximum setting from Infinite.</p>
<p>Auto commit</p>	<p>Specify the autocommit settings.</p> <p>Enable</p> <p>Select the Yes check box to enable autocommit. Note that if you enable autocommit, you can no longer disable it.</p> <p>Commit mode</p> <p>Selects the mode of the autocommit according to the following radio buttons:</p> <ul style="list-style-type: none"> - Manual <p>Select this button to enable the autocommit in manual mode.</p> <p>In manual mode, files that are specified as read-only files by clients are subject to the autocommit functionality.</p> <ul style="list-style-type: none"> - Auto <p>Select this button to enable the autocommit in auto mode.</p> <p>In auto mode, all ordinary files, except for the system files and files in the system directories, are subject to the autocommit functionality.</p> <p>Time until committed</p> <p>If the Yes check box is selected for Enable, specify how long to wait until files are turned into WORM files. Specify a value from 1 minute to 36,500 days in the day(s),</p>

Item	Description
	<p>hour(s), and minute(s) text boxes. After you have specified the setting, you cannot change it.</p> <p>Default retention period</p> <p>Specify the retention period for the files for which an autocommit has been performed. Specify a value from 1 minute to 36,500 days in the day(s), hour(s), and minute(s) text boxes. The value must be within the range specified by Minimum and Maximum in Retention period.</p> <p>To set an indefinite time period for the retention period, select the Infinite check box. If the Infinite check box is selected for Minimum in Retention period, the Infinite check box is automatically selected for this item as well.</p>
Enable rename of empty directories	Select to allow clients to change the names of empty directories.

Namespace tab

You can use the **Namespace** tab to specify namespace information. The information to be specified depends on the usage of a namespace.

Table C-30 Information specified in the Namespace tab in the Edit File System dialog box (when a namespace is used and content sharing is set to Off)

Item	Description
Namespace-access account ^{#1}	Select Create and specify a password to create an account for accessing the namespace from another HDI system.
Use file version restore	<p>Select Yes to make the past version files (past version directories) migrated to the HCP system available to clients. Additionally, select a radio button to set the method of keeping past-version directories in the <code>.history</code> directory.</p> <p>To allow CIFS clients to view to the <code>.history</code> directory, change the settings for the shared directory so that all files and folders are shown.</p> <p>Custom schedule</p> <p>Select this item to keep past-version directories that use custom scheduling. For details about custom scheduling of the file version restore functionality, see the <i>Installation and Configuration Guide</i>.</p> <p>Keep 15-MINUTE versions for: The oldest past version directory with 15-minute time units (hour <i>n</i>, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. Specify any of the following: 15, 30, 45, and 60.</p> <p>Keep HOURLY versions for: The oldest past version directory with hourly time units (hour <i>n</i>, minutes 00 to 59) is kept for the number of units specified. Specify in the range from 1 to 48.</p>

Item	Description
	<p>Keep DAILY versions for: The oldest past version directory with daily time units (day <i>n</i>, 00:00 to 23:59) is kept for the number of units specified. Specify in the range from 1 to 62.</p> <p>Keep WEEKLY versions for: The oldest past version directory with weekly time units (week <i>n</i>, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. Specify in the range from 1 to 52.</p> <p>Keep MONTHLY versions for: The oldest past version directory with monthly time units (month <i>n</i>, 1st day, 00:00 to <i>last-day</i>, 23:59) is kept for the number of units specified. Specify in the range from 1 to 36.</p> <p>Keep YEARLY versions for: The oldest past version directory with yearly time units (year <i>n</i>, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. Specify in the range from 1 to 100.</p> <p>Period to hold^{#2}</p> <p>Select this item to keep past-version directories in every interval between migrations. Specify the period to keep the past version directories in the range from 1 to 36,500 (in days).</p>
<p>#1: Displayed when the HCP namespace is allocated to the file system.</p> <p>#2: Note that the retention period of past version directories depends on the capacity of the namespace in the migration destination. For information on how to estimate the capacity requirement for a namespace in a migration destination, see the <i>Installation and Configuration Guide</i>.</p>	

Table C-31 Information specified in the Namespace tab in the Edit File System dialog box (when a namespace is used and content sharing is set to On (Read-Only))

Item	Description
External HCP host name[#]	If the HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the HCP system.
Namespace-access account[#]	Specify the user name and password for the account for accessing the namespace. If you click the Test Connection for Primary button after specifying information, you can check the connection with the HCP system.
Replica[#]	If you are using the HCP replication functionality, select the Use check box. System name Specify the replica HCP system name to Fully Qualified Domain Name. External Replica HCP host name If the replica HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network,

Item	Description
	<p>specify the host name or IP address that has been made external and is used to connect to the replica HCP system.</p> <p>After specifying the information, click the Test Connection for Replica button to check whether you can connect to the replica HCP system.</p>
#: Displayed when the HCP namespace is allocated to the file system.	

Table C-32 Information specified in the Namespace tab in the Edit File System dialog box (when a namespace is used and content sharing is set to On (Read/Write))

Item	Description
Use file version restore	<p>Select Yes to make the past version files (past version directories) migrated to the HCP system available to clients. Additionally, select a radio button to set the method of keeping past-version directories in the <code>.history</code> directory.</p> <p>To allow CIFS clients to view to the <code>.history</code> directory, change the settings for the shared directory so that all files and folders are shown.</p> <p>Custom schedule</p> <p>Select this item to keep past-version directories that use custom scheduling. For details about custom scheduling of the file version restore functionality, see the <i>Installation and Configuration Guide</i>.</p> <p>Keep 15-MINUTE versions for: The oldest past version directory with 15-minute time units (hour <i>n</i>, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. Specify any of the following: 15, 30, 45, and 60.</p> <p>Keep HOURLY versions for: The oldest past version directory with hourly time units (hour <i>n</i>, minutes 00 to 59) is kept for the number of units specified. Specify in the range from 1 to 48.</p> <p>Keep DAILY versions for: The oldest past version directory with daily time units (day <i>n</i>, 00:00 to 23:59) is kept for the number of units specified. Specify in the range from 1 to 62.</p> <p>Keep WEEKLY versions for: The oldest past version directory with weekly time units (week <i>n</i>, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. Specify in the range from 1 to 52.</p> <p>Keep MONTHLY versions for: The oldest past version directory with monthly time units (month <i>n</i>, 1st day, 00:00 to <i>last-day</i>, 23:59) is kept for the number of units specified. Specify in the range from 1 to 36.</p> <p>Keep YEARLY versions for: The oldest past version directory with yearly time units (year <i>n</i>, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. Specify in the range from 1 to 100.</p> <p>Period to hold#</p>

Item	Description
	Select this item to keep past-version directories in every interval between migrations. Specify the period to keep the past version directories in the range from 1 to 36,500 (in days).
#: Note that the retention period of past version directories depends on the capacity of the namespace in the migration destination. For information on how to estimate the capacity requirement for a namespace in a migration destination, see the <i>Installation and Configuration Guide</i> .	

Table C-33 Information specified in the Namespace tab in the Edit File System dialog box (when a namespace is used and content sharing is set to Home directory)

Item	Description
Use file version restore	<p>Select Yes to make the past version files (past version directories) migrated to the HCP system available to clients. Additionally, select a radio button to set the method of keeping past-version directories in the <code>.history</code> directory.</p> <p>To allow CIFS clients to view to the <code>.history</code> directory, change the settings for the shared directory so that all files and folders are shown.</p> <p>Custom schedule</p> <p>Select this item to keep past-version directories that use custom scheduling. For details about custom scheduling of the file version restore functionality, see the <i>Installation and Configuration Guide</i>.</p> <p>Keep 15-MINUTE versions for: The oldest past version directory with 15-minute time units (hour <i>n</i>, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. Specify any of the following: 15, 30, 45, and 60.</p> <p>Keep HOURLY versions for: The oldest past version directory with hourly time units (hour <i>n</i>, minutes 00 to 59) is kept for the number of units specified. Specify in the range from 1 to 48.</p> <p>Keep DAILY versions for: The oldest past version directory with daily time units (day <i>n</i>, 00:00 to 23:59) is kept for the number of units specified. Specify in the range from 1 to 62.</p> <p>Keep WEEKLY versions for: The oldest past version directory with weekly time units (week <i>n</i>, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. Specify in the range from 1 to 52.</p> <p>Keep MONTHLY versions for: The oldest past version directory with monthly time units (month <i>n</i>, 1st day, 00:00 to <i>last-day</i>, 23:59) is kept for the number of units specified. Specify in the range from 1 to 36.</p> <p>Keep YEARLY versions for: The oldest past version directory with yearly time units (year <i>n</i>, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. Specify in the range from 1 to 100.</p>

Item	Description
	<p>Period to hold[#]</p> <p>Select this item to keep past-version directories in every interval between migrations. Specify the period to keep the past version directories in the range from 1 to 36,500 (in days).</p>
<p>[#]: Note that the retention period of past version directories depends on the capacity of the namespace in the migration destination. For information on how to estimate the capacity requirement for a namespace in a migration destination, see the <i>Installation and Configuration Guide</i>.</p>	

Table C-34 Information specified in the Namespace tab in the Edit File System dialog box (when a namespace is not used)

Item	Description
Namespace type	<p>Specify how to link to the HCP system.</p> <p>File system</p> <p>The file system is linked to the HCP system at the file system level.</p> <p>Subtree</p> <p>The file system is linked to the HCP system at the share level.</p> <p>Note, however, that you cannot select Subtree if an entire file system is shared.</p> <p>None</p> <p>An HCP namespace is not used.</p> <p>Only Off can be specified for Content sharing. To link to the HCP system at the file system level, specify the hard quota that you want to allocate to the namespace for Quota. Specify a value smaller than the Tenant hard quota value.</p>
Migration schedule	<p>Start date</p> <p>Specify the date for the first migration in the format of YYYY-MM-DD.</p> <p>Interval</p> <p>Specify the interval between migrations.</p> <p>Start time</p> <p>Specify the migration start time.</p> <p>Maximum duration</p> <p>Specify the period for continuing migration processing (0 to 999 hours). If you do not want to limit the time, leave the entry blank or specify 0.</p>
Namespace-access account^{#1}	<p>Select Create and specify a password to create an account for accessing the namespace from another HDI system.</p>
Use file version restore	<p>Select Yes to make the past version files (past version directories) migrated to the HCP system available to</p>

Item	Description
	<p>clients. Additionally, select a radio button to set the method of keeping past-version directories in the <code>.history</code> directory.</p> <p>To allow CIFS clients to view to the <code>.history</code> directory, change the settings for the shared directory so that all files and folders are shown.</p> <p>Custom schedule</p> <p>Select this item to keep past-version directories that use custom scheduling. For details about custom scheduling of the file version restore functionality, see the <i>Installation and Configuration Guide</i>.</p> <p>Keep 15-MINUTE versions for: The oldest past version directory with 15-minute time units (hour <i>n</i>, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. Specify any of the following: 15, 30, 45, and 60.</p> <p>Keep HOURLY versions for: The oldest past version directory with hourly time units (hour <i>n</i>, minutes 00 to 59) is kept for the number of units specified. Specify in the range from 1 to 48.</p> <p>Keep DAILY versions for: The oldest past version directory with daily time units (day <i>n</i>, 00:00 to 23:59) is kept for the number of units specified. Specify in the range from 1 to 62.</p> <p>Keep WEEKLY versions for: The oldest past version directory with weekly time units (week <i>n</i>, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. Specify in the range from 1 to 52.</p> <p>Keep MONTHLY versions for: The oldest past version directory with monthly time units (month <i>n</i>, 1st day, 00:00 to <i>last-day</i>, 23:59) is kept for the number of units specified. Specify in the range from 1 to 36.</p> <p>Keep YEARLY versions for: The oldest past version directory with yearly time units (year <i>n</i>, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. Specify in the range from 1 to 100.</p> <p>Period to hold^{#2}</p> <p>Select this item to keep past-version directories in every interval between migrations. Specify the period to keep the past version directories in the range from 1 to 36,500 (in days).</p>
	<p>#1: Displayed when the HCP namespace is allocated to the file system.</p> <p>#2: Note that the retention period of past version directories depends on the capacity of the namespace in the migration destination. For information on how to estimate the capacity requirement for a namespace in a migration destination, see the <i>Installation and Configuration Guide</i>.</p>

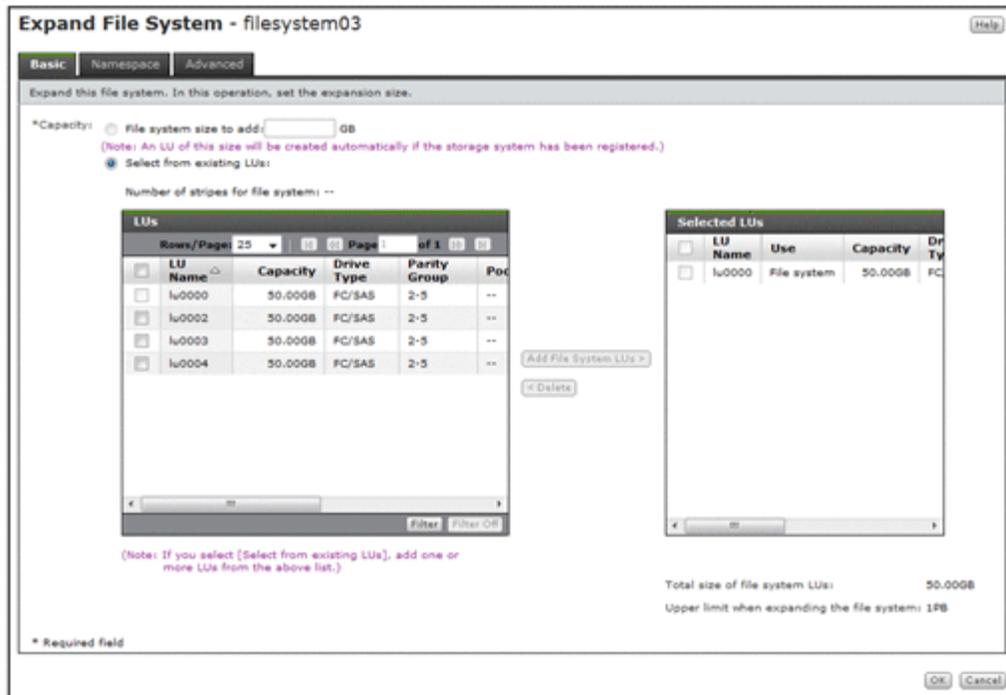
Advanced tab

To enable CIFS bypass traverse checking, select **Enable** for **CIFS bypass traverse checking**.

Expand File System dialog box

If a file system is created by using Volume Manager, you can use the **Expand File System** dialog box to expand the capacity of the file system.

To open the **Expand File System** dialog box, select the target file system in the File Systems window ([File Systems window on page C-33](#)), and then click **Expand**.



Basic tab

You can use the **Basic** tab to specify the basic attributes related to the file system.

Table C-35 Information specified in the Basic tab in the Expand File System dialog box

Item	Description
Capacity	<p>Specify the capacity of the LUs to be added to the file system. The total expanded capacity must be no more than 1 PB. Note that, depending on the capacity of the current file system, the expandable range might be less than 1 PB.</p> <p>Note that, in the following cases, you can select Select from existing LUs only:</p>

Item	Description
	<ul style="list-style-type: none"> The file system is in a striped configuration. Model and Serial Number of the LUs used for the file system are different from those of the storage system for the registered controller. <p>File system size to add[#]</p> <p>Select this to automatically create an LU to be added to the file system. Specify the size of the LU in the text box in gigabytes as an integer in the range from 1 to 1,024.</p> <p>Select from existing LUs</p> <p>Select this to add existing LUs to the file system.</p> <p>Because part of the area is used as the management area in each LU, the total capacity of the LUs differs from the capacity that can be used for the file system.</p> <p>In the LUs area, capacities shown in GB, TB, or PB are rounded to the nearest two decimal places. Take this into account when calculating the total capacity.</p> <p>A hash mark (#) is displayed for LUs that are in an external storage system.</p> <p>- Add File System LUs ></p> <p>In the LUs area, select the LUs you want to add to the file system, and then click this button. Each LU you select must have a capacity of at least 160 MB.</p> <p>If the file system is in a striping configuration, select the same number of LUs (that have the same capacity) as the number of stripes. Striping will be performed in the order the LUs are selected.</p> <p>- Add Work Space LUs ></p> <p>In the LUs area, select the LUs you want to add to the work space, and then click this button. The capacity of each selected LU must be equal to or larger than 33 MB. You can select the maximum of 128 LUs, including the ones already being used. The recommended value for the capacity of the work space differs depending on the capacity of the file system. For details about the recommended values for the capacity of the work space, see the <i>Installation and Configuration Guide</i>.</p> <p>- < Delete</p> <p>Click this button to delete LUs from Selected LUs.</p> <p>For details about how to create and allocate LUs, see the <i>Installation and Configuration Guide</i>.</p>
	<p>#: This item can only be used when all of the following conditions are met:</p> <ul style="list-style-type: none"> The storage system is a Hitachi AMS2000 or HUS100 series storage system and the IP addresses of both controllers are registered on the management server. The LUN Manager functionality is enabled for the storage system. The storage system is not made up of only pools. <p>If there is insufficient space in the existing RAID groups, a RAID5 group (15D+1P) or a RAID6 group (15D+2P) is created, depending on the RAID groups supported by the storage system. However, if 3 to 15 disk drives, in the case of RAID5, or 4 to 16 disk drives, in the case of RAID6, are available, a RAID group will be created using all of</p>

Item	Description
	those disk drives. Note that RAID5 groups are created in storage systems that support both RAID5 and RAID6.

Namespace tab

To expand the namespace capacity allocated to a file system, you can use the **Namespace** tab to specify the new capacity for **Allocate quota**. The value must be equal to or more than the capacity being used.

Advanced tab

File System subtab

For **Maximum capacity for i-nodes**, you can specify the maximum percentage of space within the expanded file system that can be used for an inode, as an integer from 1 to 100. The maximum capacity that can be used as an inode is 1 TB.

Mount File System dialog box

You can use the **Mount File System** dialog box to re-mount a file system that was temporarily unmounted.

The file system will be mounted at the following mount point:

/mnt/file-system-name



Note:

- If you unmount and then re-mount a file system, its previous settings are not applied. Check the attributes that you want to set. When remounting a file system, if you enable the quota function for a file system for which you had previously disabled the quota function, mount processing will take a long time to complete.
- The ACL type of existing directories and files in the file system are converted in the background, and the processing result is sent by an SNMP trap or email. It takes approximately 10 minutes for 100,000 files to be converted.

However, the processing result might not be reported (for example, because a failover or OS error occurred). If the conversion processing fails or if the conversion result is not sent (for example, because a failover or OS error occurred), retry the ACL type conversion by running the `fsctl` command.

To open the **Mount File System** dialog box, select the target file system in the File Systems window ([File Systems window on page C-33](#)), and then click **Mount**.

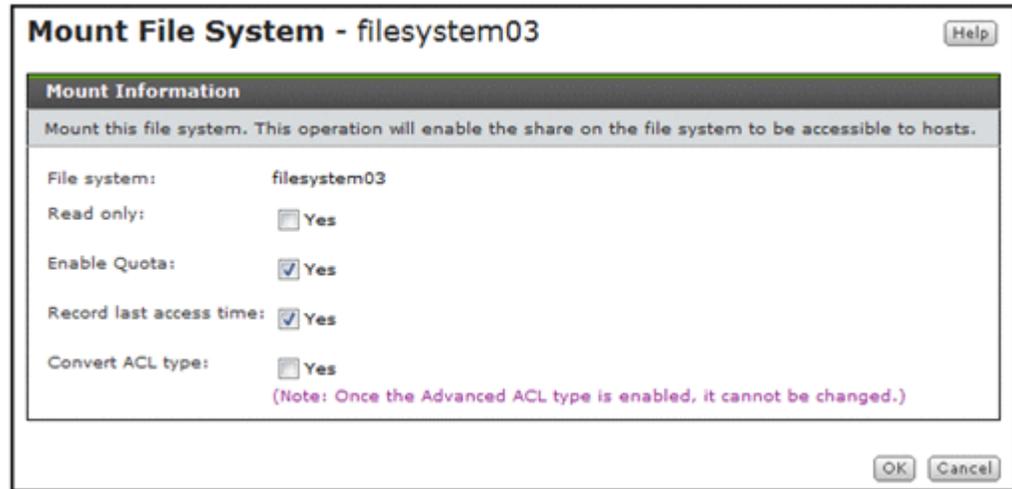


Table C-36 Information specified in the Mount File System dialog box

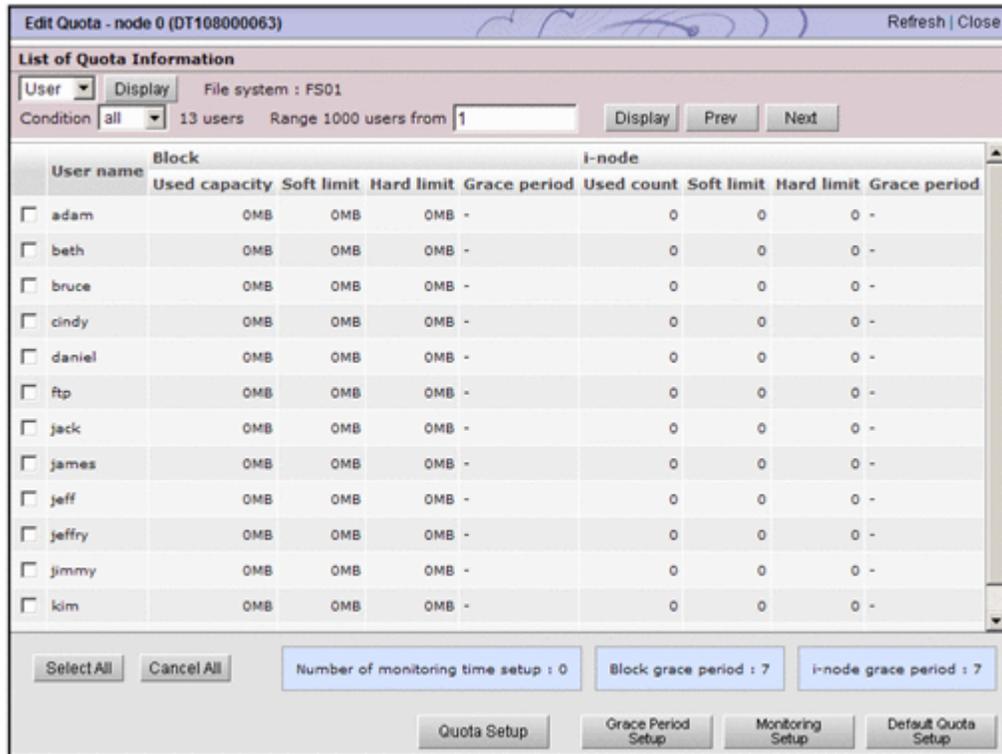
Item	Description
Read only	Select this to mount the file system as read-only.
Enable Quota	Select this to enable the quota functionality or manage the capacity of shares created in the file system.
Record last access time	Select this to update the last access time (<i>atime</i>) when a client accesses a file in the file system.
Convert ACL type	Select this to convert the file system from the Classic ACL type to the Advanced ACL type. Note that you cannot subsequently change the file system back to Classic ACL. Leave the file system type as Classic ACL if it is to be used primarily for NFS shares. When a file system is converted, its directories and files are also converted from Classic ACL to Advanced ACL. This item cannot be selected for a WORM file system.
Note: You cannot select Read only if Enable Quota , Record last access time , or Convert ACL type is selected.	

Edit Quota dialog box

You can use the **Edit Quota** dialog box to manage quota information for each file system.

You can use commands to manage subtree quotas.

To open the **Edit Quota** dialog box, select the target file system in the File Systems window ([File Systems window on page C-33](#)), and then click **Edit User/Group Quota**. After the **Edit Quota** dialog box is shown, the **List of Quota Information** page appears.



List of Quota Information page

You can use the **List of Quota Information** page to view the quota information for a user or group for which the target file system has been set. From the drop-down list on the **List of Quota Information** page, select **User** or **Group**, and then click **Display**.



Note: When the HDI system is operating in command operation mode, a message is shown instead of a list of user quota information.

After the **Edit Quota** dialog box is shown, the **List of Quota Information** page appears.

Table C-37 Quota information shown in the List of Quota Information page

Item	Description
User name or Group name	User name or Group name
Block	Block usage by individual user or group Used capacity Block space used. Shown in red if the block space used exceeds the soft limit or reaches the hard limit. The value shown is rounded up to the nearest ones place. Soft limit [#] Soft limit for block usage Hard limit [#]

Item	Description
	<p>Hard limit for block usage</p> <p>Grace period</p> <p>Remaining grace time until a new block can no longer be assigned after the block usage exceeds the soft limit. Shown in one of the following formats:</p> <p><i>n days</i></p> <p>The remaining grace time is 24 hours or longer. For example, <i>1 days</i> appears if there are 24 hours or more, but less than 48 hours remaining.</p> <p><i>n hours</i></p> <p>The remaining grace time is less than 24 hours. The value is shown in orange. For example, <i>0 hours</i> appears if less than 1 hour remains.</p> <p><i>Over</i></p> <p>Either the grace period has expired or block usage has reached the hard limit. <i>Over</i> is shown in red.</p> <p>-</p> <p>The user's block usage is within the soft limit.</p>
i-node	<p>inode usage by individual user or group</p> <p>Used count</p> <p>Number of inodes used. Shown in red if the number of inodes used exceeds the soft limit or reaches the hard limit.</p> <p>Soft limit[#]</p> <p>Soft limit for inode usage.</p> <p>Hard limit[#]</p> <p>Hard limit for inode usage.</p> <p>Grace period</p> <p>Remaining grace time until files can no longer be created after the user's inode usage exceeds the soft limit. Shown in one of the following formats:</p> <p><i>n days</i></p> <p>The remaining grace time is 24 hours or longer. For example, <i>1 days</i> appears if there are 24 hours or more, but less than 48 hours remaining.</p> <p><i>n hours</i></p> <p>The remaining grace time is less than 24 hours. The value is shown in orange. For example, <i>0 hours</i> appears if less than 1 hour remains.</p> <p><i>Over</i></p> <p>Either the grace period has expired or inode usage has reached the hard limit. <i>Over</i> is shown in red.</p> <p>-</p> <p>The user's inode usage is within the soft limit.</p>

Item	Description
Number of monitoring time setup	Number of times per day that quotas are checked
Block grace period	Grace period until a new block can no longer be assigned after the block usage exceeds the soft limit.
i-node grace period	Grace period until files can no longer be created after inode usage exceeds the soft limit.
Note: To show the usage in MB, use the quotaget command. #: 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.	

Table C-38 Operations that can be performed from the List of Quota Information page

Button	Description	See
Quota Setup	Set quotas for the user or group selected.	Quota Setup page on page C-59
Grace Period Setup	Set a grace period.	Grace Period Setup page on page C-60
Monitoring Setup	Set the method of monitoring quota information.	Monitoring Setup page on page C-61
Default Quota Setup	Set the default quota. This button is shown when User is selected from the drop-down list.	Default Quota Setup page on page C-62

When viewing quota information for users, you can specify the information items to be shown in the list.

Filtering information to be shown

Select a filter from the **Condition** drop-down list, and then click **Display**.

all

The quota information for all users.

a to z, A to Z, or 0 to 9

The quota information for users whose names begin with the selected alphanumeric character.

other

The quota information for users whose names begin with a character other than an alphanumeric character.

Operation when the number of users exceeds 1,000

A maximum of 1,000 users can be shown at the same time in the **List of Quota Information** page. If the number of users exceeds 1,000, you can use the following methods to specify the users to be shown.

Range text box

The sequence number of the user who is shown at the beginning of the **List of Quota Information** page.

Specify a value equal to or less than the total number of filtered users, and then click **Display**. This shows 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 **Display**, the value specified in the **Range** text box is ignored and users are shown beginning with the first user.

Prev

Clicking this button shows in sequential order the 1,000 users preceding the users currently shown in the **List of Quota Information** page. If there are fewer than 1,000 users preceding the user shown at the beginning of the **List of Quota Information** page, clicking **Prev** shows 1,000 users beginning with the first user. If the user shown at the beginning of the **List of Quota Information** page is the first user, or if the total number of filtered users is 0, an error message appears when you click **Prev**.

Next

Clicking this button shows in sequential order the 1,000 users following the users currently shown in the **List of Quota Information** page. If the user shown at the end of the **List of Quota Information** page is the last user, or if the total number of filtered users is 0, an error message appears when you click **Next**.

Quota Setup page

You can set quotas for a selected user or group on the **List of Quota Information** page.

To open the **Quota Setup** page, click **Quota Setup** on the **List of Quota Information** page in the **Edit Quota** dialog box ([Edit Quota dialog box on page C-55](#)).

Table C-39 Information specified in the Quota Setup page

Item	Description
Block limits	Specify the block space available to the user(s) or group(s). After entering an integer value in the text box, use the drop-down list to select the unit (MB, GB, or TB).
Soft limit[#]	Set the soft limit.

Item	Description
	<p>Specify a value from 0 to 1,073,741,823 MB, 1,048,575 GB, or 1,023 TB. This value must not exceed the Hard limit setting.</p> <p>Hard limit[#]</p> <p>Set the hard limit. You cannot set a smaller value than already used.</p> <p>Specify a value from 0 to 1,073,741,823 MB, 1,048,575 GB, or 1,023 TB.</p>
i-node limits	<p>Specify the number of inodes available to the user(s) or group(s).</p> <p>Soft limit[#]</p> <p>Set the soft limit.</p> <p>Specify a value from 0 to 4,294,967,295. This value must not exceed the Hard limit setting.</p> <p>Hard limit[#]</p> <p>Set the hard limit. You cannot set a smaller value than already used.</p> <p>Specify a value from 0 to 4,294,967,295.</p>
<p>[#]: If you specify one user or group in the List of Quota Information page, the initial values shown in Soft limit and Hard limit vary depending on whether a quota has been set for the selected user or group.</p> <ul style="list-style-type: none"> • When a quota has been set for the selected user or group: The quota that has been set is shown. • When a quota has not been set for the selected user or group: If you specify a user, and the default quota has been set for the file system, the default quota is shown. If you specify a user and the default quota has not been set, 0 is shown. If you specify a group, 0 is shown. <p>If you specify multiple users or groups, no value is initially shown.</p>	

Grace Period Setup page

You can use the **Grace Period Setup** page to set a grace period. The set grace period applies to all users and groups that use the target file system.

Even if you change the current grace period, the new setting does not apply to the users or groups whose disk drive 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 open the **Grace Period Setup** page, click **Grace Period Setup** on the **List of Quota Information** page in the **Edit Quota** dialog box ([Edit Quota dialog box on page C-55](#)).

Table C-40 Information specified in the Grace Period Setup page

Item	Description
Block grace period	Specify a grace period until a new block can no longer be assigned after the block usage exceeds the soft limit (units: days). Set a value from 1 to 9,999.
i-node grace period	Specify a grace period until files can no longer be created after inode usage exceeds the soft limit (units: days). Set a value from 1 to 9,999.

Monitoring Setup page

You can use the **Monitoring Setup** page to set the method of monitoring quota information.

To open the **Monitoring Setup** page, click **Monitoring Setup** on the **List of Quota Information** page in the **Edit Quota** dialog box ([Edit Quota dialog box on page C-55](#)).

Table C-41 Information specified in the Monitoring Setup page

Item	Description
Monitoring time setup	<p>From the Time to add drop-down list, select a time at which quota information is polled (by hour and minute). You can specify the time in 5-minute units, in the range from 00:00 to 23:55.</p> <p>Click Add 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.</p> <p>To delete a time from the list box, select the time and click Delete.</p> <p>You can set from 0 to 48 daily monitoring times. If omitted, quota monitoring will not be performed.</p>
SNMP notification mode setup	<p>Select the SNMP trap notification mode, in the options, when users or groups that have exceeded the soft limit or grace period are detected.</p> <p>Use a summary notification Select this item to set summary notification mode.</p> <p>Use individual notifications Select this item to set individual notification mode.</p> <p>If more than 100 users or groups have exceeded the soft limit or grace period, individual notification is suppressed and only the number of users or groups that have exceeded the soft limit or grace period is reported to the SNMP manager.</p>

Default Quota Setup page

You can use the **Default Quota Setup** page to set the default quota. The default quota does not apply to users for whom specific quotas have been set.

To open the **Default Quota Setup** page, click **Default Quota Setup** on the **List of Quota Information** page in the **Edit Quota** dialog box ([Edit Quota dialog box on page C-55](#)).

Table C-42 Information specified in the Default Quota Setup page

Item	Description
Default block limits	<p>Specify the block space available to the users. After entering an integer value in the text box, use the drop-down list to select the unit (MB, GB, or TB).</p> <p>Soft limit</p> <p>Set the soft limit.</p> <p>Specify a value from 0 (no soft limit) to 1,073,741,823 MB, 1,048,575 GB, or 1,023 TB. This value must not exceed the Hard limit setting.</p> <p>Hard limit</p> <p>Set the hard limit.</p> <p>Specify a value from 0 (no hard limit) to 1,073,741,823 MB, 1,048,575 GB, or 1,023 TB.</p>
Default i-node limits	<p>Specify the number of inode available to the users.</p> <p>Soft limit</p> <p>Set the soft limit.</p> <p>Specify a value from 0 (no soft limit) to 4,294,967,295. This value must not exceed the Hard limit setting.</p> <p>Hard limit</p> <p>Set the hard limit.</p> <p>Specify a value from 0 (no hard limit) to 4,294,967,295.</p>

file-system window

The *file-system* window shows the usage of a file system and information about the LUs that make up the file system. This window also shows the names of file shares in the file system and the protocol used for each file share.

To open the *file-system* window, in the **Explorer** menu of the Hitachi File Services Manager main window ([Explorer menu on page B-5](#)), select **Resources** and then **File Systems**. In the File Systems window that opens, click a desired file system name.

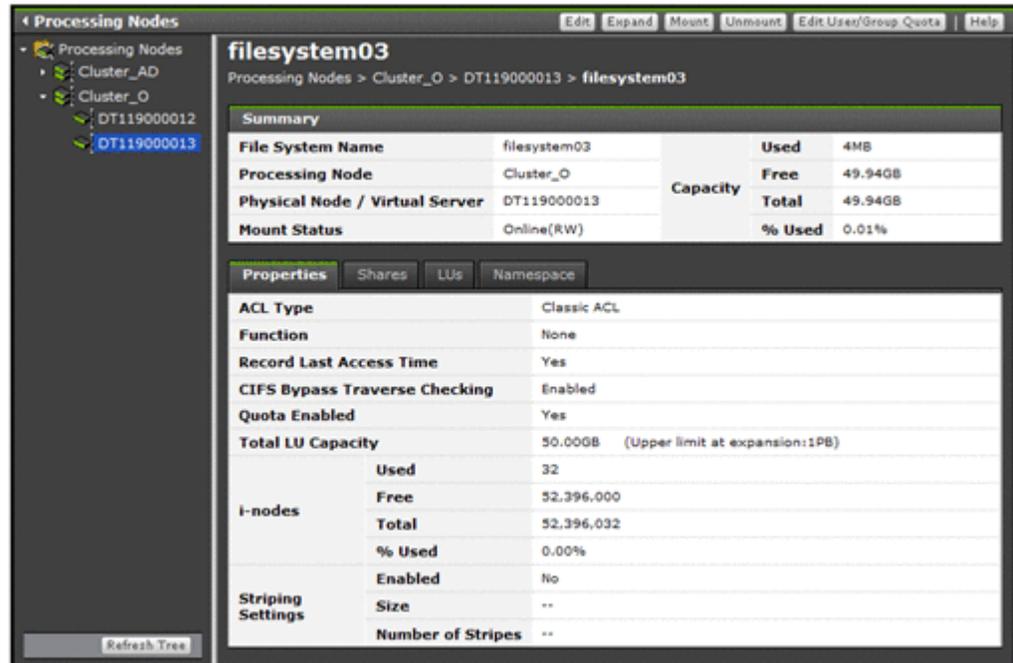


Table C-43 File system operations that can be performed from the file-system window

Button	Function	See
Edit	Edit the file system settings.	Edit File System dialog box on page C-44
Expand	Expand the capacity of a file system as needed.	Expand File System dialog box on page C-52
Mount	Mount a file system.	Mount File System dialog box on page C-54
Unmount	<p>Unmount a file system.</p> <p>Before unmounting a file system, a system administrator must release all file shares in the file system. If Backup Restore is being used, before you unmount the file system, make sure that no backup or restore operations are in progress. Check the connection status between the NDMP server and the backup server, and between the NDMP server and the media server.</p> <p>Notes:</p> <ul style="list-style-type: none"> Unmounting a file system does not delete the data. If a file system is no longer required, it should be deleted rather than unmounted. Unmounting a file system stops the services for that file system. 	N/A

Button	Function	See
Edit User/Group Quota	<p>Manage quota information for each file system.</p> <p>By clicking this button, you can open the Edit Quota dialog box for a specific file system. You can show up to 10 Edit Quota dialog boxes for a physical node at the same time. To close unnecessary Edit Quota dialog boxes, click Close. If the Edit Quota dialog box cannot be opened, quit all Web browsers, and then log on again.</p>	Edit Quota dialog box on page C-55
Note: N/A = Not applicable.		

Table C-44 Information shown in the file-system window

Item	Description		See
Summary	Detailed information about the file system.		Table C-45 Information shown in the Summary of the file-system window on page C-64
Properties	The file system attributes.		Properties tab on page C-66
Shares	Lists the file shares created in the file system.		Shares tab on page C-68
LUs	Information about the LUs that constitute the file system.		N/A
	LUs	Information about LUs.	LUs subtab on page C-70
	Pool	Pool information if virtual LUs are used in the file system.	Pools subtab on page C-72
WORM	Information about a file system's WORM settings. This item is shown only for a WORM file system.		WORM tab on page C-72
Work Space	Information about the work space used for the Active File Migration functionality.		Work Space tab on page C-73
	Work Space LUs	Information about the LUs used by the work space.	Work Space LUs subtab on page C-73
Namespace	Information about the HCP namespace.		Namespace tab on page C-74

Table C-45 Information shown in the Summary of the file-system window

Item	Description
File System Name	The name of the file system.

Item	Description
Processing Node	The name of the processing node (cluster) on which the file system was created.
Physical Node/ Virtual Server	The name of the physical node on which the file system is currently running.
Mount Status	<p>The status of the file system.</p> <p>Online (RW) The file system is mounted with both read and write operations permitted.</p> <p>Online (RO) The file system is mounted as read-only.</p> <p>Unmounted The file system is unmounted.</p> <p>Expanding The file system is being expanded or an error occurred during expansion processing. Wait a while, and then refresh the processing node information. If the status does not change, an error might have occurred during processing. Obtain all the log data, and then inform maintenance personnel.</p> <p>Reclaiming The unused area of the virtual LUs that are used for the file system is being released.</p> <p>Data corrupted The file system is blocked because of an error in the OS or a pool capacity shortage. Take corrective action by referring to the <i>Cluster Troubleshooting Guide</i>.</p> <p>Device error The file system is blocked because of an error in the LU (multiple drive failure). Take corrective action by referring to the <i>Cluster Troubleshooting Guide</i>.</p>
Capacity[#]	<p>The usage of the file system.</p> <p>Used The used capacity of the file system.</p> <p>Free The remaining capacity of the file system.</p> <p>Total The total capacity of the file system.</p> <p>% Used The percentage of the file system capacity in use.</p> <p>If the file system has not been mounted correctly, 0 is shown in all items.</p>

Item	Description
#: The values shown are calculated from the block capacity of the file system. Capacities shown in MB are rounded to the nearest ones place. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.	

Properties tab

You can use the **Properties** tab to show the file system attributes.

Table C-46 Information shown in the Properties tab in the file-system window

Item	Description
ACL Type	<p>The ACL type of the file system.</p> <p>Advanced ACL The file system is the Advanced ACL type.</p> <p>Classic ACL The file system is the Classic ACL type.</p> <p>Unknown Shown when ACL type information cannot be obtained.</p>
Function	<p>The name of the function that is using the file system.</p> <p>None The file system is not being used by another function.</p> <p>Active Migration The file system is used by a function of Active File Migration.</p> <p>WORM Shown for a WORM file system.</p>
Record Last Access Time	<p>Shows whether the last access time (<code>atime</code>) is set to be updated when a client accesses a file in the file system.</p> <p>Yes The last access time (<code>atime</code>) is set to be updated.</p> <p>No The last access time (<code>atime</code>) is not set to be updated.</p>
CIFS Bypass Traverse Checking	<p>Shows whether CIFS bypass traverse checking is enabled.</p> <p>Enabled CIFS bypass traverse checking is enabled.</p> <p>Disabled CIFS bypass traverse checking is disabled.</p>
Quota Enabled	<p>Shows whether the quota function is enabled for the file system.</p> <p>Yes The quota function is enabled.</p> <p>No</p>

Item	Description
	<p>The quota function is disabled.</p> <p>If the LU or the file system is blocked, the status in effect before the failure occurred is shown. Additionally, <code>No</code> is shown after a failure under one of the following conditions:</p> <ul style="list-style-type: none"> • The quota setting was disabled before the failure occurred. • The quota setting was enabled before the failure occurred. However, the status was changed when, for example, an unmount operation was performed after the failure.
Total LU Capacity	<p>The total capacity of the LUs that make up the file system. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.</p> <p>The upper limit for expansion of the file system capacity is also displayed. If the initial capacity of a created file system is less than 32 GB + 16 MB, the maximum capacity after expansion will be less than the displayed value. For details about the initial capacity of a created file system and the maximum capacity after expansion, see the <i>CLI Administrator's Guide</i>.</p>
i-nodes	<p>The inode usage.</p> <p>Used The used inode capacity.</p> <p>Free The free inode capacity.</p> <p>Total The total inode capacity.</p> <p>% Used The percentage of inode capacity in use.</p> <p>If the file system has not been mounted correctly, 0 is shown in all items.</p>
Striping Settings	<p>The striping information.</p> <p>Enabled <code>Yes</code> if the file system is in a striping configuration. <code>No</code> if the file system is not in a striping configuration.</p> <p>Size The stripe size. If the file system is not in a striping configuration, <code>--</code> is shown.</p> <p>Number of Stripes The number of stripes. If the file system is not in a striping configuration, <code>--</code> is shown.</p>
Work Space	<p>The capacity of the work space used for the Active File Migration functionality.</p> <p>Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.</p>
<p>#: The values shown are calculated from the block capacity of the file system. Capacities shown in MB are rounded to the nearest ones place. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.</p>	

Shares tab

You can use the **Shares** tab to view a list of the file shares created in the file system.

Table C-47 Information shown in the Shares tab in the file-system window

Item	Description
Share Name	The name of the share.
Protocol	<p>The names of the protocols used by the file share.</p> <p>CIFS The CIFS protocol is used.</p> <p>NFS The NFS protocol is used.</p> <p>CIFS, NFS The CIFS and NFS protocols are used.</p>
Use Namespace	<p>Displays whether the HCP namespace is allocated to the share.</p> <p>Yes Displayed when the HCP namespace is allocated to the share.</p> <p>No Displayed when the HCP namespace is not allocated to the share.</p> <p>If a file system is not linked to the HCP system at the share level, two hyphens (--) are displayed.</p>
Content Sharing	<p>Displays how data is shared with other HDI systems via the linked HCP.</p> <p>Off Displayed if data is not synchronized with other HDI systems</p> <p>On (Read-Only) Displayed if other HDI data is referenced as read-only</p> <p>If a file system is not linked to the HCP system at the share level, two hyphens (--) are displayed.</p>
CIFS Share Name	The name of the CIFS share when the CIFS protocol is used in the file share. This item is left as blank if the CIFS protocol is not used.
Capacity^{#1}	<p>The usage of the file system. If the capacity of the file share is managed, the usage of the file share is shown.^{#2}</p> <p>Used The used capacity of the file system or file share.</p> <p>Free The remaining capacity of the file system or file share.</p> <p>Total The total capacity of the file system or file share.</p> <p>% Used</p>

Item	Description
	The percentage of the file system or file share capacity in use. If the file system has not been mounted correctly, 0 is shown in all items.
Capacity Management Directory	The directory subject to capacity management is shown. If the capacity of the file share is not managed, the file system name is shown.
<p>#1: The values shown are calculated from the block capacity of the file system. Capacities shown in MB are rounded to the nearest ones place. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.</p> <p>#2: When the capacity of the file share is limited based on the hard quota of the migration-destination namespace, "--" will be displayed.</p>	

Table C-48 File share operations that can be performed from the Shares tab in the file-system window

Button	Function	See
Add Share	Add a file share to the existing file system. Note that a file share cannot be added if the read-write-content-sharing file system or home-directory-roaming file system and a file share has already been created.	Add Share dialog box on page C-38
Release Share	Release an unnecessary file share. Notes: <ul style="list-style-type: none"> The shared directory is not deleted even after the file share is released. When the CIFS protocol and NFS protocol are being used, both are released. Edit the file share attributes if you want to release only one protocol. For details about editing file share attributes, see Basic tab on page C-8. If the CIFS service configuration definition settings do not allow the CIFS share settings to be automatically reloaded and you released a CIFS share during degenerated operation, to enable the CIFS share settings, perform a failback operation, and then restart the CIFS services on both nodes. For details about how to carry out perform a failback operation, see Browse Cluster Status page on page C-271. For details about how to restart a CIFS service, see List of Services page on page C-218. 	N/A
Edit Share	Edit file share attributes such as the protocol and access permissions.	Edit Share dialog box on page C-7

Button	Function	See
Change Share Quota	Change the quota of the file share immediately under the mount point.	Change Share Quota dialog box on page C-19
Note: N/A = Not applicable.		

LUs tab

You can use the **LUs** tab to view information about the LUs that constitute the file system.

LUs subtab

You can use the **LUs** subtab to view information about LUs.

Table C-49 Information shown on the LUs subtab of the LU tab in the file-system window

Item	Description
LU Name	Lists the names of the LUs that constitute the file system. When an LU resides on an external storage system, a hash mark (#) is attached at the end of the LU name (If an error has occurred on the FC path or the LU path from both nodes, the hash mark is not shown).
Capacity	The LU capacity. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places. 0MB appears when: <ul style="list-style-type: none"> An LU error has occurred. An error has occurred on the FC path from both nodes. An error has occurred on the LU path from both nodes.
Used Capacity	The capacity allocated to a virtual LU. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places. If the LU is not a virtual LU or information cannot be obtained, -- is shown. Operations such as refreshing processing node information and creating file systems sometimes temporarily allocate capacity to virtual LUs. In this case, allocated capacities might also be shown for unused virtual LUs.
Drive Type	The LU drive type. FC/SAS Indicates an FC or SAS drive. SAS7K Indicates a SAS 7.2K drive. SATA

Item	Description
	<p>Indicates a SATA drive.</p> <p>SSD</p> <p>Indicates a solid-state drive.</p> <p>-- is shown if:</p> <ul style="list-style-type: none"> • The information cannot be obtained because an error occurred. • The LU is a virtual LU for VSP G1000, VSP G200, G400, G600, G800, VSP F400, F600, F800, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM. • The LU is a virtual LU that uses HUS100 series Dynamic Tiering. • The LU is in use, and an error has occurred on the FC paths from both nodes. • The LU is in use, and an error has occurred on the LU paths from both nodes. • The LU resides on an external storage system.
Parity Group#	<p>The parity group to which the LU belongs.</p> <p>If the LU is a virtual LU, if the LU resides on an external storage system, or if information cannot be obtained -- is shown.</p>
Pool#	<p>The number of the pool to which the LU belongs.</p> <p>If the LU is not a virtual LU or information cannot be obtained, -- is shown.</p>
Stripe Group Order	<p>The stripe group number and the LU order in the stripe group in the following format:</p> <p><i>group-number-order-in-the-group</i></p> <p>-- is shown if the file system is not in a striping configuration.</p>
Model	<p>The model of the storage system on which the LU resides.</p>
Serial Number	<p>The serial number of the storage system on which the LU resides. When the LU is on an external storage system, the information shown relates to the mapped storage system.</p>
Volume#	<p>The LDEV number of the LU.</p> <p>When the LUN Expansion functionality is being used, the ID of the volume at the head of the linked volumes is shown.</p>
Target	<p>The target to which the path to the LU belongs.</p> <p>-- is shown if:</p> <ul style="list-style-type: none"> • The LU is in use, and an error has occurred on the FC path from the node shown. • The LU is in use, and an error has occurred on the LU path from the node shown.
<p>#: If Hitachi Storage Navigator Modular 2 is linked to, clicking the item name opens the Hitachi Storage Navigator Modular 2 window. For details about how to use the window, see the applicable Hitachi Storage Navigator Modular 2 manual.</p>	

Pools subtab

You can use the **Pools** subtab to view pool information if the virtual LUs are used in the file system.

Table C-50 Information shown on the Pools subtab on the LUs tab in the file-system window

Item	Description
Pool	The number of the pool to which the virtual LUs used in the file system belong.
Model	The model of the storage system on which the pool resides.
Serial Number	The serial number of the storage system on which the pool resides. If the pool resides on an external storage system, information about the mapped storage system is shown.
Free Space[#]	The amount of free space in the pool. If the storage system is a VSP G1000, VSP G200, G400, G600, G800, VSP F400, F600, F800, Virtual Storage Platform, Universal Storage Platform V/VM storage system, or HUS VM, -- is shown.
Total Capacity[#]	The total capacity of the pool. If the storage system is a VSP G1000, VSP G200, G400, G600, G800, VSP F400, F600, F800, Virtual Storage Platform, Universal Storage Platform V/VM storage system, or HUS VM, -- is shown.
Capacity for This Instance[#]	The capacity available for each instance.
	Used Capacity The amount of pool space allocated to the file system.
	LU Total The total capacity of the LUs in the file system.
[#] : Capacities shown in MB are rounded to the nearest integer. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.	

WORM tab

You can use the **WORM** tab to view information about a file system's WORM settings. This item is shown only for a WORM file system.

Table C-51 Information shown in the WORM tab in the file-system window

Item	Description
Retention Period	The retention period settings.
	Minimum The minimum retention period.
	Maximum The maximum retention period.
Auto Commit	The autocommit settings.
	Enabled Shows whether autocommit is enabled. Yes

Item	Description	
		Autocommit is enabled. No Autocommit is disabled.
	Commit Mode	Displays the commit mode of the autocommit. Manual Autocommit is in manual mode. Auto Autocommit is in auto mode. -- Autocommit is disabled.
	Time Until Committed	Displays how long to wait until files are turned into WORM files. -- is shown when the autocommit setting is disabled.
	Default Retention Period	The retention period set for files for which an autocommit was performed. -- is shown when the autocommit setting is disabled.
Enable Rename of Empty Directories	Shows whether to allow clients to change the names of empty directories. Yes Changes are allowed. No Changes are not allowed.	
Note: The information in the WORM tab is shown when the file system is mounted. -- is shown for each item when the file system is not mounted. <i>Unknown</i> is shown for each item when the information cannot be obtained.		

Work Space tab

You can use the **Work Space** tab to view information about the work space used for the Active File Migration functionality.

Work Space LUs subtab

You can use the **Work Space LUs** subtab to view information about LUs being used for the work space.

Table C-52 Information shown on the Work Space LUs subtab of the Work Space tab in the file-system window

Item	Description
LU Name	Lists the names of the LUs that make up the work space.
Capacity	The LU capacity.
Used Capacity	The capacity allocated to a virtual LU.
Drive Type	The LU drive type.
Parity Group	The parity group to which the LU belongs.
Pool	The number of the pool to which the LU belongs.
Stripe Group Order	The stripe group number and the LU order within the group.
Model	The model of the storage system on which the LU resides.
Serial Number	The serial number of the storage system on which the LU resides.
Volume	The LDEV number of the LU.
Target	The target to which the path to the LU belongs.

Namespace tab

You can use the **Namespace** tab to view information about the HCP namespace. The information shown depends on the content sharing settings.

Table C-53 Information shown in the Namespace tab in the file-system window (when content sharing is set to Off)

Item	Description
Namespace Type	Displays how the file system is linked to the HCP system. <i>File System</i> The file system is linked to the HCP system at the file system level. <i>Subtree</i> The file system is linked to the HCP system at the share level.
Content Sharing	Shows <i>Off</i> .
Target Namespace[#]	The HCP namespace to which data is migrated.
Namespace-access Account[#]	The user name of the account for accessing the namespace from another HDI system.
File Version Restore	The setting for making the past version files (past version directories) migrated to the HCP system available to clients is displayed. In Use

Item	Description
	<p>Whether the past versions are to be made available to clients is displayed.</p> <p>Period to Hold</p> <p>The period to keep the past version directories in the <code>.history</code> directory is displayed.</p> <p>This item is only displayed when custom scheduling is not used.</p> <p>Custom Schedule</p> <p>The custom schedule setting is displayed.</p> <p>This item is only displayed when custom scheduling is used.</p> <p>15-MINUTE Versions: The value specified for a custom schedule in 15-minute units is displayed (unit: minutes). If a custom schedule in 15-minute units is disabled, two hyphens (--) are displayed.</p> <p>HOURLY Versions: The value specified for an hourly custom schedule is displayed (unit: hours). If an hourly custom schedule is disabled, two hyphens (--) are displayed.</p> <p>DAILY Versions: The value specified for a daily custom schedule is displayed (unit: days). If a daily custom schedule is disabled, two hyphens (--) are displayed.</p> <p>WEEKLY Versions: The value specified for a weekly custom schedule is displayed (unit: weeks). If a weekly custom schedule is disabled, two hyphens (--) are displayed.</p> <p>MONTHLY Versions: The value specified for a monthly custom schedule is displayed (unit: months). If a monthly custom schedule is disabled, two hyphens (--) are displayed.</p> <p>YEARLY Versions: The value specified for a yearly custom schedule is displayed (unit: years). If a yearly custom schedule is disabled, two hyphens (--) are displayed.</p>
#: Displayed when the HCP namespace is allocated to the file system.	

Table C-54 Information shown in the Namespace tab in the file-system window (when content sharing is set to On (Read-Only))

Item	Description
Namespace Type	<p>Displays how the file system is linked to the HCP system.</p> <p>File System</p> <p>The file system is linked to the HCP system at the file system level.</p> <p>Subtree</p> <p>The file system is linked to the HCP system at the share level.</p>

Item	Description
Content Sharing	Shows On (Read-Only).
Target Namespace[#]	The namespace that is used for referencing other HDI data as read-only via the linked HCP.
External HCP Host Name[#]	The host name or IP address that has been made external and is used to connect to the HCP system is displayed.
Namespace-access Account[#]	The user name of the account for accessing the namespace.
Replica System Name[#]	If you are using the HCP replication functionality, the system name is displayed.
External Replica HCP Host Name[#]	The host name or IP address that has been made external and is used to connect to the replica HCP system is displayed.
#: Displayed when the HCP namespace is allocated to the file system.	

Table C-55 Information shown in the Namespace tab in the file-system window (when content sharing is set to On (Read/Write))

Item	Description
Namespace Type	Displays File System.
Content Sharing	Displays On (Read/Write).
Target Namespace	The namespace for the HCP system to which data will be migrated.
Namespace-access Account	The user name of the account for accessing the namespace.
File Version Restore	<p>The setting for making the past version files (past version directories) migrated to the HCP system available to clients is displayed.</p> <p>In Use</p> <p>Whether the past versions are to be made available to clients is displayed.</p> <p>Period to Hold</p> <p>The period to keep the past version directories in the <code>.history</code> directory is displayed.</p> <p>This item is only displayed when custom scheduling is not used.</p> <p>Custom Schedule</p> <p>The custom schedule setting is displayed.</p> <p>This item is only displayed when custom scheduling is used.</p> <p>15-MINUTE Versions: The value specified for a custom schedule in 15-minute units is displayed (unit: minutes). If a custom schedule in 15-minute units is disabled, two hyphens (--) are displayed.</p>

Item	Description
	<p>HOURLY Versions: The value specified for an hourly custom schedule is displayed (unit: hours). If an hourly custom schedule is disabled, two hyphens (--) are displayed.</p> <p>DAILY Versions: The value specified for a daily custom schedule is displayed (unit: days). If a daily custom schedule is disabled, two hyphens (--) are displayed.</p> <p>WEEKLY Versions: The value specified for a weekly custom schedule is displayed (unit: weeks). If a weekly custom schedule is disabled, two hyphens (--) are displayed.</p> <p>MONTHLY Versions: The value specified for a monthly custom schedule is displayed (unit: months). If a monthly custom schedule is disabled, two hyphens (--) are displayed.</p> <p>YEARLY Versions: The value specified for a yearly custom schedule is displayed (unit: years). If a yearly custom schedule is disabled, two hyphens (--) are displayed.</p>

Table C-56 Information shown in the Namespace tab in the file-system window (when content sharing is set to Home directory)

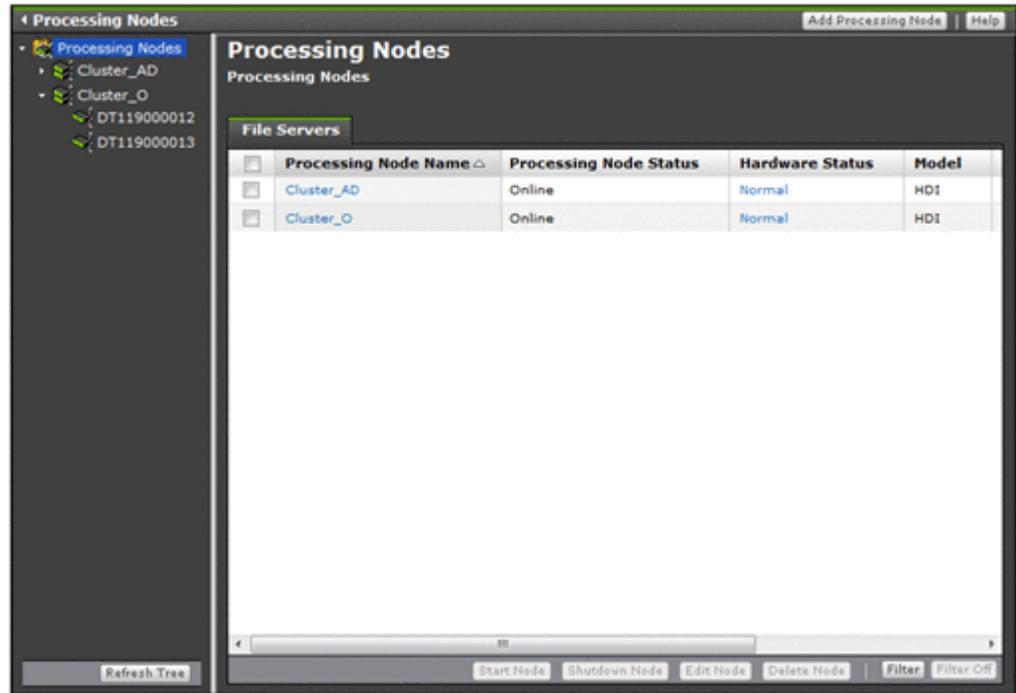
Item	Description
Namespace Type	Displays File System.
Content Sharing	Displays Home directory.
Target Namespace	The namespace for the HCP system to which data will be migrated.
File Version Restore	<p>The setting for making the past version files (past version directories) migrated to the HCP system available to clients is displayed.</p> <p>In Use</p> <p>Whether the past versions are to be made available to clients is displayed.</p> <p>Period to Hold</p> <p>The period to keep the past version directories in the .history directory is displayed.</p> <p>This item is only displayed when custom scheduling is not used.</p> <p>Custom Schedule</p> <p>The custom schedule setting is displayed.</p> <p>This item is only displayed when custom scheduling is used.</p> <p>15-MINUTE Versions: The value specified for a custom schedule in 15-minute units is displayed (unit: minutes). If a custom schedule in 15-minute units is disabled, two hyphens (--) are displayed.</p>

Item	Description
	<p>HOURLY Versions: The value specified for an hourly custom schedule is displayed (unit: hours). If an hourly custom schedule is disabled, two hyphens (--) are displayed.</p> <p>DAILY Versions: The value specified for a daily custom schedule is displayed (unit: days). If a daily custom schedule is disabled, two hyphens (--) are displayed.</p> <p>WEEKLY Versions: The value specified for a weekly custom schedule is displayed (unit: weeks). If a weekly custom schedule is disabled, two hyphens (--) are displayed.</p> <p>MONTHLY Versions: The value specified for a monthly custom schedule is displayed (unit: months). If a monthly custom schedule is disabled, two hyphens (--) are displayed.</p> <p>YEARLY Versions: The value specified for a yearly custom schedule is displayed (unit: years). If a yearly custom schedule is disabled, two hyphens (--) are displayed.</p>

Processing Nodes window

In the Processing Nodes window, you can view a list of the operating status of all processing nodes.

To open the Processing Nodes window, in the **Explorer** menu of the Hitachi File Services Manager main window ([Explorer menu on page B-5](#)), select **Resources**, and then **Processing Nodes**. Then, select **Processing Nodes** in the object tree.



File Servers tab

You can use the **File Servers** tab to view information about an HDI system registered with the management server.

Table C-57 Processing node information shown on the File Servers tab in the Processing Nodes window

Item	Description
Processing Node Name	The name of the processing node.
Processing Node Status	<p>The operating status of the processing node. If the operating status differs between physical nodes, the operating status of the physical node that has a more serious problem is shown.</p> <p>Online</p> <p>The status of the physical nodes that make up the processing node is <code>Online</code>.</p> <p>Ready for failback</p> <p>The status of the physical nodes that make up the processing node is <code>Ready for failback</code>.</p> <p>Transitional state</p> <p>The status of the physical nodes that make up the processing node is <code>Transitional state</code>.</p> <p>Maintenance required</p> <p>The status of the physical nodes that make up the processing node is <code>Maintenance required</code>.</p> <p>Unknown error</p>

Item	Description
	<p>The status of the physical nodes that make up the processing node is <code>Unknown error</code>.</p> <p><code>Credential error</code></p> <p>The status of the physical nodes that make up the processing node is <code>Credential error</code>.</p> <p><code>Shutdown</code></p> <p>The status of the physical nodes that make up the processing node is <code>Shutdown</code>.</p> <p><code>Starting</code></p> <p>The processing node is being started from the Start Processing Node dialog box. Wait a while, and then refresh the processing node information. For details about how to refresh the information, see processing-node window on page C-86.</p> <p><code>Cluster function disabled</code></p> <p>The failover functionality is disabled because of an error. For details about the operating status, see processing-node window on page C-86.</p>
Hardware Status	<p>The status of the processing node hardware.</p> <p><code>Normal</code></p> <p>The statuses of all the hardware in both physical nodes that make up the processing node are normal.</p> <p><code>Error</code></p> <p>An error has occurred in at least one piece of hardware in the physical nodes that make up the processing node.</p> <p><code>Unknown error</code></p> <p>The hardware information cannot be obtained from the physical nodes that make up the processing node.</p>
Model	The model of the processing node.
System Version	<p>The HDI system version.</p> <p><code>Upgrading</code> appears when the versions in the processing node are inconsistent (during an upgrade installation).</p> <p><code>Unknown</code> appears when the information cannot be collected from both physical nodes in the processing node.</p>
Last Refresh Time	The date and time that the information shown in the window was last refreshed.

Table C-58 Operations that can be performed on a processing node from the File Servers tab in the Processing Nodes window

Button	Function	See
Add Processing Node	<p>Registers the processing node with the management server when you added a new node.</p> <p>If the maximum number of processing nodes is registered, this button is not shown.</p>	Add Processing Node dialog box on page C-82

Button	Function	See
Start Node	Starts a processing node in an environment where the management server can communicate with the BMC of the processing node by way of IPv4. Starting a processing node starts both OSs. If you are using encryption, and the system settings are saved to the HCP system, confirm that the HCP system is operating normally and that the HDI and HCP systems can communicate normally, before starting a processing node.	N/A
Shutdown Node	Stops a specific processing node during a planned shutdown of an HDI system. When a processing node is stopped in this manner, both OSs are forcibly stopped and the nodes are powered off, regardless of service activity and any I/O operations being performed on the file system.	N/A
Edit Node	When there is a change to a physical node's fixed IP address or to the authentication password used by the management server, you can use this button to edit the processing node information so that the processing node will be recognized again by the management server.	Edit Node dialog box on page C-85
Delete Node	Deletes a processing node that is no longer needed from among those managed by the management server.	N/A
Note: N/A = Not applicable.		

Content Platform tab

You can use the **Content Platform** tab to view information about an HCP registered with the management server.

Table C-59 HCP information shown on the Content Platform tab in the Processing Nodes window

Item	Description
Nickname	The HCP nickname.
System Name	The HCP system name.
Administrator Type	The administrator type. Cluster A cluster administrator. Tenant A tenant administrator.
Tenant Name	The tenant name is shown when the Administrator Type is Tenant . -- When the Administrator Type is Cluster .

Item	Description
Port	The port number used by the management console to communicate with the HCP system.

Table C-60 HCP operations that can be performed from the Content Platform tab in the Processing Nodes window

Button	Description	See
Add Processing Node	Registers an HCP. If the maximum number of processing nodes is registered, this button is not shown.	Add Processing Node dialog box on page C-82
Manage HCP	Opens the HCP GUI. For details about how to operate the HCP GUI, see the HCP manual. To start the HCP GUI from this button, you need to register a DNS server that can resolve the HCP name to the management console.	N/A
Delete HCP	Deletes an HCP.	N/A

Note: N/A = Not applicable.

Add Processing Node dialog box

In the **Add Processing Node** dialog box, you can register a file server or HCP as a processing node with the management server.

To open the **Add Processing Node** dialog box, in the Processing Nodes window ([Processing Nodes window on page C-78](#)), click **Add Processing Node**.

For **Type** in the **Add Processing Node** dialog box, select the type of the processing node to be registered, and then specify the system information.

Table C-61 Information specified for Type in the Add Processing Node dialog box

Item	Description		See
File Servers	Select this item to register an HDI node as a processing node. A maximum of 16 such nodes can be registered.		When File Servers type is selected on page C-83
	Basic	Specify basic attributes of the HDI node.	Basic tab on page C-83
	Storage System	Specify the IP address of the controller of the storage system to be managed. You must specify this item to automatically create an LU when using a Hitachi AMS2000 or HUS100 series storage system or to use the HDD with Storage Navigator Modular 2.	Storage System tab on page C-84
Content Platform	Select this item to register an HCP processing node. A maximum of 64 such nodes can be registered. When an HCP is registered, you can see the HCP GUI from the Hitachi File Services Manager GUI.		When Content Platform type is selected on page C-84

When File Servers type is selected

You can select this item to register an HDI node as a processing node.

Basic tab

You can use the **Basic** tab to specify the basic attributes of the HDI node.

Table C-62 Information specified on the Basic tab in the Add Processing Node dialog box

Item	Description
Mgmt. IP address first node	Specify the IP address to be used by the management server for connecting to the node. Specify the fixed IP address of the processing node to which the server connects. You can also specify a host name.
Mgmt. IP address second node	If a cluster has not been configured, specify the fixed IP address for the other node. You can also specify a host name.
Password	Specify the management server's authentication password set in the node. The initial password is <code>manager</code> .

Item	Description
<p>Note: Do not register the same processing node with multiple management servers. If no clusters have been configured, UNDEF appears under Processing Node in the object tree when you register the processing node, and No Object appears in the application area.</p>	

Storage System tab

You can use the **Storage System** tab to specify the IP address of the controller of the storage system to be managed.

You must specify this item to automatically create an LU when using a Hitachi AMS2000 or HUS100 series storage system or to use the HDD with Storage Navigator Modular 2.

Table C-63 Information specified on the Storage System tab in the Add Processing Node dialog box

Item	Description
CTL0 IP address	Specify the IP address or host name of the management port of controller 0.
CTL1 IP address	Specify the IP address or host name of the management port of controller 1.

When Content Platform type is selected

You can select this item to register an HCP processing node.

A maximum of 64 such nodes can be registered. When an HCP is registered, you can see the HCP GUI from the Hitachi File Services Manager GUI.



Note: After registering an HCP with **Cluster** specified for the **Administrator type**, register the same HCP once again with **Tenant** specified for the **Administrator type**

Table C-64 HCP information specified in the Add Processing Node dialog box

Item	Description
Nickname	<p>Specify an HCP nickname of no more than 22 characters. You can use alphanumeric characters, hyphens (-), periods (.), forward slashes (/), colons (:), at marks (@), and underscores (_). However, you cannot use an underscore (_) as the first character.</p> <p>Either of the following nicknames will be set if no nickname is specified:</p> <p>When Cluster is selected in Administrator type</p>

Item	Description
	<p>The nickname will be the first 22 characters of the system name.</p> <p>When Tenant is selected in Administrator type</p> <p>The nickname will be the first 22 characters of the following string:</p> <p><i>tenant-name.system-name</i></p>
System name	Specify the HCP system name as a fully qualified domain name.
Administrator type	<p>Select the option for the type of administrator.</p> <p>Cluster</p> <p>Select this option to register a cluster administrator.</p> <p>Tenant</p> <p>If you select this item, specify the name of the target tenant for Tenant name.</p>
Port	Specify the port number used by the management console to communicate with the HCP system.

Edit Node dialog box

When there is a change to the fixed IP address of a physical node or to the authentication password used by the management server, in the **Edit Node** dialog box, the system administrator must edit the processing node information so that the processing node will be recognized again by the management server.

To open the **Edit Node** dialog box, in the Processing Nodes window ([Processing Nodes window on page C-78](#)), click **Edit Node** on the **File Servers** tab.

Basic tab

You can use the **Basic** tab to specify the basic attributes of the processing node.

Table C-65 Information specified on the Basic tab in the Edit Node dialog box

Item	Description
Mgmt. IP address first node	Specify the IP address to be used by the management server for connecting to the node. Specify the fixed IP address of the processing node to which the server connects. You can also specify a host name.
Mgmt. IP address second node	If a cluster has not been configured, specify the fixed IP address for the other node. You can also specify a host name.
Password	Specify the management server's authentication password set in the node.

Storage System tab

You can use the **Storage System** tab to specify the IP address of the controller of the storage system to be managed.

You must specify this item to automatically create an LU when using a Hitachi AMS2000 or HUS100 series storage system or to use the HDD with Storage Navigator Modular 2.

Table C-66 Information specified on the Storage System tab in the Edit Node dialog box

Item	Description
CTL0 IP address	Specify the IP address or host name of the management port of controller 0.
CTL1 IP address	Specify the IP address or host name of the management port of controller 1.

processing-node window

You can use the *processing-node* window to view the operating status of a specific processing node.

To open the *processing-node* window, in the **Explorer** menu of the Hitachi File Services Manager main window ([Explorer menu on page B-5](#)), select **Resources**, and then **Processing Nodes**. In the object tree, select **Processing Nodes**, and then the desired processing node.



Table C-67 Operation that can be performed on a processing node from the processing-node window

Button	Description	See
Reconfigure Processing Node	Reconfigures the processing node by way of the Configuration Wizard.	Configuration Wizard on page C-317
Refresh Processing Node	<p>Refreshes the information in the management server database when the information in the database cache is inconsistent with the information in a node.</p> <p>This also refreshes information about the objects shown in the GUI, such as file systems and file shares.</p> <p>Notes:</p> <ul style="list-style-type: none"> If a communication error occurs between the management server and a node, or if the OS is stopped, only the operating status of the processing node or physical node is refreshed. Information about the file system, file shares, and so on is not refreshed. Information about users and groups is not refreshed by the operation described above. To refresh user and group information, click Refresh Users and Groups in the dialog boxes that show the information. 	N/A
Note: N/A = Not applicable.		

Table C-68 Information shown in the processing-node window

Item	Description	See
Summary	Information about the selected processing node.	Table C-69 Information shown in the Summary of the processing-node window on page C-88
Physical Nodes	Information about the physical nodes that belong to the processing node.	Physical Nodes tab on page C-89

Table C-69 Information shown in the Summary of the processing-node window

Item	Description
Processing Node Name	The name of the processing node.
Processing Node Status	<p>The operating status of the processing node. If the operating status differs between physical nodes, the operating status of the physical node that has a more serious problem is shown.</p> <p>Online The status of the physical nodes that make up the processing node is Online.</p> <p>Ready for failback The status of the physical nodes that make up the processing node is Ready for failback.</p> <p>Transitional state The status of the physical nodes that make up the processing node is Transitional state.</p> <p>Maintenance required The status of the physical nodes that make up the processing node is Maintenance required.</p> <p>Unknown error The status of the physical nodes that make up the processing node is Unknown error.</p> <p>Credential error The status of the physical nodes that make up the processing node is Credential error.</p> <p>Shutdown The status of the physical nodes that make up the processing node is Shutdown.</p> <p>Starting The processing node is being started from the Start Processing Node dialog box. Wait a while, and then refresh the processing node information. For details about how to refresh the information, see processing-node window on page C-86.</p> <p>Cluster function disabled</p>

Item	Description
	The failover functionality is disabled because of an error. For details about the operating status, see processing-node window on page C-86 .
Hardware Status	The status of the processing node hardware. Normal The statuses of all the hardware in both physical nodes that make up the processing node are normal. Error An error has occurred in at least one piece of hardware in the physical nodes that make up the processing node. Unknown error The hardware information cannot be obtained from the physical nodes that make up the processing node.
System Version	The HDI system version. Upgrading appears when the versions in the processing node are inconsistent (during an upgrade installation). Unknown appears when the information cannot be collected from both physical nodes in the processing node.
Last Refresh Time	The date and time that the information shown in the window was last refreshed.
Encryption Settings	Displays whether encryption is enabled for the local data and the data to be stored in the HCP system, when an encryption license is set. Local Data: Yes or No HCP Payload: Yes or No

Physical Nodes tab

You can use the **Physical Nodes** tab to view information about the physical nodes that belong to the processing node.

Table C-70 Information shown on the Physical Nodes tab in the processing-node window

Item	Description
Physical Node Host Name	The host name of each physical node.
Mgmt. IP Address	The IP address used by the management server to connect to each physical node. If a problem exists in IP address settings, <i>Invalid</i> or <i>Unknown</i> is shown. To solve the problem, see the <i>Cluster Troubleshooting Guide</i> .
Node Number	The node number.
Physical Node Status	The operating status of each physical node. Online The physical node is running normally.

Item	Description
	<p>Ready for failback</p> <p>A failover has occurred. Services for clients are continuing on the other node that makes up the processing node. Remove the cause of the failure, and then fail back the resource group to the original node. For detailed information about the node status, see the Cluster Management dialog box.</p> <p>Transitional state</p> <p>The resource group is starting or stopping. Wait a while, and then refresh the processing node information. For details about how to refresh the information, see physical-node window on page C-91.</p> <p>Maintenance required</p> <p>The physical node is in one of the following states:</p> <ul style="list-style-type: none"> - A cluster, node, or resource group is stopped. - The resource group is excluded from the monitoring targets. - The physical node is not configured in a cluster. <p>Client services might be stopped. For detailed information about the node status, see the Cluster Management dialog box.</p> <p>Unknown error</p> <p>The physical node is in one of the following states:</p> <ul style="list-style-type: none"> - Client services have stopped because of a failure. - Because of a network error, a communication error has occurred between the management server and the physical node. - Because of an error, the failover functionality is disabled. - An error has occurred in Primary Server Base. - Because of status transitions of the cluster, a communication error has occurred. - Information could not be obtained because a failure occurred on the physical node. <p>Check the node and resource group statuses from the Cluster Management dialog box. Also check whether an error message is output from the List of RAS Information page (for <i>List of messages</i>) in the Check for Errors dialog box. If you cannot view the dialog box, see the <i>Cluster Troubleshooting Guide</i> to identify the cause.</p> <p>Credential error</p> <p>An authentication error occurred during communication between the management server and the physical node.</p> <p>In the Edit Node dialog box, re-register the authentication password set in the physical node.</p> <p>Shutdown</p> <p>Shows when you stop a processing node in the Stop Processing Node dialog box.</p> <p>Starting</p> <p>The processing node is being started from the Start Processing Node dialog box. Wait a while, and then refresh the processing node information. For details about how to refresh the information, see processing-node window on page C-86.</p>

Item	Description
Hardware Status	<p>The status of the physical node hardware.</p> <p>Normal</p> <p>The statuses of all the hardware are normal.</p> <p>Error</p> <p>An error has occurred in at least one hardware unit. Check the hardware status from the Health Monitor window.</p> <p>Unknown error</p> <p>Hardware information cannot be obtained. Check whether an error message has been output from the List of RAS Information page (for List of messages) in the Check for Errors dialog box.</p>
System Version	<p>The HDI system version.</p> <p>Shows <code>Unknown</code> when the information cannot be collected.</p>
Last Refresh Time	<p>The date and time that the information shown in the window was last refreshed.</p>

physical-node window

You can use the *physical-node* window to view the operating status of a specific physical node.

To open the *physical-node* window, in the **Explorer** menu of the Hitachi File Services Manager main window ([Explorer menu on page B-5](#)), select **Resources**, and then **Processing Nodes**. In the object tree, select **Processing Nodes**, the desired processing node, and then the desired physical node.

The screenshot shows the 'Processing Nodes' window for node DT119000013. The left pane shows a tree view with 'Processing Nodes' expanded to 'DT119000013'. The main pane displays the following summary table:

Summary			
Physical Node Host Name	DT119000013	Physical Node Status	Online
Mgmt. IP Address	10.213.137.99	Hardware Status	Normal
Node Number	node 1	System Version	5.0.0-00
Last Refresh Time	2014-06-23 14:47:30		

Below the summary is the 'Shares' section, which contains a table with the following data:

Share Name	Protocol	Use Namespace	Content Sharing	CIFS Share Name	Capacity	Used
filesystem04	CIFS, NFS	--	--	filesystem04	4MB	
filesystem04/share04	CIFS	--	--	share04	0MB	

Table C-71 Operation that can be performed on a processing node from the physical-node window

Button	Description	See
Reconfigure Processing Node	Reconfigures the processing node by way of the Configuration Wizard.	Configuration Wizard on page C-317
Refresh Processing Node	<p>Refreshes the information in the management server database.</p> <p>If the cached information in the management server database is inconsistent with the information on a node, if the operation in a dialog box opened from the Settings tab has finished, or if an error message instructs you to refresh the information, a system administrator must refresh the management server database. This also refreshes information about the objects shown in the GUI, such as file systems and file shares.</p> <p>Observe the following notes:</p> <ul style="list-style-type: none"> • If a communication error occurs between the management server and a node, or if the OS is stopped, only the operating status of the processing node or physical node is refreshed. Information about the file system, file shares, and so on is not refreshed. • Information about users and groups is not refreshed by the operation described above. To refresh user and group information, click Refresh Users and Groups in the dialog boxes that show the information. 	N/A

Note: N/A = Not applicable.

Table C-72 Information shown in the physical-node window

Item	Description	See
Summary	Information about the selected physical node	Table C-70 Information shown on the Physical Nodes tab in the processing-node window on page C-89
Shares	Information about the file shares running on the physical node	Shares tab on page C-93
File Systems	Information about the file systems running on the physical node	N/A
	File System Information about file systems	File System subtab on page C-95

Item	Description		See
LUs	Information about the LUs recognized by one of the physical nodes in the processing node		N/A
	LUs	Information about LUs	LUs subtab on page C-99
	Pool	Pool information if virtual LUs are used on the physical node	Pools subtab on page C-101
Settings	Menus for specifying settings for the physical node		N/A
	Basic	Menu for specifying basic settings for the physical node	Basic subtab on page C-102
	Advanced	Menu for specifying advanced settings for the physical node	Advanced subtab on page C-103
Note: N/A = Not applicable.			

Shares tab

You can use the **Shares** tab to view information about the file shares.

Table C-73 Information shown on the Shares tab in the physical-node window

Item	Description
Share Name	The name of the share.
Protocol	The names of the protocols used by the file share. CIFS The CIFS protocol is used. NFS The NFS protocol is used. CIFS, NFS The CIFS and NFS protocols are used.
Use Namespace	Displays whether the HCP namespace is allocated to the share. Yes Displayed when the HCP namespace is allocated to the share. No Displayed when the HCP namespace is not allocated to the share. If a file system is not linked to the HCP system at the share level, two hyphens (--) are displayed.
Content Sharing	Displays how data is shared with other HDI systems via the linked HCP. Off Displayed if data is not synchronized with other HDI systems

Item	Description
	On (Read-Only) Displayed if other HDI data is referenced as read-only If a file system is not linked to the HCP system at the share level, two hyphens (--) are displayed.
CIFS Share Name	The name of the CIFS share when the CIFS protocol is used in the file share. This item is left as blank if the CIFS protocol is not used.
Capacity ^{#1}	The usage of the file system. If the capacity of the file share is managed, the usage of the file share is shown. ^{#2} Used The used capacity of the file system or file share. Free The remaining capacity of the file system or file share. Total The total capacity of the file system or file share. % Used The percentage of the file system or file share capacity in use. If the file system has not been mounted correctly, 0 is shown in all items.
Capacity Management Directory	The directory subject to capacity management is shown. If the capacity of the file share is not managed, the file system name is shown.
<p>#1: The values shown are calculated from the block capacity of the file system. Capacities shown in MB are rounded to the nearest ones place. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.</p> <p>#2: When the capacity of the file share is limited based on the hard quota of the migration-destination namespace, "--" will be displayed.</p>	

Table C-74 File share operations that can be performed from the Shares tab in the physical-node window

Button	Function	See
Create and Share File System	Create a file system and file share at the same time.	Create and Share File System dialog box on page C-103
Release Share	Release an unnecessary file share. Notes: <ul style="list-style-type: none"> The shared directory is not deleted even after the file share is released. When the CIFS protocol and NFS protocol are being used, both are released. Edit the file share attributes if you want to release only one 	N/A

Button	Function	See
	<p>protocol. For details about editing file share attributes, see Basic tab on page C-8.</p> <ul style="list-style-type: none"> If the CIFS service configuration definition settings do not allow the CIFS share settings to be automatically reloaded and you released a CIFS share during degenerated operation, to enable the CIFS share settings, perform a failback operation. Restart the CIFS services on both nodes. For details about how to perform a failback operation, see Browse Cluster Status page on page C-271. For details about how to restart a CIFS service, see List of Services page on page C-218. 	
Edit Share	Edit file share attributes such as the protocol and access permissions.	Edit Share dialog box on page C-7
Change Share Quota	Change the capacity of the file share immediately under the mount point.	Change Share Quota dialog box on page C-19
Note: N/A = Not applicable.		

File Systems tab

You can use the **File Systems** tab to view information about the file systems.

File System subtab

You can use the **File System** subtab to view information about file systems.

Table C-75 Information shown on the File System subtab of the File Systems tab in the physical-node window

Item	Description
File System Name	The name of the file system.
Mount Status	<p>The status of the file system.</p> <p>Online (RW) The file system is mounted with both read and write operations permitted.</p> <p>Online (RO) The file system is mounted as read-only.</p> <p>Unmounted The file system is unmounted.</p> <p>Expanding The file system is being expanded or an error occurred during expansion processing. Wait a while, and then refresh the processing node information. If the status does not change, an error might have occurred during</p>

Item	Description
	<p>processing. Obtain all the log data, and then inform maintenance personnel.</p> <p>Reclaiming</p> <p>The unused area of the virtual LUs that are used for the file system is being released.</p> <p>Data corrupted</p> <p>The file system is blocked because of an error in the OS or a pool capacity shortage.</p> <p>Take corrective action by referring to the <i>Cluster Troubleshooting Guide</i>.</p> <p>Device error</p> <p>The file system is blocked because of an error in the LU (multiple drive failure).</p> <p>Take corrective action by referring to the <i>Cluster Troubleshooting Guide</i>.</p>
Namespace Type	<p>Displays how the file system is linked to the HCP system.</p> <p>File System</p> <p>The file system is linked to the HCP system at the file system level.</p> <p>Subtree</p> <p>The file system is linked to the HCP system at the share level.</p> <p>-- is shown when a namespace is not used.</p>
Content Sharing	<p>Displays how data is shared with other HDI systems via the linked HCP.</p> <p>Off</p> <p>Displayed if data is not synchronized with other HDI systems</p> <p>On (Read-Only)</p> <p>Displayed if other HDI data is referenced as read-only</p> <p>On (Read/Write)</p> <p>Displayed if the read-write-content-sharing functionality is used to share data among HDI systems (read-write-content-sharing file system)</p> <p>Home directory</p> <p>Displayed if roaming among HDI systems is enabled for home directory data created for each end user (home-directory-roaming file system)</p> <p>-- is shown when a namespace is not used.</p>
ACL Type	<p>The ACL type of the file system.</p> <p>Advanced ACL</p> <p>The file system is the Advanced ACL type.</p> <p>Classic ACL</p> <p>The file system is the Classic ACL type.</p> <p>Unknown</p>

Item	Description
	The ACL type information cannot be obtained.
Function	<p>The name of the function that is using the file system.</p> <p>None The file system is not being used by another function.</p> <p>Active Migration The file system is used by a function of Active File Migration.</p> <p>WORM A WORM file system.</p>
Quota Enabled	<p>Shows whether the quota function is enabled for the file system.</p> <p>Yes The quota function is enabled.</p> <p>No The quota function is disabled.</p> <p>If the LU or the file system is blocked, the status in effect before the failure occurred is shown. Additionally, <code>No</code> is shown after a failure under one of the following conditions:</p> <ul style="list-style-type: none"> • The quota setting was disabled before the failure occurred. • The quota setting was enabled before the failure occurred. However, the status was changed when, for example, an unmount operation was performed after the failure.
Total LU Capacity	The total capacity of the LUs that make up the file system. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.
Capacity[#]	<p>The usage of the file system.</p> <p>Used The used capacity of the file system.</p> <p>Free The remaining capacity of the file system.</p> <p>Total The total capacity of the file system.</p> <p>% Used The percentage of the file system capacity in use.</p> <p>If the file system has not been mounted correctly, 0 is shown in all items.</p>
i-nodes	<p>The inode usage.</p> <p>Used The used inode capacity.</p> <p>Free The free inode capacity.</p> <p>Total The total inode capacity.</p>

Item	Description
	<p>% Used</p> <p>The percentage of inode capacity in use.</p> <p>If the file system has not been mounted correctly, 0 is shown in all items.</p>
<p>#: The values shown are calculated from the block capacity of the file system. Capacities shown in MB are rounded to the nearest ones place. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.</p>	

Table C-76 File system operations that can be performed for a file system from the File System subtab of the File Systems tab in the physical-node window

Button	Function	See
Add Share	<p>Add a file share in the file system.</p> <p>Note that a file share cannot be added if the read-write-content-sharing file system or home-directory-roaming file system and a file share has already been created.</p>	Add Share dialog box on page C-38
Edit	<p>Edit a file system.</p>	Edit File System dialog box on page C-44
Create	<p>Create a new file system.</p>	Create File System dialog box on page C-126
Delete	<p>Delete a file system that is no longer required.</p> <p>This operation can be performed when the nodes and the resource group satisfy the following conditions:</p> <ul style="list-style-type: none"> The status of both nodes is <code>UP</code>. The status of the resource group is <code>Online/No error</code> or <code>Offline</code>. <p>Perform the following operations in advance:</p> <ul style="list-style-type: none"> Release all file shares in the target file system. <p>Notes:</p> <ul style="list-style-type: none"> If the target file system has been mounted, it is unmounted automatically. A file system cannot be deleted if it contains a file whose retention period has not expired. If a file system whose data has been migrated to an HCP is deleted, the data on the HCP is not deleted. After the file system is deleted, the LUs used for the file system can be used for other purposes. When the status of the resource group is <code>Offline</code> and a file system for which file shares have been created is deleted, its NFS shares are 	<p>N/A</p>

Button	Function	See
	automatically released but its CIFS shares are not. After starting the resource group, use the appropriate commands to release the file shares.	
Expand	Expand the capacity of a file system as needed.	Expand File System dialog box on page C-52
Mount	Mount a file system.	Mount File System dialog box on page C-54
Unmount	<p>Unmount a file system.</p> <p>Before unmounting a file system, a system administrator must release all file shares in the file system. If Backup Restore is being used, before you unmount the file system, verify that no backup or restore operations are in progress. By checking the connection status between the NDMP server and the backup server, and between the NDMP server and the media server.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Unmounting a file system does not delete the data. If a file system is no longer required, it should be deleted rather than unmounted. • Unmounting a file system stops the services for that file system. 	N/A
Edit User/ Group Quota	<p>Manage quota information for each file system.</p> <p>By clicking this button, you can open the Edit Quota dialog box for a specific file system. You can show up to 10 Edit Quota dialog boxes for a physical node at the same time. To close unnecessary Edit Quota dialog boxes, click Close. If the Edit Quota dialog box cannot be opened, quit all Web browsers, and then log on again.</p>	Edit Quota dialog box on page C-55
Note: N/A = Not applicable.		

LU's tab

You can use the **LU's** tab to view information about the LUs.

LU's subtab

You can use the **LU's** subtab to view information about LUs.

Table C-77 Information shown on the LUs subtab of the LUs tab in the physical-node window

Item	Description
LU Name	The LU name. When the LU resides on an external storage system, a hash mark (#) is attached at the end of the LU name (However, if an error has occurred on the FC path or the LU path from both nodes, the hash mark is not shown).
File System Name	The name of the file system where the LU is being used. -- is shown if the LU is not used. -Unknown- is shown if the information cannot be obtained.
Status	Shows whether the LU is in use. In use Indicates an LU that is in use. Not in use Indicates an LU that is not in use.
Capacity	The LU capacity. Capacities shown in GB or TB are rounded to the nearest two decimal places. 0MB appears when: <ul style="list-style-type: none"> • An LU error has occurred. • The LU is in use, and an error has occurred on the FC path from both nodes. • The LU is in use, and an error has occurred on the LU path from both nodes.
Used Capacity	The used capacity of a virtual LU. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places. If the LU is not a virtual LU or information cannot be obtained, -- is shown. Operations such as refreshing processing node information and creating file systems sometimes temporarily allocate capacity to virtual LUs. In this case, allocated capacities might also be shown for unused virtual LUs.
Drive Type	The LU drive type. FC/SAS Indicates an FC or SAS drive. SAS7K Indicates a SAS 7.2K drive. SATA Indicates a SATA drive. SSD Indicates a solid-state drive. -- is shown if: <ul style="list-style-type: none"> • The information cannot be obtained because an error occurred.

Item	Description
	<ul style="list-style-type: none"> The LU is a virtual LU for VSP G1000, VSP G200, G400, G600, G800, VSP F400, F600, F800, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM. The LU is a virtual LU that uses HUS100 series Dynamic Tiering. The LU resides on an external storage system.
Parity Group#	The parity group to which the LU belongs. If the LU is a virtual LU, if the LU resides on an external storage system, or if information cannot be obtained, -- is shown.
Pool#	The number of the pool to which the LU belongs. If the LU is not a virtual LU or information cannot be obtained, -- is shown.
Model	The model of the storage system on which the LU resides.
Serial Number	The serial number of the storage system on which the LU resides. When the LU is on an external storage system, the information shown relates to the mapped storage system.
Volume#	The LDEV number of the LU. When the LUN Expansion functionality is being used, the ID of the volume at the head of the linked volumes is shown.
Target	The target to which the path to the LU belongs. -- is shown if: <ul style="list-style-type: none"> The LU is in use, and an error has occurred on the FC path from the node that is shown. The LU is in use, and an error has occurred on the LU path from the node that is shown.
<p>Note: No information is shown for an unused LU if an error has occurred on the FC paths or the LU paths from both nodes.</p> <p>#: If Hitachi Storage Navigator Modular 2 is linked to, clicking the item name opens the Hitachi Storage Navigator Modular 2 window. For details about how to use the window, see the applicable Hitachi Storage Navigator Modular 2 documentation.</p>	

Pools subtab

You can use the **Pools** subtab to view pool information if virtual LUs are used.

Table C-78 Information shown on the Pools subtab on the LUs tab in the physical-node window

Item	Description
Pool	The number of the pool to which the virtual LUs used in the file system belong.
Model	The model of the storage system on which the pool resides.
Serial Number	The serial number of the storage system on which the pool resides. If the pool resides on an external storage system, information about the mapped storage system is shown.

Item	Description	
Free Space [#]	The amount of free space in the pool. If the storage system is a VSP G1000, VSP G200, G400, G600, G800, VSP F400, F600, F800, Virtual Storage Platform, Universal Storage Platform V/VM storage system, or HUS VM, -- is shown.	
Total Capacity [#]	The total capacity of the pool. If the storage system is a VSP G1000, VSP G200, G400, G600, G800, VSP F400, F600, F800, Virtual Storage Platform, Universal Storage Platform V/VM storage system, or HUS VM, -- is shown.	
Capacity for This Instance [#]	The capacity available for each instance.	
	Used Capacity	The amount of pool space allocated to the file system.
	LU Total	The total capacity of the LUs in the file system.
[#] : Capacities shown in MB are rounded to the nearest integer. Capacities shown in GB, TB, or PB are rounded to the nearest two decimal places.		

Settings tab

You can use the **Settings** tab to view menus for specifying settings for the physical node.



Note: When you finished the operations, close the dialog box. In addition, click **Refresh Processing Node** in the *physical-node* window to reflect the information on the node to the database on the management server.

Basic subtab

You can use the **Basic** subtab to view a menu for specifying basic settings for the physical node.

Table C-79 Operations that can be performed on a physical node from the Basic subtab of the Settings tab in the physical-node window

Item	Function	See
Health Check	View the statuses of hardware and the network.	Health Monitor window on page C-137
Software Update	Manage the software that is running on the nodes.	System Software window on page C-147
Local Users	Use the HDI system to manage users who access the file system and the groups.	Local Users dialog box on page C-150
Check for Errors	Manage error information on the node.	Check for Errors dialog box on page C-163

Advanced subtab

You can use the **Advanced** subtab to view a menu for specifying advanced settings for the physical node.

Table C-80 Operations that can be performed on a physical node from the Advanced subtab of the Settings tab in the physical-node window

Item	Function	See
Backup Configuration	Save or download system settings.	Backup Configuration dialog box on page C-171
Network & System Configuration	Manage information about interfaces, networks, and external servers.	Network & System Configuration dialog box on page C-178
Access Protocol Configuration	Control the operating status or change the configuration definitions of the NFS service, CIFS service, or other services.	Access Protocol Configuration dialog box on page C-217
Cluster Management	Manage clusters, nodes, and resource groups.	Cluster Management dialog box on page C-268
Proxies	Manage the proxy server that is used for communication between an HDI system and an HCP system.	Proxy Server Settings window on page C-281
Virus Scan Server Configuration	Enter settings for using the real-time virus scanning functionality provided by Anti-Virus Enabler.	Virus Scan Server Configuration dialog box on page C-283

Create and Share File System dialog box

In the **Create and Share File System** dialog box, the system administrator can share an entire file system. To do this, you can create and mount a file system, and create a file share simultaneously.

You can create a file system with a maximum size of 1 PB (total LU capacity). The file system is mounted on the following mount point directory:

/mnt/file-system-name

You can create and mount a maximum of 511 file systems per cluster.

A maximum of 1,024 NFS shares can be created per cluster. Access control when an NFS share is created in a file system of the Advanced ACL type follows the set ACL, not the permissions that can be referenced from the client side. Therefore, when only NFS shares are to be used, Hitachi Data Systems recommends a file system of the Classic ACL type. If you are using an Advanced ACL file system, Hitachi Data Systems recommends that you do not set ACE (access control entry) inheritance for directories in which NFS shares will be created.

The maximum number of CIFS shares per cluster depends on whether the setting in the CIFS service configuration definitions specifies that the CIFS

share settings are to be automatically applied to the CIFS client environment. For details about the maximum number of CIFS shares, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.



Tip: You can use commands to set even more detailed attributes for the file system.

To open the **Create and Share File System** dialog box, in the *physical-node* window ([physical-node window on page C-91](#)), click **Create and Share File System** on the **Shares** tab.

Table C-81 Information shown in the Create and Share File System dialog box

Item	Description	See
Basic	Specify basic attributes relating to the file share.	Basic tab on page C-105
Access Control	Specify attributes related to file share access permissions.	Access Control tab on page C-108

Item	Description	See
	The Directory subtab does not appear if you select Use existing directory as is under Export point owner on the Basic tab.	
CIFS	Specify attributes related to CIFS share access permissions.	CIFS subtab on page C-108
NFS	Specify attributes related to NFS share access permissions.	NFS subtab on page C-111
Directory	For the Advanced ACL type, set the ACL for the shared directory. For the Classic ACL type, set access permissions for the shared directory.	Directory subtab (A file system of the Advanced ACL type) on page C-114 Directory subtab (A file system of the Classic ACL type) on page C-115
WORM	Specify the WORM settings for the file system.	WORM tab on page C-115
Namespace	If you link to an HCP system, you can specify the HCP namespace settings.	Namespace tab on page C-117
Advanced	Specify attributes of the file share and the file system in which the file share is created as necessary.	Advanced tab on page C-121
CIFS	Specify attributes of the CIFS share as necessary.	CIFS subtab on page C-121
File System	Specify attributes of the file system in which the file share is created as necessary.	File System subtab on page C-125
Striping	Specify information about the striping settings for the file system.	Striping subtab on page C-126

Basic tab

You can use the **Basic** tab to specify basic attributes relating to the file share.

Table C-82 Information specified in the Basic tab in the Create and Share File System dialog box

Item	Description
Share name	Specify the share name of the file system. The specified name is also used as the file system name. Specify a name that is unique within the cluster. The name must be a maximum of 16 characters consisting of alphanumeric characters and the underscore (_). Note: When you use the CIFS protocol and specify <code>global</code> , <code>homes</code> , or <code>printers</code> as the CIFS share name, you need to specify the CIFS share name in CIFS share name on the Advanced tab.

Item	Description
Protocol	<p>Select the protocol to be used in the file share.</p> <p>CIFS (for Windows® clients) Select this option to use the CIFS protocol. If you select Home directory for Content sharing, you must select CIFS (for Windows® clients).</p> <p>NFS (for UNIX clients) Select this option to use the NFS protocol.</p> <p>CIFS, NFS Select this option to use the CIFS protocol and the NFS protocol.</p>
Namespace type	<p>Specify how to link to the HCP system.</p> <p>File system The file system is linked to the HCP system at the file system level.</p> <p>None An HCP namespace is not used.</p> <p>For Content sharing, select how data is to be shared with other HDI systems via the linked HCP.</p> <ul style="list-style-type: none"> • If you do not want to synchronize data with other HDI systems, select Off, and then specify the hard quota that you want to allocate to the namespace for Quota. Specify a value smaller than the Tenant hard quota value. • To reference other HDI data as read-only, select On (Read-Only). • To share data among HDI systems by using the read-write-content-sharing functionality, select On (Read/Write). To create a namespace, select Yes for Create namespace, and then specify the hard quota that you want to allocate to the namespace for Quota. Specify a value smaller than the Tenant hard quota value. • To enable roaming among HDI systems for home directory data created for each end user, select Home directory. To create a namespace, select Yes for Create namespace, and then specify the hard quota that you want to allocate to the namespace for Quota. Specify a value smaller than the Tenant hard quota value.
Capacity	<p>Specify the capacity of the file system.</p> <p>Note that, if you want to create a file system in a striped configuration, select Select from existing LUs.</p> <p>File system LU size^{#1} Select this to automatically create an LU to be used for the file system. In the text box, specify the size of the LU to be created in gigabytes as an integer from 1 to 1,024.</p> <p>Select from existing LUs Select this to use existing LUs. Select LUs to be used for the file system from the LUs area. Because part of the area is used as the management area in each LU, the total capacity of the LUs differs from the capacity that can be used for the file system.</p>

Item	Description
	<p>In the LUs area, capacities shown in GB, TB, or PB are rounded to the nearest two decimal places. Take this into account when calculating the total capacity.</p> <p>A hash mark (#) is displayed for LUs that are in an external storage system.</p> <p>- Add File System LUs ></p> <p>In the LUs area, select the LUs you want to use for the file system, and then click this button. The capacity of each selected LU must be 65 MB or more. If virtual LUs will be used, the total size of the selected LUs must be from 256 MB to 1 PB. If virtual LUs will not be used, the total size of the selected LUs must be from 130 MB to 1 PB.</p> <p>If you want to create a file system in a striping configuration, select 2 to 128 LUs that have the same capacity. The number of the selected LUs is the number of stripes. In addition, striping will be performed in the order the LUs are selected.</p> <p>- Add Work Space LUs ></p> <p>In the LUs area, select the LUs you want to add to the work space, and then click this button. The capacity of each selected LU must be equal to or larger than 33 MB. You can select a maximum of 128 LUs. The recommended value for the capacity of the work space differs depending on the capacity of the file system. For details about the recommended values for the capacity of the work space, see the <i>Installation and Configuration Guide</i>.</p> <p>- < Delete</p> <p>Click this button to delete an LU from Selected LUs.</p> <p>For details about how to create and allocate LUs, see the <i>Installation and Configuration Guide</i>.</p> <p>If the initial capacity of a created file system is less than 32 GB + 16 MB, the maximum capacity after expansion will be less than the displayed value. For details about the initial capacity of a created file system and the maximum capacity after expansion, see the <i>CLI Administrator's Guide</i>.</p>
Enable Quota	<p>Select this option to enable the quota functionality or manage the capacity of shares created in the file system.</p> <p>To enable the quota function that is disabled after creating a file system, you need to remount the file system. Because the mount processing takes a long time to complete, Hitachi Data Systems recommends that you enable the quota function.</p>
Export point owner	<p>Specify the owner and owner group for the shared directory.</p> <p>Export point owner user^{#2}</p> <p>Specify the owner of the shared directory.</p> <p>To specify a user registered in user mapping, use the following format:</p> <p><i>domain-name^{#3}\user-name</i></p> <p>Export point owner group^{#2}</p> <p>Specify the owner group for the shared directory.</p>

Item	Description
	To specify a group registered in user mapping, use the following format: <i>domain-name</i> # ³ \ <i>group-name</i>
#1:	This item can only be used when all of the following conditions are met: <ul style="list-style-type: none"> The storage system is a Hitachi AMS2000 or HUS100 series storage system and the IP addresses of both controllers are registered on the management server. The LUN Manager functionality is enabled for the storage system. The storage system is not made up of only pools. <p>If there is insufficient space in the existing RAID groups, a RAID5 group (15D+1P) or a RAID6 group (15D+2P) is created, depending on the RAID groups supported by the storage system. However, if 3 to 15 disk drives, in the case of RAID5, or 4 to 16 disk drives, in the case of RAID6, are available, a RAID group will be created using all of those disk drives. Note that RAID5 groups are created in storage systems that support both RAID5 and RAID6.</p> <p>#2: You cannot specify a Windows domain built-in user or group.</p> <p>#3: If you use the CIFS protocol and Active Directory authentication as the CIFS service authentication mode, specify the value set in Domain name (NetBIOS) in the Active Directory Authentication page of the Access Protocol Configuration dialog box for the domain name in Export point owner user and Export point owner group.</p>

Access Control tab

You can use the **Access Control** tab to specify attributes related to file share access permissions.

CIFS subtab

You can use the **CIFS** subtab to specify attributes related to CIFS share access permissions.

Table C-83 Information specified in the CIFS subtab of the Access Control tab in the Create and Share File System dialog box

Item	Description
Enable ACL # ¹	Select this check box to reference or set the ACL from the client. Note that you cannot set the ACL for the guest account (<i>nobody</i>). If you specify this setting, you cannot cancel it later.
Read only	Select this check box to allow access for the CIFS share in read-only mode. This check box is enabled for users or groups for which write access to the shared directory is allowed. Note that if the file system supports home-directory-roaming, you cannot share CIFS shares as read-only, so you cannot select this item.
Special permitted users/groups	To set permissions for a specific user or group separately from file share permissions, select the target user or group from the Users or Groups tab.

Item	Description
	<p>Add RW > Click this button to permit read-write access.</p> <p>Add RO > Click this button to permit read-only access.</p> <p>< Delete Click this button to delete users or groups from Special Permitted Users or Special Permitted Groups.</p> <p>Refresh Users and Groups Click this button to refresh information about users and groups.</p> <p>If you select the user or group whose permission has already been set and click Add RW > or Add RO >, the new permission will be applied.</p> <p>The total number of users and groups whose access permissions are set in Special permitted users/groups is limited to 100 or fewer per file share. Note that the following equation must be satisfied (the number of users is u, the number of groups is g, the total number of characters for user names is n, and the total number of characters for group names is m):</p> $u + 2g + n + m \leq 1024$ <p>(<=: Less than or equal to)</p> <p>Note that users and groups registered by using the user mapping functionality cannot be specified in the GUI.</p>
<p>Host/network based access restriction</p>	<p>To limit the CIFS clients that can access the CIFS share, specify, in the text box, the host name^{#2} or IP address of each CIFS client that is to be allowed access to the CIFS share. Alternatively, specify the network address^{#3} of the network to which each CIFS client belongs. To specify multiple CIFS clients, delimit clients by using commas (,). Note that you can specify no more than 5,631 characters in total. To allow all CIFS clients access to the CIFS share, do not specify anything in the text box.</p> <p>You must also select an option to specify whether the specified CIFS clients are to be allowed or denied access to the CIFS share.</p> <p>Notes:</p> <ul style="list-style-type: none"> - If hosts or networks with limited access are set in the CIFS service configuration definition (CIFS Service Management page of the Access Protocol Configuration dialog box), the setting applies to all file shares. To set hosts or networks with limited access for each CIFS share, do not set hosts or networks with limited access in the CIFS service configuration definition. - To specify the host name, edit the <code>/etc/hosts</code> file to add all the specified host names and IP addresses. If you do not add host names in the <code>/etc/hosts</code> file, the specified information might not take effect. Also, if any of the host names you specify for an IP address has been added as an alias after the first host name, file share access might not behave as specified. For details about how to edit the <code>/etc/hosts</code> file, see Edit System File page on page C-209. - Even if you permit access to the CIFS share, user authentication is carried out for the CIFS client.

Item	Description
Browsable share	Select this option to list the CIFS share names in the CIFS client environment.
Allow guest account access ^{#4}	<p>Select whether you permit access for guest accounts.</p> <p>Yes Allow access for guest accounts.</p> <p>No Do not allow access for guest accounts.</p> <p>Inherit CIFS service default Use the CIFS service configuration definitions.</p> <p>A guest account is handled as <code>nobody</code> (user-ID: 65534) regardless of CIFS service authentication modes. Therefore, for a CIFS share that is accessible with a guest account, set the access permissions taking into consideration that the CIFS share can be accessed by <code>nobody</code>. You cannot set the ACL for a guest account (<code>nobody</code>). However, if access with a guest account is not permitted at all in the CIFS service settings, the settings for individual CIFS shares do not apply.</p> <p>Note that if the file system supports home-directory-roaming, guest accounts are denied access by default. You cannot change this setting.</p>
Set access permissions only for the owner	In an Advanced-ACL-type file system, if only Owner has read or write permissions, select the Yes check box. Access permissions are not set for Group or Other (all users and groups).
Access permissions for new files	<p>To permit access to the CIFS share in read-write mode, set access permissions for Owner, Group, and Other when a new file is created.</p> <p>RW Select this option to permit read-write access.</p> <p>RO Select this option to permit read-only access.</p> <p>None Select this option to not permit read or write access.</p> <p>If RO or None is specified for Owner, even the owner will not be able to write to new files.</p> <p>If RO is set for Group, set RO or None for Other. To set None for Group, also set None for Other. If you set access permissions other than these for Other, Group access permissions set for files might be deleted when the files are updated.</p>
Access permissions for new directories	<p>To permit access to the CIFS share in read-write mode, set access permissions for Owner, Group, and Other when a new directory is created.</p> <p>RW Select this option to permit read-write access.</p> <p>RO Select this option to permit read-only access.</p> <p>None</p>

Item	Description
	<p>Select this option to not permit read or write access. Only searching is permitted.</p> <p>If you specify RO or None for Owner, even the owner will not be able to write to new directories.</p> <p>If you set RO for Group, set RO or None for Other as well. If you set None for Group, set None for Other as well. If you set access permissions other than these for Other, Group access permissions set for directories might be deleted when the directories are updated.</p>
<p>#1: Specify this item when creating a file system of the Classic ACL type.</p> <p>#2: You cannot specify the following names as the host name:</p> <ul style="list-style-type: none"> • ALL • FAIL • EXCEPT <p>#3: Specify the network address in the format below: <i>network-address/netmask</i> (example: 10.203.15.0/255.255.255.0)</p> <p>Specify a prefix length for the netmask for IPv6.</p> <p>#4: When the CIFS share settings and the CIFS service configuration definitions are different from each other, the CIFS share settings are applied. If Inherit CIFS service default is selected for the item, the settings specified in the CIFS service configuration definition are applied. In addition, after settings in the CIFS service configuration definition are changed, the new settings will be automatically applied.</p>	

NFS subtab

You can use the **NFS** subtab to specify attributes related to NFS share access permissions.

Table C-84 Information specified in the NFS subtab of the Access Control tab in the Create and Share File System dialog box

Item	Description
Hosts	<p>Specify the hosts allowed to access the NFS share, access permission, and a target to be mapped as an anonymous user. You can specify multiple hosts to access the NFS share.</p> <p>Add RW ></p> <p>Click this button to permit read-write access to the NFS share for the specified hosts by using the specified anonymous mapping setting.</p> <p>Add RO ></p> <p>Click this button to permit read-only access to the NFS share for the specified hosts by using the specified anonymous mapping setting.</p> <p>< Delete</p> <p>Click this button to delete a host from Selected Hosts.</p> <p>Note that the total length (specified length + 5 bytes) of the specified host names or network addresses must be less than 1,258 bytes.</p>

Item	Description
	<p>Host/network Specify 255 characters or fewer. Specify a host name beginning with an alphabetic character and consisting of alphanumeric characters, hyphens (-), and underscores (_). If you specify a host alias, the official host name also must be 255 characters or fewer. In addition to the host name and the IP address, you can use the following formats:</p> <p>Netgroup Specify an NIS netgroup. For example, for @group, only the host segment is extracted from the netgroup members.</p> <p>IP network To permit all hosts in the subnetwork to access the NFS share, specify the IP address and the netmask in the following format: <i>address/netmask</i> The netmask can be specified in dotted decimal format or as a prefix length (Specify a prefix length for IPv6).</p> <p>DNS domain Specify the name of the DNS domain to which NFS clients belong, with a period (.) added at the beginning of the name. Example: .example.com</p> <p>Wild card To specify all hosts, use an asterisk (*) as a wild card.</p> <p>When the NFS client machine has multiple network interfaces communicating with the HDI system, specify the hosts and networks allowed to access the NFS share in one of the following formats:</p> <ul style="list-style-type: none"> • Use a wild card (*). • Specify the IP addresses of all network interfaces used on the NFS client side. • Specify the host names for all network interfaces used on the NFS client side. • Specify an IP network that contains the IP addresses of all network interfaces used on the NFS client side. • Specify a netgroup that contains the host names for all network interfaces used on the NFS client side. • Specify a DNS domain that contains the host names for all network interfaces used on the NFS client side.
	<p>Security flavor Specify a security flavor. Use the default settings^{#1}</p>

Item	Description	
		<p>Select this to use the NFS service configuration definitions.</p> <p>Use the original settings</p> <p>Select this to specify different settings from the NFS service configuration definitions.</p> <p>Select one or more of the following check boxes:</p> <ul style="list-style-type: none"> - sys <p>Select this to use the UNIX (AUTH_SYS) authentication.</p> <ul style="list-style-type: none"> - krb5 <p>Select this to use the Kerberos authentication.</p> <ul style="list-style-type: none"> - krb5i <p>Select this to use the data integrity function in addition to the Kerberos authentication.</p> <ul style="list-style-type: none"> - krb5p <p>Select this to use the data integrity function and the privacy function in addition to the Kerberos authentication.</p>
	Anonymous mapping ^{#2}	<p>Select users who can access the HDI system from the hosts allowed to access the NFS share specified in the Host/network and those you want to map as anonymous users.</p> <p>Not applied</p> <p>Select this option to disable anonymous user mapping.</p> <p>For root user</p> <p>Select this option to map only the root user as an anonymous user.</p> <p>For anyone</p> <p>Select this option to map every user as an anonymous user.</p>
UID for anonymous mapping	Specify the user ID for accessing as an anonymous user. Specify a value in the range from 0 to 65535.	
GID for anonymous mapping	Specify the group ID for accessing as an anonymous user. Specify a value in the range from 0 to 65535.	
<p>#1: The NFS service configuration definitions at the time a file share is created will be used. Even if you create a file share, and then change the settings of the NFS service configuration definitions, the changes will not be applied to the existing file shares.</p> <p>#2: If you specify For root user, UID for anonymous mapping and GID for anonymous mapping will be used only for the root users after user mapping in the NFS service is performed. If you specify For anyone, UID for anonymous mapping and GID for anonymous mapping will supersede the user mapping settings in the NFS service.</p>		

Directory subtab (A file system of the Advanced ACL type)

You can use the **Directory** subtab, for the Advanced ACL type, to set the ACL for the shared directory.

The **Directory** subtab does not appear if you select **Use existing directory as is** under **Export point owner** on the **Basic** tab.

Table C-85 Information specified in the Directory subtab of the Access Control tab in the Create and Share File System dialog box for a file system of the Advanced ACL type

Item	Description
ACL registered users and groups	<p>Set the ACE (access control entry) for the shared directory.</p> <p>User Add > Click this button to add the ACE of a specified user.</p> <p>Group Add > Click this button to add the ACE of a specified group.</p> <p>< Delete Click this button to delete a user or group ACE from ACL Registered Users and Groups.</p>
	<p>User or group name</p> <p>Specify the name of the target user or group. Windows does not distinguish between uppercase and lowercase alphabetic characters.</p> <p>You can also specify the following Windows domain built-in accounts:</p> <ul style="list-style-type: none"> • Everyone Specify as a group (Group Add >). • CREATOR GROUP Specify as a group (Group Add >). • CREATOR OWNER Specify as a user (User Add >).
	<p>Permissions</p> <p>Select the appropriate check box to allow or deny access. Items for which you selected Allow are the only permitted operations.</p> <p>Full control Full control permission</p> <p>Modify Modify permission</p> <p>Read and execute Read and run permission</p> <p>Read Read permission</p> <p>Write Write permission</p> <p>List folder contents Permission to list folder contents</p>

Item	Description	
	Apply these ACLs to this folder, sub-folders, and files	<p>Select the check box to apply the ACLs to the sub-folders and files in that folder (shared directory). If you leave the check box cleared, the ACLs will apply only to the folder itself.</p> <p>Hitachi Data Systems recommends that you do not select this check box when creating NFS shares.</p>

Directory subtab (A file system of the Classic ACL type)

You can use the **Directory** subtab, for the Classic ACL type, to set access permissions for the shared directory.

The **Directory** subtab does not appear if you select **Use existing directory as is** under **Export point owner** on the **Basic** tab.

Table C-86 Information specified in the Directory subtab of the Access Control tab in the Create and Share File System dialog box for a file system of the Classic ACL type

Item	Description
Export point permissions	<p>Set access permissions of Owner, Group, and Other for the shared directory.</p> <p>RW Select this option to permit read-write access. Execution authority for the directory is permitted.</p> <p>RO Select this option to permit read-only access. Execution authority for the directory is permitted.</p> <p>None Select this option to not permit read, write, or execution permissions for the directory. This option can be set for Group and Other.</p>
Unix sticky bit	Select this option to set the sticky bit for the shared directory.

WORM tab

You can use the **WORM** tab to specify the WORM settings for a file system.

Table C-87 Information specified in the WORM tab in the Create and Share File System dialog box

Item	Description
Enable WORM	Select this option to enable WORM functionality. Note that after creating a file system, you can no longer change the setting for whether the WORM functionality is enabled or disabled.

Item	Description
Retention period	<p>Specify the minimum and maximum retention periods.</p> <p>Minimum</p> <p>Specify the minimum retention period. Specify a value from 0 minutes to 36,500 days in the day(s), hour(s), and minute(s) text boxes. To set an indefinite time period for the minimum, select the Infinite check box.</p> <p>Maximum</p> <p>Specify the maximum retention period. Specify a value from 1 minute to 36,500 days in the day(s), hour(s), and minute(s) text boxes. The value must be no less than Minimum or Default retention period in Auto commit.</p> <p>To set an indefinite time period for the maximum, select the Infinite check box. If the Infinite check box is selected for Minimum or Default retention period in Auto commit, the Infinite check box is automatically selected for this item as well.</p>
Auto commit	<p>Specify the autocommit settings.</p> <p>Enable</p> <p>Select the Yes check box to enable autocommit. Note that if you enable autocommit, you can no longer disable it.</p> <p>Commit mode</p> <p>Selects the mode of the autocommit according to the following radio buttons:</p> <ul style="list-style-type: none"> - Manual <p>Select this button to enable the autocommit in manual mode.</p> <p>In manual mode, files that are specified as read-only files by clients are subject to the autocommit functionality.</p> <ul style="list-style-type: none"> - Auto <p>Select this button to enable the autocommit in auto mode.</p> <p>In auto mode, all ordinary files, except for the system files and files in the system directories, are subject to the autocommit functionality.</p> <p>Time until committed</p> <p>Specify how long to wait until files are turned into WORM files. Specify a value from 1 minute to 36,500 days in the day(s), hour(s), and minute(s) text boxes. After you have specified the setting, you cannot change it.</p> <p>Default retention period</p> <p>Specify the retention period for the files for which an autocommit has been performed. Specify a value from 1 minute to 36,500 days in the day(s), hour(s), and minute(s) text boxes. The value must be within the range specified by Minimum and Maximum in Retention period.</p> <p>To set an indefinite time period for the retention period, select the Infinite check box. If the Infinite check box is selected for Minimum in Retention period, the Infinite check box is automatically selected for this item as well.</p>

Item	Description
Enable rename of empty directories	Select to allow clients to change the names of empty directories.

Namespace tab

You can use the **Namespace** tab to specify namespace information. The information you can specify depends on how HCP data is shared.

Table C-88 Information specified in the Namespace tab in the Create and Share File System dialog box (when Off is selected for Content sharing)

Item	Description
Migration schedule	<p>Start date Specify the date for the first migration in the format of YYYY-MM-DD.</p> <p>Interval Specify the interval between migrations.</p> <p>Start time Specify the migration start time.</p> <p>Maximum duration Specify the period for continuing migration processing (0 to 999 hours). If you do not want to limit the time, leave the entry blank or specify 0.</p>
Namespace-access account	Select Create and specify a password to create an account for accessing the namespace from another HDI system.
Use file version restore	<p>Select Yes to make the past version files (past version directories) migrated to the HCP system available to clients. Additionally, select a radio button to set the method of keeping past-version directories in the <code>.history</code> directory.</p> <p>To allow CIFS clients to view to the <code>.history</code> directory, change the settings for the shared directory so that all files and folders are shown.</p> <p>Custom schedule Select this item to keep past-version directories that use custom scheduling. For details about custom scheduling of the file version restore functionality, see the <i>Installation and Configuration Guide</i>.</p> <p>Keep 15-MINUTE versions for: The oldest past version directory with 15-minute time units (hour <i>n</i>, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. Specify any of the following: 15, 30, 45, and 60.</p> <p>Keep HOURLY versions for: The oldest past version directory with hourly time units (hour <i>n</i>, minutes 00 to 59) is kept for the number of units specified. Specify in the range from 1 to 48.</p>

Item	Description
	<p>Keep DAILY versions for: The oldest past version directory with daily time units (day <i>n</i>, 00:00 to 23:59) is kept for the number of units specified. Specify in the range from 1 to 62.</p> <p>Keep WEEKLY versions for: The oldest past version directory with weekly time units (week <i>n</i>, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. Specify in the range from 1 to 52.</p> <p>Keep MONTHLY versions for: The oldest past version directory with monthly time units (month <i>n</i>, 1st day, 00:00 to <i>last-day</i>, 23:59) is kept for the number of units specified. Specify in the range from 1 to 36.</p> <p>Keep YEARLY versions for: The oldest past version directory with yearly time units (year <i>n</i>, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. Specify in the range from 1 to 100.</p> <p>Period to hold[#]</p> <p>Select this item to keep past-version directories in every interval between migrations. Specify the period to keep the past version directories in the range from 1 to 36,500 (in days).</p>
<p>[#]: Note that the retention period of past version directories depends on the capacity of the namespace in the migration destination. For information on how to estimate the capacity requirement for a namespace in a migration destination, see the <i>Installation and Configuration Guide</i>.</p>	

Table C-89 Information specified in the Namespace tab in the Create and Share File System dialog box (when On (Read-Only) is selected for Content sharing)

Item	Description
Namespace FQDN	Specify the fully qualified domain name of the namespace that is used for referencing other HDI data as read-only via the linked HCP.
External HCP host name	If the HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the HCP system.
Namespace-access account	Specify the user name and password for the account for accessing the namespace. If you click the Test Connection for Primary button after specifying information, you can check the connection with the HCP system.
Replica	If you are using the HCP replication functionality, select the Use check box. System name Specify the replica HCP system name to Fully Qualified Domain Name. External Replica HCP host name

Item	Description
	<p>If the replica HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the replica HCP system.</p> <p>After specifying the information, click the Test Connection for Replica button to check whether you can connect to the replica HCP system.</p>

Table C-90 Information specified in the Namespace tab in the Create and Share File System dialog box (when On (Read/Write) is selected for Content sharing)

Item	Description
Namespace settings	<p>If you did not specify Yes for Create namespace in the Basic tab, specify the name of the namespace for the HCP system to which data will be migrated.</p> <p>After the namespace name is specified, click the Test Connection button to confirm that you can connect to the HCP system.</p>
Use file version restore	<p>Select Yes to make the past version files (past version directories) migrated to the HCP system available to clients. Additionally, select a radio button to set the method of keeping past-version directories in the <code>.history</code> directory.</p> <p>To allow CIFS clients to view to the <code>.history</code> directory, change the settings for the shared directory so that all files and folders are shown.</p> <p>Custom schedule</p> <p>Select this item to keep past-version directories that use custom scheduling. For details about custom scheduling of the file version restore functionality, see the <i>Installation and Configuration Guide</i>.</p> <p>Keep 15-MINUTE versions for: The oldest past version directory with 15-minute time units (hour <i>n</i>, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. Specify any of the following: 15, 30, 45, and 60.</p> <p>Keep HOURLY versions for: The oldest past version directory with hourly time units (hour <i>n</i>, minutes 00 to 59) is kept for the number of units specified. Specify in the range from 1 to 48.</p> <p>Keep DAILY versions for: The oldest past version directory with daily time units (day <i>n</i>, 00:00 to 23:59) is kept for the number of units specified. Specify in the range from 1 to 62.</p> <p>Keep WEEKLY versions for: The oldest past version directory with weekly time units (week <i>n</i>, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. Specify in the range from 1 to 52.</p>

Item	Description
	<p>Keep MONTHLY versions for: The oldest past version directory with monthly time units (month <i>n</i>, 1st day, 00:00 to <i>last-day</i>, 23:59) is kept for the number of units specified. Specify in the range from 1 to 36.</p> <p>Keep YEARLY versions for: The oldest past version directory with yearly time units (year <i>n</i>, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. Specify in the range from 1 to 100.</p> <p>Period to hold[#]</p> <p>Select this item to keep past-version directories in every interval between migrations. Specify the period to keep the past version directories in the range from 1 to 36,500 (in days).</p>
<p>[#]: Note that the retention period of past version directories depends on the capacity of the namespace in the migration destination. For information on how to estimate the capacity requirement for a namespace in a migration destination, see the <i>Installation and Configuration Guide</i>.</p>	

Table C-91 Information specified in the Namespace tab in the Create and Share File System dialog box (when Home directory is selected for Content sharing)

Item	Description
Namespace settings	<p>If you did not specify Yes for Create namespace in the Basic tab, specify the name of the namespace for the HCP system to which data will be migrated.</p> <p>After the namespace name is specified, click the Test Connection button to confirm that you can connect to the HCP system.</p>
Use file version restore	<p>Select Yes to make the past version files (past version directories) migrated to the HCP system available to clients. Additionally, select a radio button to set the method of keeping past-version directories in the <code>.history</code> directory.</p> <p>To allow CIFS clients to view to the <code>.history</code> directory, change the settings for the shared directory so that all files and folders are shown.</p> <p>Custom schedule</p> <p>Select this item to keep past-version directories that use custom scheduling. For details about custom scheduling of the file version restore functionality, see the <i>Installation and Configuration Guide</i>.</p> <p>Keep 15-MINUTE versions for: The oldest past version directory with 15-minute time units (hour <i>n</i>, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. Only 60 can be specified.</p> <p>Keep HOURLY versions for: The oldest past version directory with hourly time units (hour <i>n</i>, minutes 00 to 59) is kept for the number of units specified. Specify in the range from 1 to 48.</p>

Item	Description
	<p>Keep DAILY versions for: The oldest past version directory with daily time units (day <i>n</i>, 00:00 to 23:59) is kept for the number of units specified. Specify in the range from 1 to 62.</p> <p>Keep WEEKLY versions for: The oldest past version directory with weekly time units (week <i>n</i>, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. Specify in the range from 1 to 52.</p> <p>Keep MONTHLY versions for: The oldest past version directory with monthly time units (month <i>n</i>, 1st day, 00:00 to <i>last-day</i>, 23:59) is kept for the number of units specified. Specify in the range from 1 to 36.</p> <p>Keep YEARLY versions for: The oldest past version directory with yearly time units (year <i>n</i>, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. Specify in the range from 1 to 100.</p> <p>Period to hold[#]</p> <p>Select this item to keep past-version directories in every interval between migrations. Specify the period to keep the past version directories in the range from 1 to 36,500 (in days).</p>
<p>[#]: Note that the retention period of past version directories depends on the capacity of the namespace in the migration destination. For information on how to estimate the capacity requirement for a namespace in a migration destination, see the <i>Installation and Configuration Guide</i>.</p>	

Advanced tab

You can use the **Advanced** tab to specify attributes of the file share and the file system in which the file share is created as necessary.

CIFS subtab

You can use the **CIFS** subtab to specify attributes of the CIFS share as necessary.



Note: If the CIFS service configuration definition settings do not allow the CIFS share settings to be automatically reloaded and you added a CIFS share during degenerated operation, to enable the CIFS share settings, perform a failback operation, and then restart the CIFS services on both nodes. For details about how to perform a failback operation, see [Browse Cluster Status page on page C-271](#). For details about how to restart a CIFS service, see [List of Services page on page C-218](#).

Table C-92 Information specified in the CIFS subtab of the Advanced tab in the Create and Share File System dialog box

Item	Description
CIFS share name	Specify the CIFS share name.

Item	Description
	<p>Specify 80 characters or fewer.</p> <p>You can use any alphanumeric character, exclamation mark (!), hash mark (#), dollar sign (\$), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), plus sign (+), comma (,), hyphen (-), period (.), semicolon (;), equal sign (=), at mark (@), left square bracket ([), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), right curly bracket (}), tilde (~), or space. You can also specify multi-byte characters. However, the string cannot contain only a dollar sign or periods (e.g., \$, ., or ..) and cannot end with a period (e.g., Abc.). If the string ends with a dollar sign, you cannot specify a period just before that dollar sign (e.g., Abc.\$). The space specified at the end of the string will be removed.</p> <p>If you use a percent sign (%) in the CIFS share name, make sure the percent sign is not used in any of the following combinations:</p> <p>%D, %G, %H, %I, %L, %M, %N, %P, %R, %S, %T, %U, %V, %a, %d, %g, %h, %i, %m, %p, %u, %v, %w, %\$</p> <p>In addition, the CIFS share name cannot be global, homes, printers, admin\$, c\$, global\$, homes\$, ipc\$, or printers \$.</p> <p>Windows does not distinguish between uppercase and lowercase alphabetic characters. Specify a unique name on the physical node regardless of uppercase and lowercase alphabetic characters.</p> <p>If omitted, the share name of the file system is used as a CIFS share name.</p>
<p>Comment shown to CIFS clients</p>	<p>Specify the CIFS share comment, using 256 characters or fewer.</p> <p>You can use any alphanumeric character, exclamation mark (!), hash mark (#), dollar sign (\$), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), forward slash (/), colon (:), left angle bracket (<), right angle bracket (>), question mark (?), at mark (@), left square bracket ([), backslash (\), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (), right curly bracket (}), and tilde (~). In addition, you can specify multi-byte characters. You can also specify a space, but a string cannot start or end with a space. Also, a string cannot end with a backslash (\).</p>
<p>Enable auto creation of home directory</p>	<p>Select this option to use the function for automatically creating a home directory in the CIFS share.</p> <p>However, if the file share was created in a home-directory-roaming file system, the function for automatically creating a home directory is enabled by default. To disable the function, use the <code>cifsedit</code> command.</p>

Item	Description
Users allowed to change file time stamp ^{#1#2}	<p>Select the users who can update the time-stamps of files in the CIFS share. To share files using only the CIFS protocol, select Write permitted users.</p> <p>Write permitted users Enable all users allowed to write files to update the time-stamps.</p> <p>Owner only Enable only the file owner to update the time-stamps.</p> <p>Inherit CIFS service default Use the CIFS service configuration definitions.</p>
Disk synchronization policy ^{#2}	<p>Specify the operations for write requests from CIFS clients to the CIFS share.</p> <p>At write and close Select this to write synchronously with a write request or a close request.</p> <p>At close Select this to write synchronously with a close request.</p> <p>Routine disk flush only Select this to write at a fixed interval, regardless of when write requests and close requests are made.</p> <p>Inherit CIFS service default Use the CIFS service configuration definitions.</p> <p>For details about how the system works for each setting, see the notes in Table C-202 Information specified in the CIFS Service Management page (Setting Type: Performance) on page C-236.</p>
Windows® client access policy ^{#2}	<p>Select the method for processing accesses from Windows clients.</p> <p>Parallel Process accesses in parallel.</p> <p>Serial Process accesses serially.</p> <p>Inherit CIFS service default Use the CIFS service configuration definitions.</p>
Allow CIFS client cache ^{#2}	<p>Specify whether the updated data of the file in the CIFS share is cached to the client.</p> <p>Specify No for read-write-content-sharing file systems. If the updated data of the file in the CIFS share is cached on the client, the update date might not be reflected properly on other sites.</p> <p>Yes Cache data. The performance can be improved by caching the updated data for files in a CIFS share to the client. However, data reliability might be degraded if a failure occurs in the CIFS client or network.</p>

Item	Description
	<p>For the file systems listed below, we recommend also setting Allow read-only client cache for access conflicts values to Yes, because there is a risk that the client cache will fail to validate.</p> <ul style="list-style-type: none"> - File systems that migrate data to an HCP system <p>No</p> <p>Do not cache data.</p> <p>Inherit CIFS service default</p> <p>Use the CIFS service configuration definitions.</p>
<p>Allow read-only client cache for access conflicts^{#2}</p>	<p>Specify whether to use a read-only client cache when multiple CIFS clients simultaneously attempt to access a file.</p> <p>Yes</p> <p>Select this to use a read-only client cache. This improves system performance because data is cached on the client PC when a CIFS client opens a file. This item can be selected if Yes is selected under Allow CIFS client cache. In addition, this item can be selected if Inherit CIFS service default is selected under Allow CIFS client cache when the CIFS service configuration definitions are set to cache updates to the files in CIFS shares.</p> <p>No</p> <p>Select this to not use a read-only client cache.</p> <p>Inherit CIFS service default</p> <p>Select this if the CIFS service configuration definitions determine whether a read-only client cache is used.</p> <p>Note that we recommend that you do not use the read-only client cache if you also want to use the NFS protocol to access the file shares because changes might not be applied. If you need to use the read-only client cache, we recommend implementing file sharing individually for each protocol to ensure that the NFS protocol is not used to access the share.</p>
<p>Allow Access Based Enumeration^{#2}</p>	<p>Specify whether to enable access-based enumeration.</p> <p>Yes</p> <p>Select this to enable access-based enumeration.</p> <p>No</p> <p>Select this to disable access-based enumeration.</p> <p>Inherit CIFS service default</p> <p>Select this if the CIFS service configuration definitions determine whether access-based enumeration is enabled.</p>
<p>Use Volume Shadow Copy Service</p>	<p>This item is not supported.</p>
<p>SMB encryption^{#2#3}</p>	<p>Specify whether communication with the CIFS client is to be encrypted.</p> <p>The setting for this item is only valid if you select SMB 3.0 for the SMB protocol in CIFS Service Management page (Setting Type: Basic) of the Access Protocol</p>

Item	Description
	<p>Configuration dialog box. If you select an option other than SMB 3.0 for the SMB protocol, select Disable or set communication with the CIFS client not to be encrypted in the configuration definition of the CIFS service, and then select the Inherit CIFS service default.</p> <p>Auto Select this option if communication with the client is to be encrypted only when the client supports encryption.</p> <p>Mandatory Select this option if communication with the client is always to be encrypted. Only clients that support SMB 3.0 or later can access a CIFS share. Note that clients cannot access a CIFS share by using guest accounts.</p> <p>Disable Select this option if communication with the client is not to be encrypted.</p> <p>Inherit CIFS service default Use the CIFS service configuration definitions.</p>
	<p>#1: Specify when creating a file system of the Classic ACL type.</p> <p>#2: When the CIFS share settings and the CIFS service configuration definitions are different from each other, the CIFS share settings are applied. If Inherit CIFS service default is selected for the item, the settings specified in the CIFS service configuration definition are applied. In addition, after settings in the CIFS service configuration definition are changed, the new settings will be automatically applied.</p> <p>#3: If Mandatory is selected in SMB encryption for some CIFS shares and Disable is selected for others, select Auto. Note that when Disable is selected in SMB encryption for the CIFS share, if you select Mandatory, the CIFS share will become inaccessible. If Mandatory or Disable is selected in SMB encryption in the CIFS service configuration definitions, select Inherit CIFS service default.</p>

File System subtab

You can use the **File System** subtab to specify attributes of the file system in which the file share is created as necessary.

Table C-93 Information specified in the File System subtab of the Advanced tab in the Create and Share File System dialog box

Item	Description
Maximum capacity for i-nodes	Specify the maximum percentage amount of file system capacity that can be used as an inode, as an integer from 1 to 100. The maximum capacity that can be used as an inode is 1 TB.
Record last access time	Select this option to update the last access time (<i>atime</i>) each time a client accesses a file in the file system.

Item	Description
Enable Advanced ACL type	Select this option to create a file system of the Advanced ACL type. When created as the Advanced ACL type, the file system cannot be changed to Classic ACL. For a WORM file system, you cannot change the ACL type after creation. If you do not select this check box, the created file system will be the Classic ACL type. Leave the file system as the Classic ACL type if it is to be used primarily for NFS shares.
CIFS bypass traverse checking	Select this option to enable CIFS bypass traverse checking. This option is not displayed if in the Basic tab, Home directory is selected for Content sharing .

Striping subtab

You can use the **Striping** subtab to specify the striping settings for the file system.

Table C-94 Information specified in the Striping subtab of the Advanced tab in the Create and Share File System dialog box

Item	Description
Enable striping for the file system	Select Yes when you want to create a file system in a striping configuration. In addition, specify the stripe size for Size in KB.

Create File System dialog box

You can use the **Create File System** dialog box to create file systems that have a maximum size of 1 PB (total LU capacity).

When you create a file system, it is automatically mounted as read-write enabled at the following mount point:

/mnt/file-system-name

You can create and mount a maximum of 511 file systems per cluster.

To create file shares for subdirectories in the file system, create the file system in the **Create File System** dialog box, and then add a file share for each subdirectory that you want to share. For details about how to share a file system in its entirety, [Create and Share File System dialog box on page C-103](#).

The volume manager is always used when you use the GUI to create file systems.

If you want to migrate data in the file system to the HCP system, set up data migration for the file system.



Tip:

- You can use commands to set even more attributes for the file system.
- If you want to mount the file system as read-only, use either of the following procedures:
 - After creating the file system, unmount it, and then mount it again.
 - Use commands to create and mount the file system.

To open the **Create File System** dialog box, on the **File System** subtab of the **File Systems** tab in the *physical-node* window ([physical-node window on page C-91](#)), click **Create**.

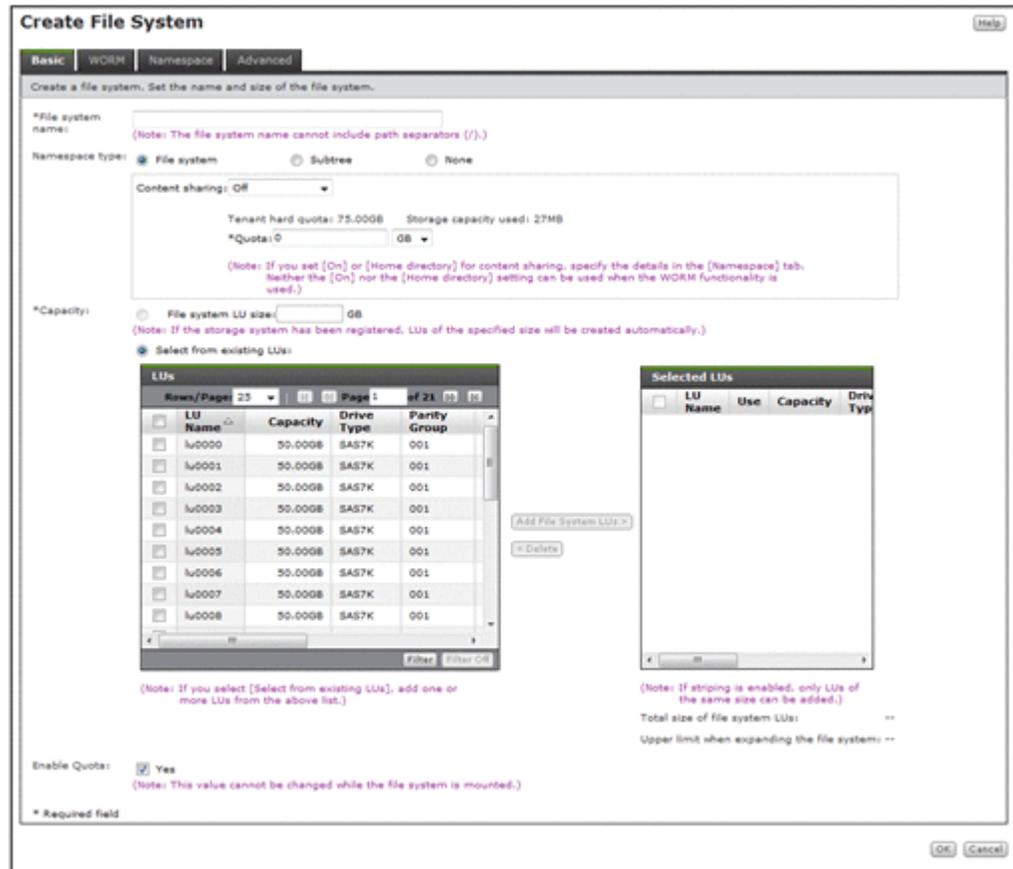


Table C-95 Information shown in the Create File System dialog box

Item	Description	See
Basic	Specify basic attributes relating to the file system.	Basic tab on page C-128
WORM	Specify the WORM settings for the file system.	WORM tab on page C-130
Namespace	Specify HCP namespace information.	Namespace tab on page C-132
Advanced	Specify attributes of the file system as necessary.	Advanced tab on page C-136

Item	Description		See
	File System	Specify attributes of the file system in which the file share is created as necessary.	File System subtab on page C-136
	Striping	Specify information about the striping settings for the file system.	Striping subtab on page C-136

Basic tab

You can use the **Basic** tab to specify the basic attributes relating to the file system.

Table C-96 Information specified in the Basic tab in the Create File System dialog box

Item	Description
File System Name	Enter the name of the file system. The name must be unique within the cluster. Enter no more than 16 alphanumeric characters and underscores (_).
Namespace type	<p>Specify how to link to the HCP system.</p> <p>File system The file system is linked to the HCP system at the file system level.</p> <p>Subtree The file system is linked to the HCP system at the share level. Note, however, that you cannot select Subtree if an entire file system is shared.</p> <p>None An HCP namespace is not used.</p> <p>For Content sharing, select how data is to be shared with other HDI systems via the linked HCP.</p> <ul style="list-style-type: none"> • If you do not want to synchronize data with other HDI systems, select Off, and then specify the hard quota that you want to allocate to the namespace for Quota. Specify a value smaller than the Tenant hard quota value. • To reference other HDI data as read-only, select On (Read-Only). • To share data among HDI systems by using the read-write-content-sharing functionality, select On (Read/Write). To create a namespace, select Yes for Create namespace, and then specify the hard quota that you want to allocate to the namespace for Quota. Specify a value smaller than the Tenant hard quota value. If you select On (Read/Write), you need to allocate the namespace to the file system. • To enable roaming among HDI systems for home directory data created for each end user, select Home directory. To create a namespace, select Yes for Create

Item	Description
	<p>namespace, and then specify the hard quota that you want to allocate to the namespace for Quota. Specify a value smaller than the Tenant hard quota value. If you select Home directory, you need to allocate the namespace to the file system.</p>
<p>Capacity</p>	<p>Specify the capacity of the file system.</p> <p>Note that if you want to create a file system in a striping configuration, select Select from existing LUs.</p> <p>File system LU size#</p> <p>Select this to automatically create an LU to be used for the file system. In the text box, specify the size of the LU to be created in gigabytes as an integer from 1 to 1,024.</p> <p>Select from existing LUs</p> <p>Select this to use existing LUs.</p> <p>Select LUs to be used for the file system from the LUs area.</p> <p>Because part of the area is used as the management area in each LU, the total capacity of the LUs differs from the capacity that can be used for the file system.</p> <p>In the LUs area, capacities shown in GB, TB, or PB are rounded to the nearest two decimal places. Take this into account when calculating the total capacity.</p> <p>A hash mark (#) is displayed for LUs that are in an external storage system.</p> <p>- Add File System LUs ></p> <p>In the LUs area, select the LUs you want to use for the file system, and then click this button. The capacity of each selected LU must be 65 MB or more. If virtual LUs will be used, the total size of the selected LUs must be from 256 MB to 1 PB. If virtual LUs will not be used, the total size of the selected LUs must be from 130 MB to 1 PB.</p> <p>If you want to create a file system in a striping configuration, select 2 to 128 LUs that have the same capacity. The number of the selected LUs is the number of stripes. In addition, striping will be performed in the order the LUs are selected.</p> <p>- Add Work Space LUs ></p> <p>In the LUs area, select the LUs you want to add to the work space, and then click this button. The capacity of each selected LU must be equal to or larger than 33 MB. You can select a maximum of 128 LUs. The recommended value for the capacity of the work space differs depending on the capacity of the file system. For details about the recommended values for the capacity of the work space, see the <i>Installation and Configuration Guide</i>.</p> <p>- < Delete</p> <p>Click this button to delete an LU from Selected LUs.</p> <p>For details about how to create and allocate LUs, see the <i>Installation and Configuration Guide</i>.</p>

Item	Description
	If the initial capacity of a created file system is less than 32 GB + 16 MB, the maximum capacity after expansion will be less than the displayed value. For details about the initial capacity of a created file system and the maximum capacity after expansion, see the <i>CLI Administrator's Guide</i> .
Enable Quota	Select this check box to enable the quota functionality or manage the capacity of shares created in the file system. To enable the quota function that is disabled after creating a file system, you need to remount the file system. Because the mount processing takes a long time to complete, Hitachi Data Systems recommends that you enable the quota function.
<p>#: This item can only be used when all of the following conditions are met:</p> <ul style="list-style-type: none"> • The storage system is a Hitachi AMS2000 or HUS100 series storage system and the IP addresses of both controllers are registered on the management server. • The LUN Manager functionality is enabled for the storage system. • The storage system is not made up of only pools. <p>If there is insufficient space in the existing RAID groups, a RAID5 group (15D+1P) or a RAID6 group (15D+2P) is created, depending on the RAID groups supported by the storage system. However, if 3 to 15 disk drives, in the case of RAID5, or 4 to 16 disk drives, in the case of RAID6, are available, a RAID group will be created using all of those disk drives. Note that RAID5 groups are created in storage systems that support both RAID5 and RAID6.</p>	

WORM tab

You can use the **WORM** tab to specify the WORM settings for a file system.

Table C-97 Information specified in the WORM tab in the Create File System dialog box

Item	Description
Enable WORM	Select this option to enable WORM functionality. Note that after creating a file system, you can no longer change the setting for whether the WORM functionality is enabled or disabled.
Retention period	Specify the minimum and maximum retention periods. Minimum Specify the minimum retention period. Specify a value from 0 minutes to 36,500 days in the day(s) , hour(s) , and minute(s) text boxes. To set an indefinite time period for the minimum, select the Infinite check box. Maximum Specify the maximum retention period. Specify a value from 1 minute to 36,500 days in the day(s) , hour(s) , and minute(s) text boxes. The value must be no less than Minimum or Default retention period in Auto commit .

Item	Description
	<p>To set an indefinite time period for the maximum, select the Infinite check box. If the Infinite check box is selected for Minimum or Default retention period in Auto commit, the Infinite check box is automatically selected for this item as well.</p>
<p>Auto commit</p>	<p>Specify the autocommit settings.</p> <p>Enable</p> <p>Select the Yes check box to enable autocommit. Note that if you enable autocommit, you can no longer disable it.</p> <p>Commit mode</p> <p>Selects the mode of the autocommit according to the following radio buttons:</p> <ul style="list-style-type: none"> - Manual <p>Select this button to enable the autocommit in manual mode.</p> <p>In manual mode, files that are specified as read-only files by clients are subject to the autocommit functionality.</p> <ul style="list-style-type: none"> - Auto <p>Select this button to enable the autocommit in auto mode.</p> <p>In auto mode, all ordinary files, except for the system files and files in the system directories, are subject to the autocommit functionality.</p> <p>Time until committed</p> <p>Specify how long to wait until files are turned into WORM files. Specify a value from 1 minute to 36,500 days in the day(s), hour(s), and minute(s) text boxes. After you have specified the setting, you cannot change it.</p> <p>Default retention period</p> <p>Specify the retention period for the files for which an autocommit has been performed. Specify a value from 1 minute to 36,500 days in the day(s), hour(s), and minute(s) text boxes. The value must be within the range specified by Minimum and Maximum in Retention period.</p> <p>To set an indefinite time period for the retention period, select the Infinite check box. If the Infinite check box is selected for Minimum in Retention period, the Infinite check box is automatically selected for this item as well.</p>
<p>Enable rename of empty directories</p>	<p>Select to allow clients to change the names of empty directories.</p>

Namespace tab

You can use the **Namespace** tab to specify namespace information. The information you can specify depends on how HCP data is shared.

Table C-98 Information specified in the Namespace tab in the Create File System dialog box (when Off is selected for Content sharing)

Item	Description
Migration schedule	<p>Start date Specify the date for the first migration in the format of YYYY-MM-DD.</p> <p>Interval Specify the interval between migrations.</p> <p>Start time Specify the migration start time.</p> <p>Maximum duration Specify the period for continuing migration processing (0 to 999 hours). If you do not want to limit the time, leave the entry blank or specify 0.</p>
Namespace-access account^{#1}	<p>Select Create and specify a password to create an account for accessing the namespace from another HDI system.</p>
Use file version restore	<p>Select Yes to make the past version files (past version directories) migrated to the HCP system available to clients. Additionally, select a radio button to set the method of keeping past-version directories in the <code>.history</code> directory.</p> <p>To allow CIFS clients to view to the <code>.history</code> directory, change the settings for the shared directory so that all files and folders are shown.</p> <p>Custom schedule</p> <p>Select this item to keep past-version directories that use custom scheduling. For details about custom scheduling of the file version restore functionality, see the <i>Installation and Configuration Guide</i>.</p> <p>Keep 15-MINUTE versions for: The oldest past version directory with 15-minute time units (hour <i>n</i>, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. Specify any of the following: 15, 30, 45, and 60.</p> <p>Keep HOURLY versions for: The oldest past version directory with hourly time units (hour <i>n</i>, minutes 00 to 59) is kept for the number of units specified. Specify in the range from 1 to 48.</p> <p>Keep DAILY versions for: The oldest past version directory with daily time units (day <i>n</i>, 00:00 to 23:59) is kept for the number of units specified. Specify in the range from 1 to 62.</p> <p>Keep WEEKLY versions for: The oldest past version directory with weekly time units (week <i>n</i>, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. Specify in the range from 1 to 52.</p>

Item	Description
	<p>Keep MONTHLY versions for: The oldest past version directory with monthly time units (month <i>n</i>, 1st day, 00:00 to <i>last-day</i>, 23:59) is kept for the number of units specified. Specify in the range from 1 to 36.</p> <p>Keep YEARLY versions for: The oldest past version directory with yearly time units (year <i>n</i>, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. Specify in the range from 1 to 100.</p> <p>Period to hold^{#2}</p> <p>Select this item to keep past-version directories in every interval between migrations. Specify the period to keep the past version directories in the range from 1 to 36,500 (in days).</p>
<p>#1: Displayed when the HCP namespace is allocated to the file system.</p> <p>#2: Note that the retention period of past version directories depends on the capacity of the namespace in the migration destination. For information on how to estimate the capacity requirement for a namespace in a migration destination, see the <i>Installation and Configuration Guide</i>.</p>	

Table C-99 Information specified in the Namespace tab in the Create File System dialog box (when On (Read-Only) is selected for Content sharing)

Item	Description
Namespace FQDN[#]	Specify the fully qualified domain name of the HCP namespace that is used for data sharing.
External HCP host name	If the HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the HCP system.
Namespace-access account[#]	Specify the user name and password for the account for accessing the namespace. If you click the Test Connection for Primary button after specifying information, you can check the connection with the HCP system.
Replica[#]	<p>If you are using the HCP replication functionality, select the Use check box.</p> <p>System name</p> <p>Specify the replica HCP system name to Fully Qualified Domain Name.</p> <p>External Replica HCP host name</p> <p>If the replica HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the replica HCP system.</p> <p>After specifying the information, click the Test Connection for Replica button to check whether you can connect to the replica HCP system.</p>
<p>#: Displayed when the HCP namespace is allocated to the file system.</p>	

Table C-100 Information specified in the Namespace tab in the Create File System dialog box (when On (Read/Write) is selected for Content sharing)

Item	Description
Namespace settings	<p>If you did not specify Yes for Create namespace in the Basic tab, specify the name of the namespace for the HCP system to which data will be migrated.</p> <p>After the namespace name is specified, click the Test Connection button to confirm that you can connect to the HCP system.</p>
Use file version restore	<p>Select Yes to make the past version files (past version directories) migrated to the HCP system available to clients. Additionally, select a radio button to set the method of keeping past-version directories in the <code>.history</code> directory.</p> <p>To allow CIFS clients to view to the <code>.history</code> directory, change the settings for the shared directory so that all files and folders are shown.</p> <p>Custom schedule</p> <p>Select this item to keep past-version directories that use custom scheduling. For details about custom scheduling of the file version restore functionality, see the <i>Installation and Configuration Guide</i>.</p> <p>Keep 15-MINUTE versions for: The oldest past version directory with 15-minute time units (hour <i>n</i>, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. Specify any of the following: 15, 30, 45, and 60.</p> <p>Keep HOURLY versions for: The oldest past version directory with hourly time units (hour <i>n</i>, minutes 00 to 59) is kept for the number of units specified. Specify in the range from 1 to 48.</p> <p>Keep DAILY versions for: The oldest past version directory with daily time units (day <i>n</i>, 00:00 to 23:59) is kept for the number of units specified. Specify in the range from 1 to 62.</p> <p>Keep WEEKLY versions for: The oldest past version directory with weekly time units (week <i>n</i>, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. Specify in the range from 1 to 52.</p> <p>Keep MONTHLY versions for: The oldest past version directory with monthly time units (month <i>n</i>, 1st day, 00:00 to <i>last-day</i>, 23:59) is kept for the number of units specified. Specify in the range from 1 to 36.</p> <p>Keep YEARLY versions for: The oldest past version directory with yearly time units (year <i>n</i>, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. Specify in the range from 1 to 100.</p> <p>Period to hold[#]</p> <p>Select this item to keep past-version directories in every interval between migrations. Specify the period to keep the past version directories in the range from 1 to 36,500 (in days).</p>

Item	Description
	<p>#: Note that the retention period of past version directories depends on the capacity of the namespace in the migration destination. For information on how to estimate the capacity requirement for a namespace in a migration destination, see the <i>Installation and Configuration Guide</i>.</p>

Table C-101 Information specified in the Namespace tab in the Create File System dialog box (when Home directory is selected for Content sharing)

Item	Description
<p>Namespace settings</p>	<p>If you did not specify Yes for Create namespace in the Basic tab, specify the name of the namespace for the HCP system to which data will be migrated.</p> <p>After the namespace name is specified, click the Test Connection button to confirm that you can connect to the HCP system.</p>
<p>Use file version restore</p>	<p>Select Yes to make the past version files (past version directories) migrated to the HCP system available to clients. Additionally, select a radio button to set the method of keeping past-version directories in the <code>.history</code> directory.</p> <p>To allow CIFS clients to view to the <code>.history</code> directory, change the settings for the shared directory so that all files and folders are shown.</p> <p>Custom schedule</p> <p>Select this item to keep past-version directories that use custom scheduling. For details about custom scheduling of the file version restore functionality, see the <i>Installation and Configuration Guide</i>.</p> <p>Keep 15-MINUTE versions for: The oldest past version directory with 15-minute time units (hour <i>n</i>, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. Only 60 can be specified.</p> <p>Keep HOURLY versions for: The oldest past version directory with hourly time units (hour <i>n</i>, minutes 00 to 59) is kept for the number of units specified. Specify in the range from 1 to 48.</p> <p>Keep DAILY versions for: The oldest past version directory with daily time units (day <i>n</i>, 00:00 to 23:59) is kept for the number of units specified. Specify in the range from 1 to 62.</p> <p>Keep WEEKLY versions for: The oldest past version directory with weekly time units (week <i>n</i>, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. Specify in the range from 1 to 52.</p> <p>Keep MONTHLY versions for: The oldest past version directory with monthly time units (month <i>n</i>, 1st day, 00:00 to <i>last-day</i>, 23:59) is kept for the number of units specified. Specify in the range from 1 to 36.</p> <p>Keep YEARLY versions for: The oldest past version directory with yearly time units (year <i>n</i>, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. Specify in the range from 1 to 100.</p>

Item	Description
	<p>Period to hold[#]</p> <p>Select this item to keep past-version directories in every interval between migrations. Specify the period to keep the past version directories in the range from 1 to 36,500 (in days).</p>
<p>[#]: Note that the retention period of past version directories depends on the capacity of the namespace in the migration destination. For information on how to estimate the capacity requirement for a namespace in a migration destination, see the <i>Installation and Configuration Guide</i>.</p>	

Advanced tab

You can use the **Advanced** tab to specify the attributes of the file system as necessary.

File System subtab

You can use the **File System** subtab to specify attributes of the file system in which the file share is created as necessary.

Table C-102 Information specified in the File System subtab in the Advanced tab in the Create File System dialog box

Item	Description
Maximum capacity for i-nodes	Specify the maximum percentage of space within the file system that can be used for an inode, as an integer from 1 to 100. The maximum capacity that can be used as an inode is 1 TB.
Record last access time	Select this to update the last access time (<i>atime</i>) when a client accesses a file in the file system.
Enable Advanced ACL type	<p>Select this to create a file system of the Advanced ACL type. An Advanced ACL file system cannot be converted to the Classic ACL type. For a WORM file system, you cannot change the ACL type after creation.</p> <p>If you do not select this check box, the created file system will be the Classic ACL type. If the file system is to be used mainly for NFS shares, use the Classic ACL type.</p>
CIFS bypass traverse checking	<p>Select this to enable CIFS bypass traverse checking.</p> <p>This item is not displayed if in the Basic tab, Home directory is selected for Content sharing.</p>

Striping subtab

You can use the **Striping** subtab to specify the striping settings for the file system.

Table C-103 Information specified in the Striping subtab of the Advanced tab in the Create File System dialog box

Item	Description
Enable striping for the file system	Select Yes when you want to create a file system in a striping configuration. In addition, specify the stripe size for Size in KB.

Health Monitor window

You can use the Health Monitor window to view hardware information.

To open the Health Monitor window, in the *physical-node* window ([physical-node window on page C-91](#)), click **Health Check** on the **Basic** subtab of the **Settings** tab.

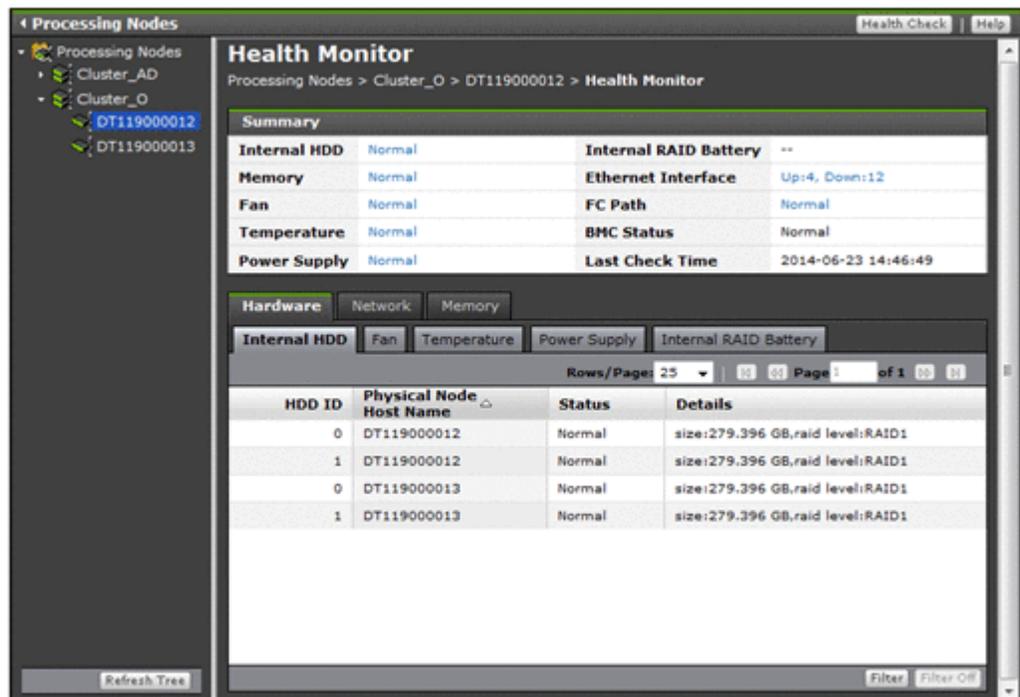


Table C-104 Operations that can be performed from the Health Monitor window

Button	Description
Health Check	Refreshes hardware information. If the cached information in the management server database is inconsistent with the information on a node, the system administrator must refresh the management server database. This also refreshes the hardware information shown in the GUI.

Table C-105 Hardware summary information shown in the Health Monitor window

Item	Description
Internal HDD	<p>The collective status of the internal hard disk drives.</p> <p>Normal</p> <p>All of the internal hard disk drives are working normally.</p> <p>Error</p> <p>An error has occurred in one or more internal hard disk drives.</p> <p>Unknown error</p> <p>The information regarding the internal hard disk drives cannot be obtained.</p>
Memory	<p>The memory status.</p> <p>Normal</p> <p>All of the memory is working normally.</p> <p>Unknown error</p> <p>The memory information cannot be obtained.</p>
Fan	<p>The collective status of the fans.</p> <p>Normal</p> <p>All of the fans are working normally.</p> <p>Error</p> <p>An error has occurred in one or more fans.</p> <p>Unknown error</p> <p>The fan information cannot be obtained.</p>
Temperature	<p>The detected results of the temperature sensors.</p> <p>Normal</p> <p>All of the temperature sensors have detected normal temperatures.</p> <p>Error</p> <p>One or more temperature sensors have detected anomalous temperatures.</p> <p>Unknown error</p> <p>The temperature information cannot be obtained.</p>
Power Supply	<p>The collective status of the power supply units.</p> <p>Normal</p> <p>All of the power supply units are working normally.</p> <p>Error</p> <p>An error has occurred in one or more power supply units.</p> <p>Unknown error</p> <p>The information of the power supply units cannot be obtained.</p>
Internal RAID Battery	<p>The collective status of the internal RAID batteries.</p> <p>Normal</p>

Item	Description
	<p>All of the internal RAID batteries are working normally.</p> <p>Error</p> <p>An error has occurred in one or more internal RAID batteries.</p> <p>Unknown error</p> <p>The information of the internal RAID batteries cannot be obtained.</p>
Ethernet Interface	<p>The collective status of the Ethernet interfaces.</p> <p>Up:<i>n</i>, Down:<i>n</i></p> <p>Shown the number of ports whose link statuses are Up and Down as <i>n</i>.</p> <p>Unknown error</p> <p>The information of the Ethernet interfaces cannot be obtained.</p>
FC Path	<p>The collective status of the FC paths.</p> <p>Normal</p> <p>All of the FC paths are working normally.</p> <p>Error</p> <p>An error has occurred in one or more FC paths.</p> <p>Unknown error</p> <p>The information of the FC paths cannot be obtained.</p>
BMC Status	<p>The BMC status.</p> <p>Normal</p> <p>The BMC is working normally.</p> <p>Error</p> <p>An error has occurred in the BMC.</p> <p>Unknown error</p> <p>The BMC information cannot be obtained.</p>
Last Check Time	<p>The last date and time that the hardware information was obtained.</p>
<p>Note: -- is shown for any items for which the applicable device is not installed or whose information cannot be obtained.</p>	

Table C-106 Information shown in the Health Monitor window

Item	Description	See
Hardware	Information about the hardware in the node.	Hardware tab on page C-140
	Internal HDD Information about the internal hard disk drives.	Internal HDD subtab on page C-140
	Fan Information about the fans.	Fan subtab on page C-141

Item	Description		See
	Temperature	Temperature information.	Temperature subtab on page C-141
	Power Supply	Information about the power supply unit.	Power Supply subtab on page C-142
	Internal RAID Battery	Information about the internal RAID battery.	Internal RAID Battery subtab on page C-142
Network	Information about the network connection of the node.		Network tab on page C-144
	Ethernet Interface	Information about the Ethernet interface.	Ethernet Interface subtab on page C-144
	FC Path	Information about the FC path.	FC Path subtab on page C-145
Memory	Information about the memory installed in the node.		Memory tab on page C-146
	Memory Total	The total size of the memory.	Memory Total subtab on page C-147
	Details	Detailed information about the memory.	Details subtab on page C-147

Hardware tab

You can use the **Hardware** tab to view information about the hardware in the node.

Internal HDD subtab

You can use the **Internal HDD** subtab to view information about the internal hard disk drives.

Table C-107 Internal hard disk drive information shown in the Internal HDD subtab of the Hardware tab in the Health Monitor window

Item	Description
HDD ID	The ID of the internal hard disk drive.
Physical Node Host Name	The name of the physical node in which the internal hard disk drive exists.
Status	The status of the internal hard disk drive. Normal The internal hard disk drive is working normally.

Item	Description
	<p>Error</p> <p>An error has occurred in the internal hard disk drive or the internal hard disk drive is not installed. Check the error messages on the List of RAS Information page (for <i>List of messages</i>) of the Check for Errors dialog box, and then take action accordingly.</p> <p>Rebuild</p> <p>The RAID is being reconfigured.</p> <p>Not supported</p> <p>No programs for acquiring information are installed.</p>
Details	Shows detailed, vendor-specific information for the internal hard disk drive.

Fan subtab

You can use the **Fan** subtab to view information about the fans.

Table C-108 Fan information shown in the Fan subtab of the Hardware tab in the Health Monitor window

Item	Description
Fan ID	The ID of the fan.
Physical Node Host Name	The name of the physical node in which the fan exists.
Status	<p>The fan status.</p> <p>Normal</p> <p>The fan is working normally.</p> <p>Error</p> <p>An error has occurred in the fan or the fan is not installed. Check the error messages on the List of RAS Information page (for <i>List of messages</i>) of the Check for Errors dialog box, and then take action accordingly.</p>
Details	Shows detailed, vendor-specific information for the fan.

Temperature subtab

You can use the **Temperature** subtab to view information about the temperature.

Table C-109 Temperature information shown in the Temperature subtab of the Hardware tab in the Health Monitor window

Item	Description
Sensor ID	The ID of the temperature sensor.

Item	Description
Physical Node Host Name	The name of the physical node in which the temperature sensor exists.
Status	<p>The detection result of the temperature sensor.</p> <p>Normal</p> <p>The temperature sensor has detected normal temperature.</p> <p>Error</p> <p>The temperature sensor has detected anomalous temperature. Check the error messages on the List of RAS Information page (for <i>List of messages</i>) of the Check for Errors dialog box, and then take action accordingly.</p>
Details	Shows detailed, vendor-specific information for the temperature sensor.

Power Supply subtab

You can use the **Power Supply** subtab to view information about the power supply unit.

Table C-110 Power supply unit information shown in the Power Supply subtab of the Hardware tab in the Health Monitor window

Item	Description
Power Supply ID	The ID of the power supply unit.
Physical Node Host Name	The name of the physical node in which the power supply unit exists.
Status	<p>The status of the power supply unit.</p> <p>Normal</p> <p>The power supply unit is working normally.</p> <p>Error</p> <p>An error has occurred in the power supply unit. Check the error messages on the List of RAS Information page (for <i>List of messages</i>) of the Check for Errors dialog box, and then take action accordingly.</p> <p>Not installed</p> <p>The power supply unit is not installed.</p>
Details	Shows detailed, vendor-specific information for the power supply unit.

Internal RAID Battery subtab

You can use the **Internal RAID Battery** subtab to view information about the internal RAID battery.

Table C-111 Internal RAID battery information shown in the Internal RAID Battery subtab of the Hardware tab in the Health Monitor window

Item	Description
Battery ID	The ID of the internal RAID battery.
Physical Node Host Name	The name of the physical node in which the internal RAID battery exists.
Status	<p>The status of the internal RAID battery.</p> <p>Normal The internal RAID battery is working normally.</p> <p>Error An error has occurred in the internal RAID battery. Check the error messages on the List of RAS Information page (for <i>List of messages</i>) of the Check for Errors dialog box, and then take action accordingly.</p> <p>Charging The internal RAID battery is being charged.</p> <p>Not supported No programs for acquiring information are installed.</p>
Details	Shows detailed, vendor-specific information for the internal RAID battery.

BMC Status subtab

You can use the **BMC Status** subtab to view information about the BMC.

Table C-112 BMC information shown in the BMC Status subtab of the Hardware tab in the Health Monitor window

Item	Description
Physical Node Host Name	The name of the physical node in which the BMC.
BMC Status of Own Node	<p>The status of the BMC.</p> <p>Normal The BMC is working normally.</p> <p>Error An error has occurred in the BMC. Check the error messages on the List of RAS Information page (for <i>List of messages</i>) of the Check for Errors dialog box, and then take action accordingly.</p> <p>Unknown error The BMC information cannot be obtained. Check the error messages on the List of RAS Information page (for <i>List of messages</i>) of the Check for Errors dialog box, and then take action accordingly.</p>

Item	Description
Connection with BMC of Other Node	<p>Status of the connection with the BMC on the other node.</p> <p>Normal</p> <p>The connection with the BMC on the other node is normal.</p> <p>Error</p> <p>The communication with the BMC on the other node has failed. Check the error messages on the List of RAS Information page (for <i>List of messages</i>) of the Check for Errors dialog box, and then take action accordingly.</p> <p>Unknown error</p> <p>The BMC information cannot be obtained. Check the error messages on the List of RAS Information page (for <i>List of messages</i>) of the Check for Errors dialog box, and then take action accordingly.</p> <p>-- is shown if the cluster is not configured.</p>

Network tab

You can use the **Network** tab to view information about the network connection of the node.

Ethernet Interface subtab

You can use the **Ethernet Interface** subtab to view information about the Ethernet interface.

Table C-113 Ethernet interface information shown in the Ethernet Interface subtab of the Network tab in the Health Monitor window

Item	Description
Port Name	The port name of the Ethernet interface.
Physical Node Host Name	The name of the physical node on which the Ethernet interface exists.
Type	<p>The port type.</p> <p>Data port</p> <p>The port is a data port.</p> <p>Heartbeat port</p> <p>The port is a heartbeat port.</p> <p>Management port</p> <p>The port is a management port.</p> <p>Private maintenance port</p> <p>The port is a private maintenance port.</p>
Link Status	<p>The link status.</p> <p>Up</p> <p>The link is connected normally.</p>

Item	Description
	Down The link is disconnected. Check the negotiation mode of the switch connected to the port, and then set the negotiation mode again.
Media Type	The media type. Copper Metal cables are supported. Fiber Optical cables are supported.
Link Speed	The current communication speed. Note that 10Base is not a recommended communication speed. Check and, if necessary, correct the setting of the connected switch so that the communication speed is 100Base or greater. <code>Unknown</code> is shown when the communication speed information cannot be obtained.

FC Path subtab

You can use the **FC Path** subtab to view information about the FC path.

Table C-114 FC path information shown in the FC Path subtab of the Network tab in the Health Monitor window

Item	Description
Path	The FC path name. -- is shown if the information cannot be obtained.
Physical Node Host Name	The name of the physical node that the FC path belongs to.
Status	The FC path status. Online The FC path is working normally. Online (LU error) The FC path is in the <code>Online</code> status, and an error has been detected in an LU. Offline The FC path has been placed offline by an operation from a system administrator. Offline (LU error) The FC path is in the <code>Offline</code> status, and an error has been detected in an LU. Partially online The FC path is working normally, but some LUs are inaccessible. For example, this is shown in the following cases: - When the FC path is placed offline and an LU is added manually - When the FC path is placed offline and an LU is added by automatically creating the LU

Item	Description
	<p>Partially online (LU error)</p> <p>The FC path is in the <code>Partially online</code> status, and an error has been detected in an LU.</p> <p>Error</p> <p>Shown when all LUs belonging to the target FC path are inaccessible.</p> <p>For example, this is shown in the following cases:</p> <ul style="list-style-type: none"> - When an error has occurred on the FC path - When the FC cable is disconnected - When an error has occurred on the HBA card - When no LU is assigned to a host group associated with the FC path <p>Configuration mismatch</p> <p>The assignment of LUs to the host groups associated with one FC path differs from the assignment for the alternate FC path, or when an alternate FC path does not exist.</p> <p>Unknown</p> <p>The FC path status cannot be confirmed.</p> <p>For example, this is shown in the following cases:</p> <ul style="list-style-type: none"> - When the FC port (host port) on the node side cannot be identified - When the FC port (storage port) on the storage system side cannot be identified
Target	<p>The target.</p> <p>-- is shown if the information cannot be obtained.</p>
Model	<p>The model of the storage system.</p>
Serial Number	<p>The serial number of the storage system.</p>
Host Port	<p>The name of the FC port (host port) on the node side.</p> <p>-- is shown if the information cannot be obtained.</p>
Host Port WWN	<p>The WWN of the FC port on the node side.</p> <p>-- is shown if the FC port cannot be identified.</p>
Storage Port	<p>The name of the FC port on the storage system side.</p>
Storage Port WWN	<p>The WWN of the FC port on the storage system side.</p> <p>-- is shown if an error has occurred on the FC path.</p>
<p>Note: Until a cluster configuration is defined, the FC path information is not shown and <code>No object</code> is shown.</p>	

Memory tab

You can use the **Memory** tab to view information about the memory installed in the node.

Memory Total subtab

You can use the **Memory Total** subtab to view the total size of the memory.

Table C-115 Memory information shown in the Memory Total subtab of the Memory tab in the Health Monitor window

Item	Description
Physical Node Host Name	The name of the physical node in which the memory exists.
Size	The memory size is shown in the following format: <i>size:memory-capacity-recognized-by-system (installed-memory-capacity)</i>

Details subtab

You can use the **Details** subtab to view detailed information about the memory.

Table C-116 Memory information shown in the Details subtab of the Memory tab in the Health Monitor window

Item	Description
Memory ID	The ID of the memory.
Physical Node Host Name	The name of the physical node in which the memory exists.
Status	The memory status. Normal The memory is working normally. Not installed The memory is not installed.
Details	Shows detailed, vendor-specific information for the memory.

System Software window

You can view software information in the System Software window.

To open the System Software window, click **Software Update** on the **Basic** subtab of the **Settings** tab in the *physical-node* window ([physical-node window on page C-91](#)).

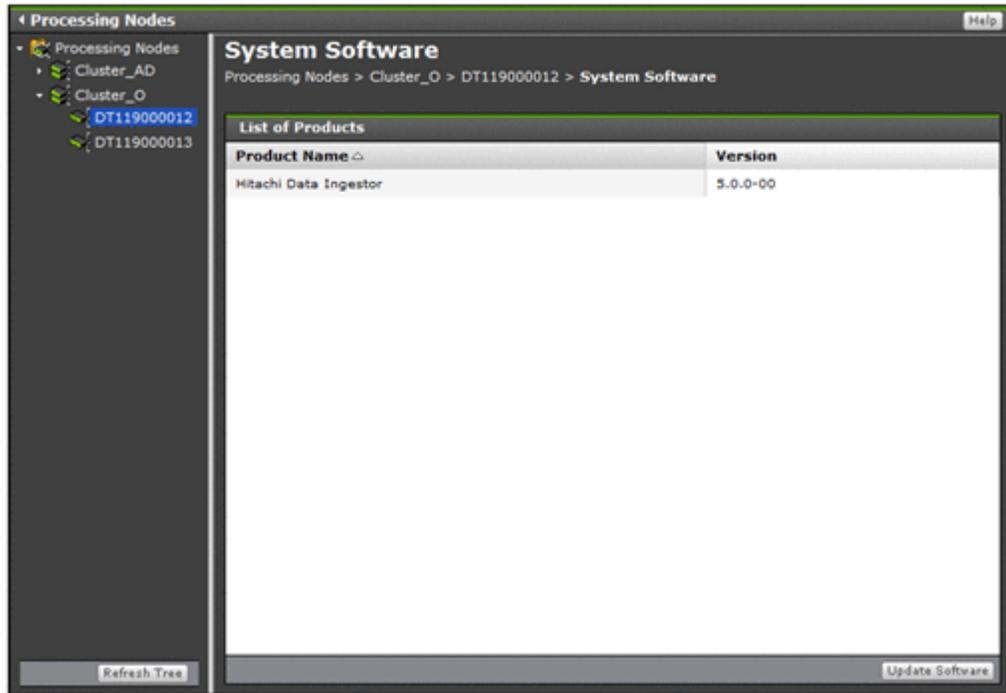


Table C-117 Software information shown in the System Software window

Item	Description
Product Name	Name of an installed product.
Version	Version of the installed product.

Table C-118 Operations that can be performed from the System Software window

Button	Description	See
Update Software	If you are using the management console from the management LAN, you can install an upgrade of the software running on the node.	System Software Installation Wizard on page C-148

System Software Installation Wizard

You can install software upgrades on nodes from the management console of the management LAN. Install the software of the same versions on the both nodes in the cluster.

For details about how to install a Hitachi File Services Manager on the management server, see the *Installation and Configuration Guide*.

The software can be installed when the following conditions are satisfied.

When installing the software on both nodes:

- The status of both nodes is `UP` or `INACTIVE`.

- The status of the resource groups on both nodes or the status of is Online or Offline.

When installing the software on either node:

- The status of both nodes is UP, or the status of the node on which the software will be installed is INACTIVE.
- The status of the resource groups on both nodes or the status of is Online or Offline.



Note: You need free space of 2 GB or more in the area where Hitachi File Services Manager for the management server is to be installed.

To open the System Software Installation Wizard, click **Update Software** in the System Software window ([System Software window on page C-147](#)).

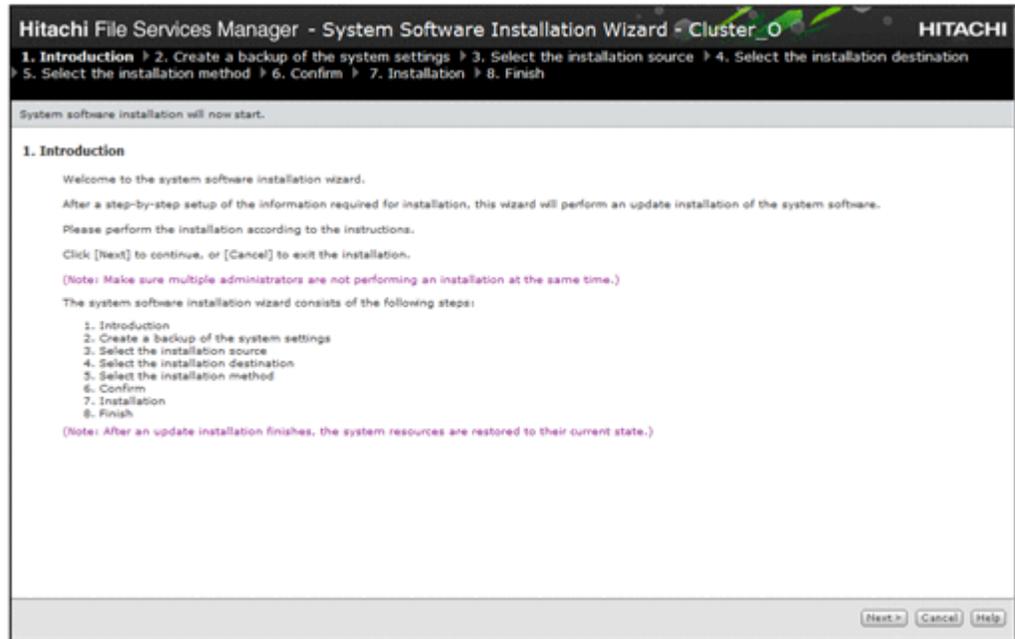


Table C-119 Pages shown for the System Software Installation Wizard

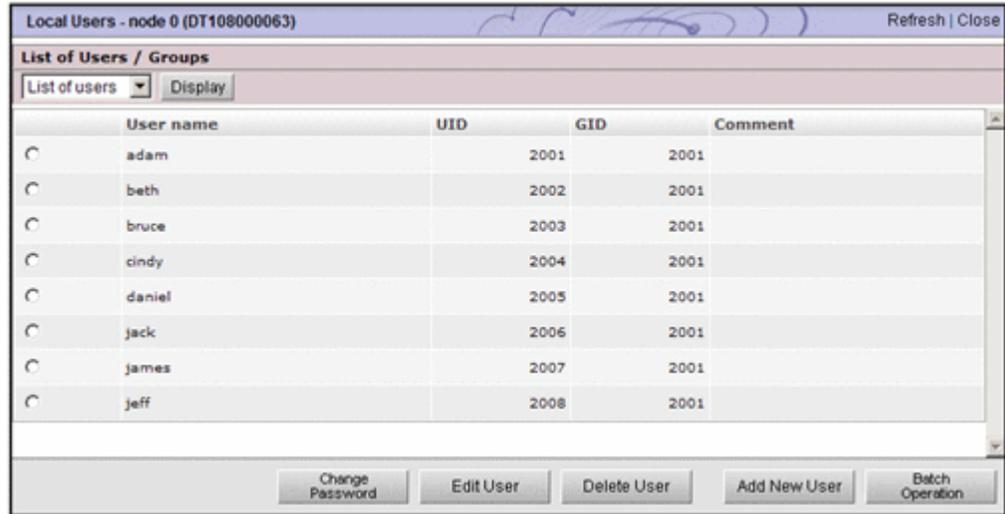
Page	Description
1. Introduction	Check the information shown, and then click Next > .
2. Create a backup of the system settings	Click Backup Configuration to show the Backup Configuration dialog box. From this dialog box, use the Save System Settings Menu page to save system settings. After saving the system settings, select the appropriate check box and then click Next > . For details about how to use the Backup Configuration dialog box, see Backup Configuration dialog box on page C-171 .
3. Select the installation source	Specify the file to be installed, and then click Next > . To use an installation file on the management console:

Page	Description
	<p>Select the Install from a local file option, and then specify <code>install_files.tar.gz</code> in the installation medium. Click Browse to browse files and then select the file name.</p> <p>Clicking Next > starts file transfer to the node. When the file has been transferred, go to the next step.</p> <p>To use an installation file that has been transferred to a node:</p> <p>Check the product information that is shown, and then select the Install from the transferred file option.</p>
<p>4. Select the installation destination</p>	<p>Select the installation destination physical node, and then click Next >.</p> <p>To install the software on both physical nodes:</p> <p>Select the Both physical nodes option.</p> <p>To install the software on either physical node:</p> <p>Select the Only on <i>target-physical-node-name</i> option.</p> <p>Make sure that the same version of software products is used on all nodes in the cluster.</p>
<p>5. Select the installation method</p>	<p>Specify the installation method, and then click Next >.</p> <p>To perform all installation steps automatically, select the Automatically perform all installation steps check box.</p>
<p>6. Confirm</p>	<p>After checking the information that is shown, select the appropriate check box, and then click Confirm.</p>
<p>7. Installation</p>	<p>To perform the installation steps manually:</p> <p>Upon completion of each step, click Start Next Step to start the next step.</p> <p>To switch to the automatic installation mode when a step has been completed, select the Automatically perform the remaining installation steps check box and then click Start Next Step.</p> <p>To switch installation mode from automatic:</p> <p>Click Change Installation Method to switch to manual installation mode.</p>
<p>8. Finish</p>	<p>Check the processing result and then click Close.</p>

Local Users dialog box

In the **Local Users** dialog box, you can manage information about users who can access file systems.

To open the **Local Users** dialog box, click **Local Users** on the **Basic** subtab of the **Settings** tab in the *physical-node* window ([physical-node window on page C-91](#)). After the **Local Users** dialog box is shown, the **List of Users / Groups** page appears.



List of Users / Groups page

You can view information about the users registered on the HDI system, and the groups to which users belong.

After the **Local Users** dialog box is shown, the **List of Users / Groups** page appears.

Select the information to be shown with the drop-down list, and click **Display**.

Table C-120 Targets that can be selected from the drop-down list on the List of Users / Groups page

Item	Description	See
List of users	The user information is shown.	List of Users / Groups page (for List of users) on page C-151
List of groups	The information about the group to which the user belongs to is shown.	List of Users / Groups page (for List of groups) on page C-152

List of Users / Groups page (for List of users)

In the **List of Users / Groups** page (for List of users), you can view the user information.

To open the **List of Users / Groups** page (for List of users), select **List of users** in the drop-down list of the **List of Users / Groups** page in the **Local Users** dialog box ([Local Users dialog box on page C-150](#)), and then click **Display**.

Table C-121 Information shown in the List of Users / Groups page (for List of users)

Item	Description
User name	User name
UID	User ID
GID	ID of the primary group to which the user belongs
Comment	Comment for the user Nothing is shown unless a comment has been set.

Table C-122 Operations that can be performed from the List of Users / Groups page (for List of users)

Button	Description	See
Change Password	Change the password of the user selected.	Change Password page on page C-153
Edit User	Edit information for the user selected.	Edit User page on page C-153
Delete User	Delete information for the user selected. Information for users registered in a batch operation can also be deleted.	N/A
Add New User	Add a user.	Add User page on page C-154
Batch Operation	Here you can register or delete information for multiple users.	Batch Operation page on page C-156
Note: N/A = Not applicable.		

List of Users / Groups page (for List of groups)

In the **List of Users / Groups** page (for List of groups), you can view the group information.

To open the **List of Users / Groups** page (for List of groups), select **List of groups** in the drop-down list of the **List of Users / Groups** page in the **Local Users** dialog box ([Local Users dialog box on page C-150](#)), and then click **Display**.

Table C-123 Group information shown in the List of Users / Groups page (for List of groups)

Item	Description
Group name	Group name
GID	Group ID

Table C-124 Operations that can be performed from the List of Users / Groups page (for List of groups)

Button	Description	See
Edit Group	Edit information for the group selected.	Edit Group page on page C-162
Delete Group	Delete information for the group selected.	N/A
Add New Group	Add a group.	Add Group page on page C-162
Note: N/A = Not applicable.		

Change Password page

You can use the **Change Password** page to change the password of the user selected.

To open the **Change Password** page, select **List of users** from the drop-down list on the **List of Users / Groups** page ([List of Users / Groups page on page C-151](#)), and then click **Display**. Select the target user, and then click **Change Password**.

Table C-125 Information specified in the Change Password page

Item	Description
New password	Enter the new password.
Re-enter new password	Re-enter the password you set in New password .

Edit User page

You can use the **Edit User** page to edit information for the user selected.

To open the **Edit User** page, select **List of users** from the drop-down list on the **List of Users / Groups** page ([List of Users / Groups page on page C-151](#)), and then click **Display**. Select the target user, and then click **Edit User**.

Table C-126 Information specified in the Edit User page

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	Using the List of selectable groups list box, select the groups to which the user belongs.

Item	Description
	<p>Up to 32 groups can be specified per user.</p> <p>However, if a user belongs to more than 16 groups and is using UNIX (AUTH_SYS) authentication for when they access NFS file shares, they will only be granted access permission for the first 16 groups.</p> <p>When you click ▼, 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.</p> <p>To delete a group from the Selected groups list box, select the group and click ▲.</p>
<p>Note: Items, whose information is not changed, retain their current settings.</p>	

Add User page

You can use the **Add User** page to add a user.



Note:

- The groups that include the users to be added must be registered beforehand.
- Make sure that there are no more than 2,000 users per cluster.

To open the **Add User** page, select **List of users** from the drop-down list on the **List of Users / Groups** page ([List of Users / Groups page on page C-151](#)), click **Display**, and then click **Add New User**.

Table C-127 Information specified in the Add User page

Item	Description
User name	<p>Enter the user name. You cannot specify a user name that has already been registered on the HDI system, the NIS server, or the LDAP server for user authentication. To add the user as a user of CIFS shares, you cannot specify a name that is the same as that of an existing group configured to use the ACL functionality.</p> <p>Enter a maximum of 16 characters. The first character must be an alphanumeric character. You can use any alphanumeric character, hyphen (-), and underscore (_) after the first character.</p> <p>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.</p> <p>Also, you cannot specify a user name already reserved in the OS. For details about reserved words, see List of reserved words on page F-2.</p>
UID	<p>Enter the user ID from 200 to 2147483147.</p> <p>You cannot specify 65534 or any other value that has already been registered on the HDI system, the NIS server, or the LDAP server for user authentication. In addition, when user mapping is</p>

Item	Description
	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	<p>Enter the user password, using from 6 to 20 characters.</p> <p>You can use any alphanumeric character, exclamation mark (!), double quotation mark ("), hash mark (#), dollar sign (\$), percent sign (%), ampersand (&), single quotation mark ('), 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 square bracket ([), backslash (\), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (), right curly bracket (}), and tilde (~).</p>
Re-enter password	Re-enter the password you set in Password .
Comment	<p>Enter a comment for the user, using no more than 32 characters.</p> <p>You can use any alphanumeric character, hash mark (#), percent sign(%), ampersand(&), single quotation mark('), left parenthesis((), right parenthesis()), asterisk(*), plus sign(+), hyphen(-), period(.), forward slash(/), semicolon(;), left angle bracket(<), right angle bracket(>), question mark(?), at mark(@), left square bracket([), right square bracket(]), caret(^), underscore(_), left curly bracket({), vertical bar(), right curly bracket(}), and tilde(~). You can also specify spaces, but not at the beginning or end of the character string.</p> <p>This item is optional.</p> <p>When the user uses CIFS shares, this comment is used for showing ACLs.</p>
Apply to CIFS environment	Select this check box when you want to add the user as a user of CIFS shares.
Groups	<p>Using the List of selectable groups list box, specify the groups to which the user belongs.</p> <p>Up to 32 groups can be specified per user.</p> <p>However, if a user belongs to more than 16 groups and is using UNIX (AUTH_SYS) authentication for when they access NFS file shares, they will only be granted access permission for the first 16 groups.</p> <p>When you click ▼, 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.</p> <p>To delete a group from the Selected groups list box, select the group and click ▲.</p>

Batch Operation page

Use a CSV file containing user information to register or delete information about multiple users in a batch operation.



Note:

- Prepare the CSV file containing user information in advance. For details about the CSV file format, see [CSV file format on page C-156](#).
- 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.
- Depending on the number of users whose information is to be registered or deleted, it might take 20 to 50 minutes to finish the operation.

To open the **Batch Operation** page, select **List of users** from the drop-down list on the **List of Users / Groups** page ([List of Users / Groups page on page C-151](#)), click **Display**, and then click **Batch Operation**.

Table C-128 Information specified on the Batch Operation page

Item	Description
Name of batch configuration file	Specify the path to the CSV file containing user information.

Table C-129 Operations that can be performed for the CSV file specified on the Batch Operation page

Button	Description
Check and Register	Check the CSV file format, and then register or delete user information in a batch operation. If there is no error in the CSV file, user information is registered or deleted in a batch operation. If an error is found, none of the user information is registered or deleted.
Check File	Only check the CSV file format.

When the check is completed, you can download the result file containing the check results. Check the result file and, if an error is found, take corrective action.

For details about the error description and corrective actions, see [Table C-131 Error messages, error causes, and actions when an error occurs during batch registration of user information on page C-159](#) or [Table C-132 Error messages, error causes, and actions when an error occurs during batch deletion of user information on page C-161](#).

CSV file format

You can use any alphanumeric character, hyphen (-), underscore (_), and period (.) in the file name. Also make sure that the path name of a CSV file

specified on the **Batch Operation** page does not contain more than 512 characters.

Table C-130 Information specified in a CSV file for batch registration or batch deletion of user information

Item	When registering	When deleting	Description
Execution category	R	R	Specify the execution category of the data. Write as <code>Data</code> . Specify a hash mark (#) for a comment line.
Data classification	R	R	The processing classification of the data. <code>UA01</code> Batch-register the data. <code>UD01</code> Batch-delete the data. Note that <code>UA01</code> and <code>UD01</code> cannot exist within the same file.
Data registration destination	R	N/R	Specify the destination where the user information is to be registered. 1 Register in the HDI system. 3 Register the users in the HDI system as users who access CIFS shares.
User name	R	R	Specify the user name. The values that can be specified are the same as those that can be specified in User name , in the Add User page. For more details about specifiable values, see Add User page on page C-154 .
UID	R	N/R	Specify the user ID. The values that can be specified are the same as those that can be specified in UID , in the Add User page. For more details about specifiable values, see Add User page on page C-154 .
GID	R	N/R	Specify the ID of the primary group to which the user belongs.
Password	R	N/R	Specify the user password. The values that can be specified are the same as those that can be specified in Password , in the Add

Item	When registering	When deleting	Description
			User page. For more details about specifiable values, see Add User page on page C-154 .
Comment	I	N/R	Specify a comment for the user. The values that can be specified are the same as those that can be specified in Comment , in the Add User page. For more details about specifiable values, see Add User page on page C-154 .
Groups	I	N/R	Use a group name or group ID to specify the other groups to which the user belongs. Use commas to delimit multiple group names or group IDs, and enclose the entire string with double quotation marks (").
Note: R = Required. I = If necessary. N/R = Not required.			

Example of batch registration

```
#execution-category,data-classification,data-registration-destination,user-
name,UID,GID,password,comment,groups
Data,UA01,3,username,205,205,password,fullname,"206,207,208"
```

Example of batch deletion

```
#execution-category,data-classification,,user-name
Data,UD01,,username
```

Execution result file format

Example when CSV file check is only performed and no error is found

OK is output to the execution category of the user.

```
#execution-category,data-classification,data-registration-destination,user-
name,UID,GID,password,comment,groups
OK,UA01,3,user04,1004,1000,password,Leader,"unit01,2000"
```

Example when batch registration or deletion is performed normally

#Completed is output to the execution category of the user.

```
#execution-category,data-classification,data-registration-destination,user-
name,UID,GID,password,comment,groups
#Completed,UA01,3,user04,1004,1000,password,Leader,"unit01,2000"
```

Example when the CSV file contains an error

NG (*error-message*) is output to the execution category for the user.

```
#execution-category,data-classification,data-registration-destination,user-
name,UID,GID,password,comment,groups
NG(The specified UID is already
registered),UA01,3,user04,1004,1000,password,Leader,"unit01,2000"
```

Table C-131 Error messages, error causes, and actions when an error occurs during batch registration of user information

Error message	Error cause	Action
The group to which the user belongs is incorrect	The group name or group ID specified in the Groups could not be found.	Check the Groups.
The comment is invalid	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 invalid	The value specified in the process category is incorrect.	Check the value specified in the process category. Specify UA01 in the process category.
The value for the data registration destination is invalid	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 invalid	The value specified in the execution category is incorrect.	Check the value specified in the execution category. Specify Data or hash mark (#) in the execution category.
The GID value is invalid	The group ID value is incorrect or a group with the specified group ID cannot be found. The value might contain a character that cannot be used or specified value is outside the valid range.	Check the group ID. The valid range of the value is from 200 to 2147483147. However, you cannot use 65534.
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.
An invalid character is specified in the password	The specified password is incorrect. The password might contain a character that	Check the password. The length of the password is from 6 to 20 characters.

Error message	Error cause	Action
	cannot be used or the value length might be incorrect.	
The UID is duplicated in the CSV file	The same user ID exists in the CSV file.	Check the user ID.
The user name is duplicated in the CSV file	The same user name exists in the CSV file.	Check the user name.
The specified UID is already registered	The specified user ID has already been registered.	Check the user ID.
The specified user is already registered	The specified user name has already been registered.	Check the user name.
The UID value is invalid	The user ID value is incorrect. The value might contain a character that cannot be used or specified value is outside the valid range.	Check the user ID. The valid range of the value is from 200 to 2147483147. However, you cannot use 65534.
The user name value is invalid	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 a locked resource failed	An internal error occurred. <ul style="list-style-type: none"> You could not obtain an exclusive resource (a timeout occurred). 	Rerun the batch registration of the user information. If the error occurs repeatedly, download all the File Services Manager log files and then contact maintenance personnel. For details about how to download log files, see List of RAS Information page on page C-164 .
Registration failed	An internal error occurred. <ul style="list-style-type: none"> You could not obtain an exclusive resource (a timeout does not cause the error). The group ID of the group to which the user belongs could not be converted into the group name (file operations might fail or 	Rerun the batch registration of the user information. If the error occurs repeatedly, download all the File Services Manager log files and then contact maintenance personnel. For details about how to download log files, see List of RAS Information page on page C-164 .

Error message	Error cause	Action
	<p>group information might not exist).</p> <ul style="list-style-type: none"> The user registration command failed. 	

Table C-132 Error messages, error causes, and actions when an error occurs during batch deletion of user information

Error message	Error cause	Action
The data classification value is invalid	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 invalid	The value specified in the execution category is incorrect.	Check the value specified in the execution category. Specify Data or hash mark (#) 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. For batch deletion of user information, assume four elements as shown below: #execution-category,data-classification,,user-name Data,UD01,,username
The user name is duplicated in the CSV file	The same user name exists in the CSV file.	Check the user name.
The specified user does not exist	The specified user name has not been registered.	Check the user name.
The user name value is invalid	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.
An attempt to acquire a locked resource failed	<p>An internal error occurred.</p> <ul style="list-style-type: none"> You could not obtain an exclusive resource (a timeout occurred). 	Rerun the batch deletion of user information. If the error occurs repeatedly, download all the File Services Manager log files and then contact maintenance personnel. For details about how to download log files, see List of RAS Information page on page C-164 .
Deletion failed	<p>An internal error occurred.</p> <ul style="list-style-type: none"> The user deletion command failed. You could not obtain an exclusive resource (a 	Rerun the batch deletion of user information. If the error occurs repeatedly, download all the File Services Manager log files and then contact maintenance personnel. For

Error message	Error cause	Action
	timeout does not cause the error).	details about how to download log files, see List of RAS Information page on page C-164 .

Edit Group page

You can use the **Edit Group** page to edit information for the group selected.

To open the **Edit Group** page, select **List of groups** from the drop-down list on the **List of Users / Groups** page ([List of Users / Groups page on page C-151](#)), click **Display**, select the target group, and then click **Edit Group**.

Table C-133 Information specified in the Edit Group page

Item	Description
Group name	Enter the group name. Note, however, that the group name cannot be changed when Applied 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. When you click ▼, 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. To delete a group member listed in the Selected users list box, select the user and click ▲.
Note: Items, whose information is not changed, retain their current settings.	

Add Group page

You can use the **Add Group** page to add a group.



Note: Make sure that there are no more than 2,000 groups per cluster.

To open the **Add Group** page, select **List of groups** from the drop-down list on the **List of Users / Groups** page ([List of Users / Groups page on page C-151](#)), click **Display**, select the target group, and then click **Add New Group**.

Table C-134 Information specified in the Add Group page

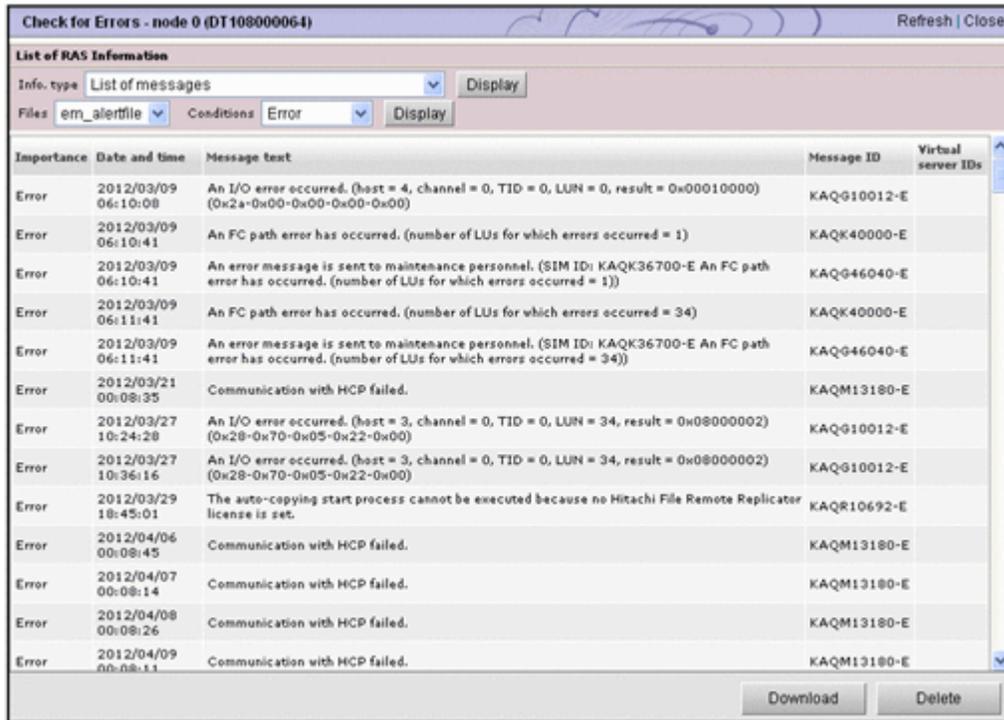
Item	Description
Group name	Enter the group name. You cannot enter any group name that has already been registered on the HDI system, the NIS server, or the LDAP server for user authentication.

Item	Description
	<p>Enter a maximum of 16 characters. The first character must be an alphanumeric character. You can use any alphanumeric character, hyphen (-), and underscore (_) after the first character.</p> <p>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.</p> <p>If ACL functionality is to be used for the group being added, you cannot specify a name that is the same as that of any user configured to access CIFS shares.</p> <p>Also, you cannot specify a group name already reserved in the OS. For details about reserved words, see List of reserved words on page F-2.</p>
GID	<p>Enter the group ID from 200 to 2147483147.</p> <p>You cannot specify 65534 or any other value that has already been registered on the HDI system, 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.</p>
Apply to CIFS ACL environment	<p>Select this check box when setting an ACL for the adding group.</p>
Users in group	<p>In the List of selectable users list box, specify the users who belong to this group.</p> <p>When you click ▼, 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.</p> <p>To delete a group member listed in the Selected users list box, select the user and then click ▲.</p>

Check for Errors dialog box

You can check the error information for the nodes in the **Check for Errors** dialog box.

To open the **Check for Errors** dialog box, in the *physical-node* window ([physical-node window on page C-91](#)), click **Check for Errors** on the **Basic** subtab of the **Settings** tab. After the **Check for Errors** dialog box is shown, the **List of RAS Information** page appears.



List of RAS Information page

You can select and show the desired error information from the **Info. type** drop-down list in the **List of RAS Information** page.

The **List of RAS Information** page first appears after the **Check for Errors** dialog box is shown.

Table C-135 Error information selected from the Info. type drop-down list on the List of RAS Information page

Item	Description	See
List of messages	The system messages, which are important messages related to errors that occurred in the hardware or software.	List of RAS Information page (for List of messages) on page C-165
List of system logs	The system logs.	List of RAS Information page (for List of system logs) on page C-167
List of other log files	The log files other than system messages and system logs.	List of RAS Information page (for List of other log files) on page C-167
Batch-download	The log groups for batch downloading or batch deletion of log files.	List of RAS Information page (for Batch-download) on page C-168
List of core files	The core files and dump files.	List of RAS Information page (for List of core files) on page C-169

Item	Description	See
Server check	The connection between nodes and external servers.	List of RAS Information page (for Server check) on page C-170
Transfer all logs including the virtual server logs	Transfers all the log files of the node to an FTP server in a batch operation.	List of RAS Information page (for Transfer all logs including the virtual server logs) on page C-170

List of RAS Information page (for List of messages)

You can use the **List of RAS Information** page (for `List of messages`) to view the system messages, which are important messages related to errors that occurred in the hardware or software.

To open the **List of RAS Information** page (for `List of messages`), in the **Check for Errors** dialog box ([Check for Errors dialog box on page C-163](#)), select **List of Messages** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.

To view previous system messages, select a specific past file from the **Files** drop-down list, and then click **Display**. To narrow down the messages shown by severity level, select the severity level from the **Conditions** drop-down list, and then click **Display**.

Table C-136 Past system messages that can be selected from the Files drop-down list on the List of RAS Information page (for List of messages)

File name	Description
em_alertfile	Select this item to show the most recent system message file. This item is selected by default.
em_alertfile.n	Select this item to show a file of past system messages. You can select the saved system message files such as em_alertfile.1 and em_alertfile.2 , where <i>n</i> indicates the generation number. The higher the number, the older the system message file.

Table C-137 Message severity levels that can be selected from the Conditions drop-down list on the List of RAS Information page (for List of messages)

Severity level	Description
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.

Severity level	Description
Fatal error	Select to view fatal error messages only.

Table C-138 Information shown on the List of RAS Information page (for List of messages)

Item	Description
Importance	<p>Message severity level</p> <p>Information The information message.</p> <p>Warning The warning message.</p> <p>Error The error message.</p> <p>Fatal error The fatal error message.</p>
Date and time	Date and time at which the message was output
Message text	Message text
Message ID	<p>Message ID</p> <p>The message ID takes the following format:</p> <p>$KAX^1X^2Y^1Y^2Y^3Y^4Y^5-Z$</p> <p>The variable portions indicate the source, type, and severity level of the message.</p> <p>X^1X^2</p> <p>Symbol representing the program that produced the message. The following shows the symbols that might be shown and what they represent:</p> <p>QB: Backup Restore QG: File Sharing QK: Data Control QM: File Services Manager QV: Anti-Virus Enabler</p> <p>$Y^1Y^2Y^3Y^4Y^5$</p> <p>Number representing the message type</p> <p>Z</p> <p>Symbol representing the message severity level. The following shows the symbols that might be shown and what they represent:</p> <p>E: Error message I: Information message W: Warning message Q: Question message</p>

Table C-139 Operations that can be performed for system messages on the List of RAS Information page (for List of messages)

Button	Description
Download	Download the system messages of the generation shown.
Delete	Delete the system messages of the generation shown.

List of RAS Information page (for List of system logs)

You can use the **List of RAS Information** page (for List of system logs) to view the system logs.

To open the **List of RAS Information** page (for List of system logs), in the **Check for Errors** dialog box ([Check for Errors dialog box on page C-163](#)), select **List of system logs** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.

To view previous system log files, select a specific past file from the **Displayed files** drop-down list, and then click **Display**.

Table C-140 Files that can be selected from the Displayed files drop-down list on the List of RAS Information page (for List of system logs)

File name	Description
syslog	Select this item to show the most recent system logs file. This item is selected by default.
syslog.n	Select this item to show a file of past system logs. You can select the saved system log files, such as syslog.1 and syslog.2 , where <i>n</i> indicates the generation number. The higher the number, the older the system log file.

Table C-141 Operations that can be performed for system log files on the List of RAS Information page (for List of system logs)

Button	Description
Download	Download the system log files that are currently shown.
Delete	Delete the system log files that are currently shown.

List of RAS Information page (for List of other log files)

You can use the **List of RAS Information** page (for List of other log files) to view log files other than system messages and system logs.

To open the **List of RAS Information** page (for List of other log files), in the **Check for Errors** dialog box ([Check for Errors dialog box on page C-163](#)), select **List of other log files** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.

When you select the type of log file from the **File type** drop-down list and then click **Display**, the latest information for the selected log file is shown. To view previous log files, select a specific past file from the **Displayed files** drop-down list, and then click **Display**. For previous log files, generation numbers are appended at the end of the file names or in front of the extensions. Older log files have larger numbers.

Table C-142 Operations that can be performed for log files on the List of RAS Information page (for List of other log files)

Button	Description
Download	Download the log files of the generation that is shown.
Delete	Delete the log files of the generation that is shown. Note that Delete is not shown for some log files, and you cannot delete these log files.

List of RAS Information page (for Batch-download)

You can use the **List of RAS Information** page (for Batch-download) to view log groups for batch downloading or batch deletion of log files.

To open the **List of RAS Information** page (for Batch-download), in the **Check for Errors** dialog box ([Check for Errors dialog box on page C-163](#)), select **Batch-download** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.

Table C-143 Information shown on the List of RAS Information page (for Batch-download)

Item	Description
Log group	Name of a log group
File type	Type of log files that belong to the log group
Number of files	Total number of currently saved log files (the total number of the most recent and previous log files)
Explanation	Explanation of the log file

Table C-144 Operations that can be performed for log groups on the List of RAS Information page (for Batch-download)

Button	Description
Download	Batch download all previous log files that belong to the log group selected. In batch downloading, log files are archived by <code>tar</code> and compressed by <code>gzip</code> . When you perform batch downloading, some data might be missed if the disk selected to store the Temporary Internet files folder for Internet Explorer has insufficient space. In this situation, Internet Explorer does not generate an error or message.

Button	Description
Delete	Batch delete all previous log files that belong to the log group selected.

List of RAS Information page (for List of core files)

You can use the **List of RAS Information** page (for `List of core files`) to view the core files and dump files.

To open the **List of RAS Information** page (for `List of core files`), in the **Check for Errors** dialog box ([Check for Errors dialog box on page C-163](#)), select **List of core files** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.

Note that the system automatically deletes core files that exceeded the set storage period. If a core file has been created, download it and send it to the maintenance personnel. Also, delete those downloaded core files manually. For details about how to set a storage period for core files, see [Core File Auto. Deletion Setup page on page C-208](#).



Note: The dump files are listed along with the core files if the OS dump files are output. 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. Also, there are three levels of dump files, 1, 3, and 4. The names of dump files contain a string such as the following:

`1vdump-file-level (1, 3, or 4)`

Maintenance personnel can obtain level 1 files, but cannot obtain level 3 or 4 files because they contain access data for the file system (NFS services and CIFS services). Depending on the error level, you might be asked by maintenance personnel to collect dump files. Because level 3 and 4 dump files contain user information, be especially careful when managing these files.

Table C-145 Information shown on the List of RAS Information page (for List of core files)

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 space for core files	The amount of free space (units: MB) and used space (units: %) in the OS disk space for storing core files is shown. If there is insufficient free space, delete old, unnecessary core files and downloaded core files.

Table C-146 Operations that can be performed for core files or dump files on the List of RAS Information page (for List of core files)

Button	Description	See
Download	Downloads the core file and dump file selected.	N/A
Delete	Deletes the core file and dump file selected.	N/A
Transfer All Files	Transfers all core files and dump files to an FTP server in a batch operation.	Transfer All Files page on page C-171
Delete All Files	Deletes all core files and dump files.	N/A
Note: N/A = Not applicable.		
Note: These operations must be performed for each node in the cluster.		

List of RAS Information page (for Server check)

You can use the **List of RAS Information** page (for `Server check`) to view the connection between nodes and external servers.

To open the **List of RAS Information** page (for `Server check`), in the **Check for Errors** dialog box ([Check for Errors dialog box on page C-163](#)), select **Server check** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.

Table C-147 Information shown on the List of RAS Information page (for Server check)

Item	Description
Results	You can view the status of the connection between the node and the external servers. For details about the content shown, see the description about the <code>log_interfaces_check</code> file in the <i>Cluster Troubleshooting Guide</i> .

List of RAS Information page (for Transfer all logs including the virtual server logs)

You can use the **List of RAS Information** page (for `Transfer all logs including the virtual server logs`) to transfer all the log files on the node in one operation.

To open the **List of RAS Information** page (for `Transfer all logs including the virtual server logs`), in the **Check for Errors** dialog box ([Check for Errors dialog box on page C-163](#)), select **Transfer all logs including the virtual server logs** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.

Specify the necessary information, and then click **Transfer**.

Table C-148 Information specified in the List of RAS Information page (for Transfer all logs including the virtual server logs)

Item	Description
FTP Server	Specify the IP address or host name of the FTP server.
User name	Specify the user name to log on to the FTP server.
Password	Specify the password of the user.
Directory	Specify the transfer destination directory. You cannot specify a string that contains a non-ASCII character. Create the directory on the FTP server before transferring files.

Transfer All Files page

You can use the **Transfer All Files** page to transfer all core files and dump files to an FTP server in a batch operation.

To open the **Transfer All Files** page, click **Transfer All Files** on the **List of RAS Information** page (for List of core files) ([List of RAS Information page \(for List of core files\) on page C-169](#)).

Specify the necessary information, and then click **Transfer**.

Note:

In some cases, such as when many files to be transferred exist, processing might take a long time, and an error might occur in Internet Explorer. If such cases occur, disable the SmartScreen filter function in Internet Explorer temporarily, and then execute the processing again.

Table C-149 Information specified on the Transfer All Files page

Item	Description
FTP Server	Specify the IP address or host name of the FTP server.
User name	Specify the user name to log on to the FTP server.
Password	Specify the password of the user.
Directory	Specify the transfer destination directory. You cannot specify a string that contains a non-ASCII character. Create the directory on the FTP server before transferring files.

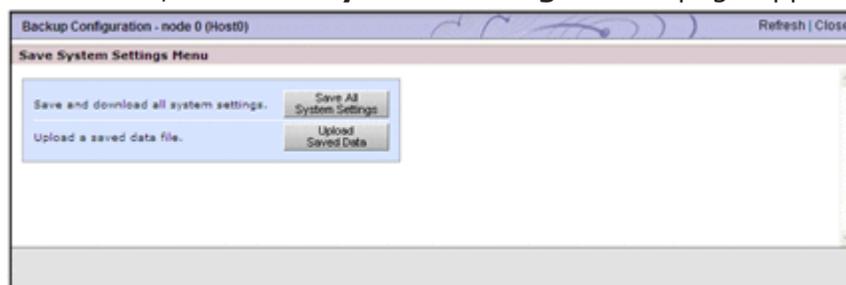
Backup Configuration dialog box

A system administrator uses the **Backup Configuration** dialog box to back up system configuration information (data of the cluster management LU and both OS disks in the cluster).

**Note:**

- If the system configuration file (the file in which system configuration information is archived) is not downloaded, you might not be able to correctly restore the system after a failure occurs in a system LU or storage system. Therefore, download the system configuration file, and then save the file to storage media outside of the system. For details about how to download the system configuration file, see [Save System Settings Menu page on page C-173](#).
- When periodic saving of system configuration information is enabled, if you change the system configuration, you need to manually save the system configuration information, and download the system configuration information file.
- If an error occurs while periodic saving of system configuration information is enabled, and you can still show the **Backup Configuration** dialog box, disable periodic saving. Periodic saving might overwrite correct data with incorrect data generated after the failure.
- The system configuration information file contains password information for system administrators, end users, and administrators of external servers. Be especially careful when managing the downloaded system configuration information file.
- The system administrator cannot edit a downloaded system configuration file. In addition, the system configuration file cannot be used in a different system version of the HDI system.
- Make sure that you set the time for periodic saving to a time period during which no jobs of the NDMP functionality are running. In addition, make sure that you do not execute a command or use the GUI at the time when periodic saving is performed.
- You cannot save the system configuration information when any of the following conditions apply:
 - A failover occurred in the resource group.
 - A cluster, node, or resource group is stopped or an error has occurred in the cluster, node, or resource group.

To open the **Backup Configuration** dialog box, click **Backup Configuration** in the **Advanced** subtab of the **Settings** tab in the *physical-node* window ([physical-node window on page C-91](#)). After the **Backup Configuration** dialog box is shown, the **Save System Settings Menu** page appears.



Save System Settings Menu page

This is the menu window for the backup settings of the system configuration.

The **Save System Settings Menu** page appears first when the **Backup Configuration** dialog box is shown.

Table C-150 Operations that can be performed from the Save System Settings Menu page

Button	Description	See
Save All System Settings	Save system configuration information and download the system configuration information file. Settings related to periodical saving can also be specified.	Save All System Settings page on page C-173
Upload Saved Data	Upload the system configuration information file on the node according to the instruction from maintenance personnel, or delete the uploaded file from the node.	Upload Saved Data page on page C-176

Save All System Settings page

You can use the **Save All System Settings** page to save the system configuration information and download the system configuration information file. Settings related to periodical saving can also be specified.



Note: It takes about 4 minutes to save the system configuration information. When there is a heavy load on a node, a save operation for system LUs might automatically stop to reduce the load on the node (the processing of OS disks times out after about 5 minutes from the start of the save processing, and the processing of a cluster management LU times out after about 20 minutes). In this case, after the load on the node is reduced and stabilized, retry the save operation.

To open the **Save All System Settings** page, click **Save All System Settings** on the **Save System Settings Menu** page in the **Backup Configuration** dialog box ([Backup Configuration dialog box on page C-171](#)).

Table C-151 Information shown in the Save All System Settings page

Item	Description
Cluster management LU save status	Information about the cluster management LU.
Cluster management LU status	The save and restore status of the cluster management LU: Normal The save or restore processing for the data of the cluster management LU has finished. Now saving... The data of the cluster management LU is being saved.

Item	Description
	<p>Now restoring...</p> <p>The data of the cluster management LU is being restored.</p> <p>When the status of the cluster management LU is not <code>Normal</code>, do not save or download system configuration information.</p>
Last save date of cluster management LU	<p>The date and time the cluster management LU was last saved.</p> <p>Note that a hyphen (-) is shown in the following cases:</p> <ul style="list-style-type: none"> • The saved data of the cluster management LU does not exist on the node. • The data of the cluster management LU and both OS disks in the cluster is being saved. • The data of the cluster management LU and both OS disks in the cluster is being restored. • The system configuration file that stores the data of the cluster management LU and both of the OS disks in the cluster is being uploaded.
OS disk save status	<p>Information about the OS disk.</p> <p>In the left area, information about the OS disk of the node that you are currently accessing is shown.</p> <p>In the right area, information about the OS disk of the other node in the cluster is shown.</p> <p>To the right of the text OS disk save status, the node number and node host name are shown in the following format:</p> <p><i>(node-number (host-name))</i></p>
OS disk status	<p>The save and restore status of the OS disk:</p> <p><code>Normal</code></p> <p>The save or restore processing for the data of the OS disk has finished.</p> <p>Now saving...</p> <p>The data of the OS disk is being saved.</p> <p>Now restoring...</p> <p>The data of the OS disk is being restored.</p> <p>When the status of the OS disk is not <code>Normal</code>, do not save or download system configuration information.</p>
Last save date of OS disk	<p>The date and time the OS disk was last saved.</p> <p>Note that a hyphen (-) is shown in the following cases:</p> <ul style="list-style-type: none"> • The saved data of the OS disk does not exist on the node. • The data of the cluster management LU and both OS disks in the cluster is being saved. • The data of the cluster management LU and both OS disks in the cluster is being restored.

Item	Description
Schedule setting status	Whether periodic saving of system configuration information is enabled or disabled: On Periodic saving is enabled. Off Periodic saving is disabled.
Schedule interval	The interval when periodic saving of system configuration information is run. Daily Periodic saving is run daily. Weekly Periodic saving is run on a specified day of the week. The specified day of the week is also shown. Monthly Periodic saving is run on a specified date every month. The specified date is also shown.
Scheduled time	The time when periodic saving of system configuration information starts.
Output setting	The location to which the system configuration file is periodically saved. Transfer to HCP The system configuration file is to be saved in an HCP system. directory-path The output directory is shown when the system configuration file is to be saved in a file system. - is shown if the system configuration file is not output.

Table C-152 Operations that can be performed from the Save All System Settings page

Button	Description	See
Batch Save and Download	Download the system configuration information file.#	N/A
Save	Save system configuration information.	N/A
Save and Download	Download the system configuration information file.#	N/A
Enable Scheduling or Disable Scheduling	Enable or disable periodic saving of system configuration information. You can check the setting status in the Schedule setting status on the Save All System Settings page.	N/A
Modify Schedule	Set a schedule for periodic saving of system configuration information.	Schedule Settings for

Button	Description	See
		Saving All System Settings page on page C-177
<p>Note: N/A = Not applicable.</p> <p>#: When processing for saving system configuration information has finished, the system configuration information file is downloaded to the destination specified in the downloading dialog box for the Web browser. The file is automatically named in the following format:</p> <pre>sysbk_FC-GWserial-number-of-node0_YYYYMMDD_hhmm.tgz</pre> <p>Hitachi Data Systems recommends that you do not change the file name. If you want to change the file name, use the following characters: alphanumeric characters, periods (.), hyphens (-), and underscores (_).</p>		

Upload Saved Data page

Upload the system configuration information file on the node according to the instruction from maintenance personnel, or delete the uploaded file from the node.



Note: When you restore the data of the system LUs, check the following:

- If a file system is deleted after downloading the system configuration file, you need to manually delete the file system again after restoring the data of the system LUs. If CIFS shares have been created, release them. (NFS shares will automatically be released.)
- When you want to restore the other settings that were changed after downloading the file, retry the same setting operation after restoring the data of the system LUs.

To open the **Upload Saved Data** page, click **Upload Saved Data** on the **Save System Settings Menu** page in the **Backup Configuration** dialog box ([Backup Configuration dialog box on page C-171](#)).

Table C-153 Information shown in the Upload Saved Data page

Item	Description
Name of saved file	The name of the system configuration file if the file has already been uploaded. If the file has not been uploaded, a hyphen (-) is shown.
Available OS disk space (KB)	The amount of free space in the OS disk. If there is no free space, or the information about space cannot be obtained, a hyphen (-) is shown.

Table C-154 Operations that can be performed from the Upload Saved Data page

Button	Description
Upload	Specify the system configuration information file to be uploaded to the node. Clicking Upload shows the Select Saved Data File page. For Saved file , specify the absolute path of the system configuration information file.
Delete	Delete the system configuration information file uploaded to the node. Note: This operation does not allow you to delete a system configuration file that has been transferred by using the <code>scp</code> command. For details about how to delete a system configuration file that has been transferred by using the <code>scp</code> command, see the <i>CLI Administrator's Guide</i> .

Schedule Settings for Saving All System Settings page

You can use the **Schedule Settings for Saving All System Settings** page to set a schedule for periodic saving of system configuration information.

Hitachi Data Systems recommends that you enable periodic saving of system configuration information on only one of the nodes.



Note: Saving system configuration information imposes heavy loads on the node. When specifying a date and time for an interval for periodic saving, avoid time periods when you expect heavy access to the node (such as when the system administrator performs maintenance tasks or when end users use file systems).

In addition, we recommend that you avoid periods that will include the switchover date for daylight saving time when specifying the start time of periodic saving. If periodic saving is executed on the switchover date for daylight saving time, data might not be saved or might be saved twice.

To open the **Schedule Settings for Saving All System Settings** page, click **Modify Schedule** on the **Save All System Settings** page, which is shown by clicking **Save All System Settings** on the **Save System Settings Menu** page in the **Backup Configuration** dialog box ([Backup Configuration dialog box on page C-171](#)).

Table C-155 Information specified on the Schedule Settings for Saving All System Settings page

Item	Description
Interval	The interval in which periodic saving of system configuration information is run. Select an option. Daily Periodic saving is run daily.

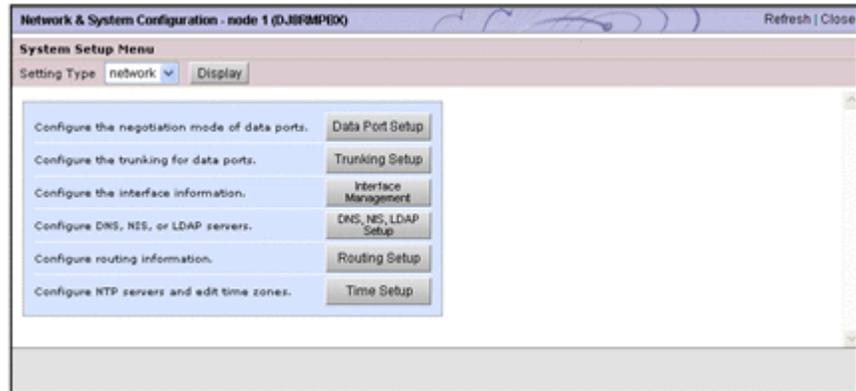
Item	Description
	<p>Weekly</p> <p>Periodic saving is run on the specified day of the week. Select the check box to specify the day of the week when periodic saving is to be run.</p> <p>Monthly</p> <p>Periodic saving is run on the specified date every month. Select the check box to specify the date when periodic saving is to be run.</p> <p>Periodic saving is not run on a date that does not exist for a given month. (Example: the 31st day of February)</p>
Time	The time when periodic saving starts. You can specify the time in one-minute units, in the range from 00:00 to 23:59.
Output setting	<p>Specify the location to which the system configuration file is to be saved.</p> <p>Transfer to HCP</p> <p>Select to save the system configuration file in an HCP system.</p> <p>Output directory</p> <p>Select to save the system configuration file in a file system. In the text box, specify the directory to save the system configuration file in. Make sure that you specify an absolute path that begins with <code>/mnt/#</code>.</p> <p>If you click Select, the List of Mounted File Systems page is shown. Select the target file system.</p> <p>Not output</p> <p>Select when the system configuration file is not to be output.</p>
<p>#: Specify a directory in a file system that is mounted with both read and write operations permitted. Note that the following directories cannot be specified:</p> <ul style="list-style-type: none"> • A directory whose path contains a symbolic link • A directory in a file system that shares data with other HDI systems via the linked HCP • A directory whose path contains any of the following directory names: <code>.conflict, .conflict_longpath, .history, .snaps, .lost+found</code> • The following directories directly under a file system: <code>.arc, .system_gi, .system_reorganize, and lost+found</code> 	

Network & System Configuration dialog box

You can configure the network and system in the **Network & System Configuration** dialog box. By using commands, you can manage the current time of a node, the assignment of user LUNs, and FC paths.

To open the **Network & System Configuration** dialog box, in the *physical-node* window ([physical-node window on page C-91](#)), click **Network & System Configuration** in the **Advanced** subtab of the **Settings** tab. After

the **Network & System Configuration** dialog box is shown, the **System Setup Menu** page appears.



System Setup Menu page

To open the menu window, select an item from the **Setting Type** drop-down list, and then click **Display** from the **System Setup Menu** page.

The **System Setup Menu** page first appears after the **Network & System Configuration** dialog box is shown.

Select the item in the **Setting Type** drop-down list, and click **Display**.

Table C-156 Targets that can be selected from the Setting Type drop-down list on the System Setup Menu page

Item	Description	See
network	Specify settings related to the network.	System Setup Menu page (Setting Type: network) on page C-179
system	Specify settings related to the system.	System Setup Menu page (Setting Type: system) on page C-180

System Setup Menu page (Setting Type: network)

You can use the **System Setup Menu** page (**Setting Type**: network) to specify the settings related to the network.

To open the **System Setup Menu** page (**Setting Type**: network), select **network** from the **Setting Type** drop-down list on the **System Setup Menu** page in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)), and then click **Display**.

Table C-157 Operations that can be performed from the System Setup Menu page (Setting Type: network)

Button	Description	See
Data Port Setup	Set the negotiation mode for the port. This operation must be performed for each node in the cluster.	List of Data Ports page on page C-181
Trunking Setup	Specify trunking for the data port.	List of Trunking Configurations page on page C-187
Interface Management	Set interface information.	List of Interfaces page on page C-192
DNS, NIS, LDAP Setup	Set DNS, NIS, and LDAP server information.	DNS, NIS, LDAP Setup page on page C-197
Routing Setup	Set routing information.	List of Routings page on page C-200
Time Setup	Set NTP server information and time zone.	Time Setup page on page C-203

System Setup Menu page (Setting Type: system)

You can use the **System Setup Menu** page (**Setting Type:** `system`) to specify the settings related to the system.

To open the **System Setup Menu** page (**Setting Type:** `system`), select **system** from the **Setting Type** drop-down list on the **System Setup Menu** page in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)), and then click **Display**.

Table C-158 Operations that can be performed from the System Setup Menu page (Setting Type: system)

Button	Description	See
Syslog Setup ^{#1}	Edit the system log setup file (<code>syslog.conf</code>).	Syslog Setup page on page C-204
Log File Capacity Setup ^{#1}	Set the maximum number of log files that can be saved and the file capacity.	Log File Capacity Setup page on page C-206
Core File Auto. Deletion Setup ^{#1}	Set the storage period for a core file and the time to automatically delete the core file.	Core File Auto. Deletion Setup page on page C-208
Edit System File ^{#2}	Edit the HDI system file.	Edit System File page on page C-209
Performance Tuning ^{#1}	Tune the system performance. However, there is no need to change the settings during normal operation.	Performance Tuning page on page C-213

Button	Description	See
SNMP Setup ^{#1}	When using SNMPv2, set SNMP manager information, community name, and MIB object configuration.	List of SNMPs page on page C-214
Select User Interface	Select the user interface mode used for setting quotas.	Select User Interface page on page C-216
<p>#1: Perform the operation for each node in the cluster.</p> <p>#2: Certain settings must be specified for each node in the cluster. For details, see the references.</p>		

List of Data Ports page

You can use the **List of Data Ports** page to view information about the port.

To open the **List of Data Ports** page, click **Data Port Setup** on the **System Setup Menu** page (**Setting Type:** *network*) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-159 Information shown in the List of Data Ports page

Item	Description
Data port	The name of the data port (<i>ethnumber</i> or <i>xgbenumber</i>). <i>mng0</i> is shown in the same way as other data ports.
Media type	The media type of the port. Copper Metal cables are supported. Fiber Optical cables are supported.
Negotiation mode	The negotiation mode for the port. Auto Auto negotiation is used. 10GBase Full Duplex 10GBase full duplex communication is used. The negotiation mode is fixed. 1000Base Full Duplex (Auto Negotiation) 1000Base full duplex communication is used. Auto negotiation is also used. 100Base Full Duplex 100Base full duplex communication is used. The negotiation mode is fixed. 100Base Full Duplex (Auto Negotiation) [#] 100Base full duplex communication is used. Auto negotiation is also used. 100Base Half Duplex

Item	Description
	<p>100Base half duplex communication is used. The negotiation mode is fixed.</p> <p>100Base Half Duplex(Auto Negotiation) #</p> <p>100Base half duplex communication is used. Auto negotiation is also used.</p>
Connected status	<p>The communication status of a port.</p> <p>Link status</p> <p>The link status.</p> <p>Up</p> <p>The link is connected normally.</p> <p>Down</p> <p>The link is disconnected. Check the negotiation mode of the switch connected to the port, and then set the negotiation mode again.</p> <p>Error</p> <p>The link cannot be recognized. If this is shown, an error might have occurred in the HDI system. Download all the File Services Manager log files, and contact maintenance personnel. For details about how to download log files, see List of RAS Information page on page C-164.</p> <p>Speed</p> <p>The current communication speed. Note that 10Base is not a recommended communication speed. Check and, if necessary, correct the setting of the connected switch so that the communication speed is 100BASE or greater. - is shown if communication is not being performed (Link status is Down).</p> <p>Duplex</p> <p>The current communication method.</p> <p>Full</p> <p>Full duplex communication is used.</p> <p>This is also displayed when the negotiation mode of the connected switch is auto negotiation and Negotiation mode of the HDI port is Auto.</p> <p>Half</p> <p>Half duplex communication is used.</p> <p>This is also displayed when the negotiation mode of the connected switch is fixed mode (non-auto-negotiation 100Base half duplex, 100Base full duplex, or 10GBase full duplex) and Negotiation mode of the HDI port is Auto.</p> <p>-</p> <p>Communication is not being performed (Link status is Down).</p>
	<p>#: If the negotiation mode is set to 100Base Full Duplex or 100Base Half Duplex in system versions earlier than 3.2.3, then after an upgrade installation, the negotiation mode is displayed as 100Base Full Duplex(Auto Negotiation) or 100Base Half Duplex(Auto Negotiation).</p>

Table C-160 Operations that can be performed from the List of Data Ports page

Button	Description	See
Negotiation Mode Setup	Change the negotiation mode for the selected port. This operation must be performed for each node in the cluster.	Negotiation Mode Setup page on page C-183

Negotiation Mode Setup page

You can use the **Negotiation Mode Setup** page to change the negotiation mode for the selected port. This operation must be performed for each node in the cluster.



Note: If you change the negotiation mode while a resource group is running and the switch settings are also changed, all the port communication links might temporarily go down. If you want to change the negotiation mode while a resource group is running, on the **Browse Cluster Status** page (for *Resource group status*), disable the monitoring of the resource groups, change the negotiation mode, and then restart the monitoring. For details about the **Browse Cluster Status** page, see [Browse Cluster Status page on page C-271](#).

If you set a negotiation mode that differs from the one set for the connected switch, a linkage error might occur, preventing communication with the port. If communication cannot be established, check whether the negotiation modes for the port and the connected switch are the same. If the negotiation modes are the same, the problem might pertain to a hardware error. Contact maintenance personnel, if necessary.

For details about the communication status when the connected switch or HDI is using auto negotiation, and the negotiation modes for a port and the connected switch are different, see [Table C-162 Network communication status when auto negotiation is being used, and the negotiation modes for a port and the connected switch are different on page C-185](#).

To ensure that the negotiation mode setting of the connected switch matches the negotiation mode setting of the HDI port:

1. Display the **List of Data Ports** page.
2. Make sure that **Negotiation mode** is **Auto**.
The default mode for the HDI port is **Auto**. If the current mode is not **Auto**, change it to **Auto**.

Note:

If **Negotiation mode** of the HDI port is **Auto**, you can identify the negotiation mode of the connected switch in step 4.

3. In **Connected status**, make sure that **Speed** is 100Base or better.
If it is **10Base** or a hyphen (-), a problem may have occurred with a LAN cable, a port, or the connected switch. Resolve the problem.

4. In **Connected status**, review the information in **Duplex** and then take the necessary actions.

If **Duplex** is **Half**:

You can assume that the negotiation mode setting of the connected switch is fixed mode (non-auto-negotiation 100Base half duplex, 100Base full duplex, or 10GBase full duplex).

Change the negotiation mode of the HDI port so that it matches the negotiation mode of the connected switch.

If **Duplex** is **Full**:

You can assume that the negotiation mode setting of the connected switch is auto negotiation.

If you already changed **Negotiation mode** of the HDI port to **Auto** in step 2, you do not need to cancel the change.

To open the **Negotiation Mode Setup** page, click **Negotiation Mode Setup** on the **List of Data Ports** page in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-161 Information specified in the Negotiation Mode Setup page

Item	Description
ethnumber	<p>Select a negotiation mode for each <i>ethnumber</i> from the drop-down list.</p> <p>Auto Select this to use the auto negotiation mode for communication.</p> <p>1000Base Full Duplex(Auto Negotiation) Select this to use 1000Base full duplex communication. Auto negotiation is also used.</p> <p>100Base Full Duplex Select this to use 100Base full duplex communication. The negotiation mode is fixed.</p> <p>100Base Half Duplex Select this to use 100Base half duplex communication. The negotiation mode is fixed.</p> <p>100Base Full Duplex(Auto Negotiation) Select this to use 100Base full duplex communication. Auto negotiation is also used.</p> <p>100Base Half Duplex(Auto Negotiation) Select this to use 100Base half duplex communication. Auto negotiation is also used.</p>
mng0	<p>Select a negotiation mode for <i>mng0</i> from the drop-down list. Only Auto is selectable for 10GbE ports.</p> <p>Auto Select this to use the auto negotiation mode for communication.</p> <p>1000Base Full Duplex(Auto Negotiation)</p>

Item	Description
	<p>Select this to use 1000Base full duplex communication. Auto negotiation is also used.</p> <p>100Base Full Duplex</p> <p>Select this to use 100Base full duplex communication. The negotiation mode is fixed.</p> <p>100Base Half Duplex</p> <p>Select this to use 100Base half duplex communication. The negotiation mode is fixed.</p> <p>100Base Full Duplex(Auto Negotiation)</p> <p>Select this to use 100Base full duplex communication. Auto negotiation is also used.</p> <p>100Base Half Duplex(Auto Negotiation)</p> <p>Select this to use 100Base half duplex communication. Auto negotiation is also used.</p>
<i>xgbenumber</i>	<p>Select a negotiation mode for each <i>xgbenumber</i> from the drop-down list.</p> <p>When the model of the node is D51B-2U, only Auto is selectable.</p> <p>Auto</p> <p>Select this to use the auto negotiation mode for communication. When the model of the node is not D51B-2U, this mode can be selected only when the port supports metal cables.</p> <p>10GBase Full Duplex</p> <p>Select this to use 10GBase full duplex communication. The negotiation mode is fixed. When the model of the node is not D51B-2U, this mode can be selected only when the port supports optical cables.</p> <p>After setting the negotiation mode, confirm that 10GBase is displayed for Speed on the List of Data Ports page. If 10GBase is not displayed, correct the network configuration, such as the settings of the connected switch or LAN cables.</p>

Table C-162 Network communication status when auto negotiation is being used, and the negotiation modes for a port and the connected switch are different

Negotiation mode for the port	Negotiation mode for the connected switch	Value displayed in Connected status on the List of Data Ports page
Auto negotiation mode (when Auto is set)	Auto negotiation mode	<p>The communication status is chosen, in the following order, depending on the negotiation modes of the port and the connected switch: #1</p> <ol style="list-style-type: none"> 1. 10GBase full duplex 2. 1000Base full duplex 3. 1000Base half duplex

Negotiation mode for the port	Negotiation mode for the connected switch	Value displayed in Connected status on the List of Data Ports page
		4. 100Base full duplex 5. 100Base half duplex 6. 10Base full duplex 7. 10Base half duplex Note that, for 10GbE ports, even if auto negotiation mode is enabled for both the port and the connected switch, the following communication cannot be used: 1000Base half duplex communication, 10Base full duplex communication, and 10Base half duplex communication. Note that 10Base is not a recommended communication speed. Correct the setting of the connected switch so that the communication speed is 100Base or greater.
	100Base half duplex	100Base half duplex
	100Base full duplex	100Base half duplex ^{#2}
100Base half duplex (when 100Base Half Duplex is set)	Auto negotiation mode	100Base half duplex
100Base full duplex (when 100Base Full Duplex is set)	Auto negotiation mode	100Base full duplex ^{#2}
Auto negotiation mode: • 1000Base full duplex (when 1000Base Full Duplex(Auto Negotiation) is set)	Auto negotiation mode	1000Base full duplex
Auto negotiation mode: • 100Base half duplex (when 100Base Half Duplex(Auto Negotiation) is set)	Auto negotiation mode	100Base half duplex
	100Base half duplex	100Base half duplex
	100Base full duplex	100Base half duplex ^{#2}
Auto negotiation mode: • 100Base full duplex (when 100Base Full Duplex(Auto Negotiation) is set)	Auto negotiation mode	100Base full duplex
	100Base half duplex	Communication impossible ^{#2}

Negotiation mode for the port	Negotiation mode for the connected switch	Value displayed in Connected status on the List of Data Ports page
	100Base full duplex	Communication impossible ^{#2}
<p>#1: Depending on the switch type, the actual communication speed might become lower than expected or communication might become impossible even if the auto negotiation mode is set for both the port and switch. In this case, configure the fixed negotiation modes so that the settings on both the port and switch are the same.</p> <p>#2: When one of the connected devices uses auto negotiation mode and the other uses the fixed mode, the device in auto negotiation mode will use the half duplex method. At this time, if the other device uses the full duplex method, communication between the devices might be impossible because the negotiation modes do not match. Even if communication is possible, the throughput and response might degrade.</p>		

List of Trunking Configurations page

You can use the **List of Trunking Configurations** page to specify trunking for the data port.



Note:

- Trunking cannot be specified for `mng0`.
- Cascaded trunking is recommended for trunking setup. To set cascaded trunking, first set link aggregation on the **Link Aggregation Setup** page of the **Network & System Configuration** dialog box. Then, set link alternation on the **Link Alternation Setup** page.
- If you enable cascaded trunking for a port, always set up a tagged VLAN for that port in order to stabilize the communication between the client and the HDI system.
- When using cascaded trunking, always use it together with a tagged VLAN. If a VLAN is not used together with cascaded trunking, the communication between the client and an HDI system might not be stable.
- Make sure that an OS is running on each node.
- When an interface has been created for a data port in which trunking will be set up, edited, or deleted, make sure that the cluster either is running normally or was stopped without any problems.
- When an interface has been created for a data port in which trunking will be set up, edited, or deleted, and that interface is being used, make sure that the resource groups on both nodes either are running normally or were stopped without any problems.
- If you edit the trunking information, the virtual IP address is reconfigured. Reconfiguration of a virtual IP address usually takes about 10 to 20 seconds. However, it might take longer if the system load is high.

- When you edit trunking settings, you will temporarily be unable to communicate with or use any services by way of the interface of the target port.
- If trunking is set during operation of the HDI system, the system automatically deletes the interface information (including VLAN settings) set for the data port selected as the trunking target, and routing information set for the corresponding interface.
- 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 trunking is set or released, the number of virtual IP addresses for running resource groups might become 0. If this situation occurs, the CIFS service will not stop, but CIFS access will be unavailable. To enable CIFS access, set virtual IP addresses.
- If you have changed trunking settings, review the interface information, routing information, and VLAN settings.
- You cannot trunk data ports that have different negotiation modes or different communication speeds or methods. Check the **List of Data Ports** page in the **Network & System Configuration** dialog box, and only trunk ports that have identical **Negotiation mode**, **Speed**, and **Duplex** settings.

To open the **List of Trunking Configurations** page, click **Trunking Setup** on the **System Setup Menu** page (**Setting Type**: *network*) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-163 Information shown in the List of Trunking Configurations page

Item	Description
Trunking configuration	The trunking configuration.
Port	<p>The port name.</p> <p><i>agrnumber</i></p> <p>Shown for a link aggregation port.</p> <p>When cascaded trunking is used, the name of the link aggregation port that comprises the link alternation is shown.</p> <p><i>rdnnumber</i></p> <p>Shown for a link alternation port or a cascaded trunking port.</p> <p><i>ethnumber</i> or <i>xgbnumber</i></p> <p>The name of the data port.</p> <p>When trunking is used, the names of the data ports that make up the trunking are shown.</p>
Trunking type	<p>The type of trunking being used.</p> <p>Link Aggregation</p> <p>Shown for a link aggregation port.</p>

Item	Description
	<p>Link Alternation</p> <p>Shown for a link alternation port or a cascaded trunking port.</p> <p>-</p> <p>Shown for ports for which trunking is not set. This is also shown for ports that comprise a trunking configuration.</p>
Link status	<p>The link status of each port.</p> <p>Up</p> <p>The link is normal.</p> <p>Down</p> <p>The link is disconnected.</p> <p>Note that, immediately after link trunking settings are changed, <code>Down</code> might be shown for the port that comprises link trunking even if <code>Up</code> is shown for the link trunking port. Click Refresh after a short time has passed to update the contents shown to the latest information.</p>
MII (ms)	<p>The monitoring interval for the Media Independent Interface link status set for the link aggregation port or the link alternation port.</p>
LACP	<p>The LACP interval (checking interval for the status of aggregated ports) set in the link aggregation port, and shows whether each port is currently aggregated.</p> <p>Rate</p> <p>Shows <code>Slow</code> or <code>Fast</code> as the LACP interval.</p> <p><code>Slow</code></p> <p>The LACP interval is set to 30 seconds.</p> <p><code>Fast</code></p> <p>The LACP interval is set to 1 second.</p> <p>Aggregate</p> <p>Shows whether each port is currently aggregated.</p> <p>If <code>Aggregated</code> is shown for all ports that comprise the link aggregation port, all the ports have been aggregated.</p> <p><code>Aggregated</code></p> <p>Indicates that the port is currently aggregated.</p> <p><code>Not aggregated</code></p> <p>Indicates that the port has not participated in aggregation.</p> <p>Note that <code>Not aggregated</code> might be shown for a port that has normally participated in aggregation, for example, immediately after trunking settings are changed. Click Refresh after a short time has passed to update the contents shown to the latest information.</p>
Active port	<p>The status of the ports for which link alternation is set.</p> <p>Status</p> <p><code>Active</code></p> <p>Indicates that the port is operating.</p> <p><code>Standby</code></p> <p>Indicates that the port is standing by.</p>

Item	Description
	<p>Default</p> <p>Shown for the port that is set to operate during normal operation.</p>

Table C-164 Operations that can be performed from the List of Trunking Configurations page

Button	Description	See
Create Link Aggregation	Set link aggregation for the selected ports.	Link Aggregation Setup page on page C-191
Create Link Alternation	Set link alternation for the selected two ports.	Link Alternation Setup page on page C-191
Edit Trunking	Change the trunking settings for the selected port. To change a link aggregation port, click the Release Trunking button to cancel the link aggregation settings, and then click the Edit Trunking button to set up link aggregation again.	For a link aggregation port: Link Aggregation Setup page on page C-191 For a link alternation port: Link Alternation Setup page on page C-191 For a cascaded trunking port: Edit Cascaded Trunking page on page C-192
Release Trunking	Cancel the trunking settings for the selected port.	N/A
Change Active Port Status	Replace the selected port used for link alternation with another port. This operation must be performed for each node in the cluster. The system administrator 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, after link alternation occurs automatically when an error occurs in a port set for link alternation, link alternation back to the port that is used in normal operation does not occur automatically even after the failed link is recovered and ready to communicate. To get the port operation back to the one before the error occurred, the	N/A

Button	Description	See
	system administrator must perform link alternation again using the List of Trunking Configurations page.	
Note: N/A = Not applicable.		

Link Aggregation Setup page

You can use the **Link Aggregation Setup** page to set up link aggregation.

The **Link Aggregation Setup** page is shown by performing either of the following operations in the **List of Trunking Configurations** page of the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

- Selecting two or more ports and then clicking **Create Link Aggregation**
- Selecting a link aggregation port and then clicking **Edit Trunking**

Table C-165 Information specified in the Link Aggregation Setup page

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. Slow Select this to conduct a status check every 30 seconds. Fast Select this to conduct a status check every second.
MII	Specify the interval for checking the Media Independent Interface link status, as a value from 1 to 100 in units of 10 milliseconds.

Link Alternation Setup page

You can use the **Link Alternation Setup** page to set up link alternation.



Note: In the **List of Trunking Configurations** page, 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 latest status, click **Refresh**. If the port to be used during normal operation does not become *Active* within 5 seconds, one of the other ports that comprise link alternation automatically becomes *Active*. To make the port to be used during normal operation become *Active*, switch the link manually.

The **Link Alternation Setup** page is shown by performing either of the following operations in the **List of Trunking Configurations** page of the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

- Selecting two ports and then clicking **Create Link Alternation**

- Selecting a link alternation port and then clicking **Edit Trunking**

Table C-166 Information specified in the Link Alternation Setup page

Item	Description
Default active port	This is a drop-down list that lets you select the port to be used during normal operation. Select a port that is in the normal state. You can check the link status in Link status of the List of Trunking Configurations page.
MII	Specify the interval for checking the Media Independent Interface link status, as a value from 1 to 100 in units of 10 milliseconds.

Edit Cascaded Trunking page

You can use the **Edit Cascaded Trunking** page to change the trunking settings for the selected port.

To open the **Edit Cascaded Trunking** page, select a cascaded trunking port and then click **Edit Trunking** on the **List of Trunking Configurations** page in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-167 Information specified in the Edit Cascaded Trunking page

Type of trunking	Item	Description
<i>rdnnumber</i> (Link alternation)	Default active port	From the drop-down list, select the port to be used during normal operation. Hitachi Data Systems recommends that you select a link aggregation port for cascaded trunking setup.
	MII	Specify the interval for checking the Media Independent Interface link status as a value from 1 to 100 in units of 10 milliseconds.
<i>agrnumber</i> (Link aggregation)	LACP rate	From the drop-down list, select the interval for checking the status of ports for which link aggregation is set. Slow Select this to conduct a status check every 30 seconds. Fast Select this to conduct a status check every second.
	MII	Specify the interval for checking the Media Independent Interface link status as a value from 1 to 100 in units of 10 milliseconds.

List of Interfaces page

You can use the **List of Interfaces** page to set the interface information.



Note: Before managing an interface, be aware of the following:

- Whenever interface settings are to be changed, all clients accessing the HDI system by way of the interface must be notified ahead of time that the interface settings will be changed.
- Whenever interface settings are changed, you will temporarily be unable to communicate or use any services by way of that interface, even if you do not change the virtual IP address.
- Make sure that the OSs are running on both nodes, and the cluster is either is running normally or was stopped without any problems.
- Before managing an interface (other than `mng0`), the following is required:
 - When adding or changing a virtual IP address for an active resource group:
 - Make sure that the port's communication link is up.
 - When changing the fixed IP address of the interface whose virtual IP address is being used for an active resource group:
 - Make sure that the port's communication link is up.
 - When adding, changing, or deleting a virtual IP address for a resource group:
 - Make sure that the resource groups on both nodes either are running normally or were stopped without any problems.
 - When changing the fixed IP address of the interface whose virtual IP address is being used for the resource group:
 - Make sure that the resource groups on both nodes either are running normally or were stopped without any problems.
- To change the fixed IP address, netmask, prefix length, or MTU value of the `mng0` interface, you must stop the resource groups on both nodes and the cluster. After you have changed the settings, restart the resource groups and the cluster that were stopped.
- To connect a BMC port to an IP switch, the network address of the BMC port must be the same as the network address of `mng0`. To disconnect a BMC port from an IP switch, you need to make sure that the network address of the BMC port is different from the network address of `mng0`. When changing the connection configuration, you must use the `bmcctl` command to change the BMC port settings.
- If the number of virtual IP addresses of running resource groups becomes 0, the CIFS service will not stop, but CIFS access will be unavailable. To enable CIFS access, set virtual IP addresses.
- Before using Jumbo Frame packets, make sure that the peripheral equipment and clients support Jumbo Frame packets, and then set an appropriate MTU value.
- If you change an interface MTU value, change the peripheral equipment and client MTU values to the same values. For details about how to change peripheral equipment and client MTU values, see the documentation corresponding to the peripheral equipment and clients. If the MTU value is changed while a resource group is running and the switch settings are also changed, all the port communication links might

temporarily go down. If you want to change the MTU value while a resource group is running, disable the monitoring of the resource groups on both nodes, change the MTU value, and then restart the monitoring. For details about how to disable or restart the monitoring of resource groups, see [Browse Cluster Status page on page C-271](#).

- If switching the IP addresses between the nodes or changing an interface IP address to one that was just being used by another interface, then communication might not be possible for the interfaces until the ARP cache for the external equipment (such as routers and other servers) is refreshed.
- Do not edit interface or network information while data is being migrated to an HCP system. If the information is edited, data might not be migrated correctly.

To open the **List of Interfaces** page, click **Interface Management** on the **System Setup Menu** page (**Setting Type:** *network*) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

To view specific information, select the corresponding items from the **Protocol version** and **Port** drop-down lists, and then click **Display**.

Table C-168 Information shown in the List of Interfaces page

Item	Description
Interface	Interface information. Port The port name. VLAN ID The VLAN ID. A hyphen (-) is shown if a VLAN is not used.
Node or virtual server name	The host name of the node.
Fixed IP addr ^{#1}	The fixed IP address. A hyphen (-) is shown if the fixed IP address has not been specified.
Virtual IP addr ^{#1}	The virtual IP address. A hyphen (-) is shown if the virtual IP address has not been specified.
Netmask	The netmask for IPv4.
Prefix length	The prefix length for IPv6.
MTU ^{#2}	The MTU values.
<p>#1: If the information cannot be obtained because the OS is not running, a communication error occurred, or for some other reason, <code>Unknown</code> is shown. If the collected information is invalid, such as when the interface settings have been specified for only one node or when different IP addresses are specified for network addresses in the same interface, <code>Invalid</code> is shown. When <code>Invalid</code> is shown, a value is shown on the next line in the format <code>(incorrect-value)</code>.</p> <p>For example:</p> <pre>Invalid</pre>	

Item	Description
(192.168.0.1)	<p>#2: If the MTU values in the cluster do not match each other, <code>Invalid</code> is shown, and the values are shown on the following line in the format <code>(MTU-value-of-the-node-currently-being-accessed, MTU-value-of-the-other-node)</code>.</p> <p>If an MTU value cannot be obtained because the OS is not running, a communication error has occurred, or for some other reason, <code>Unknown</code> is shown.</p> <p>Example:</p> <pre>Invalid (1500,Unknown)</pre> <p>If an MTU value cannot be obtained for some other reason, <code>None</code> is shown.</p> <p>Example:</p> <pre>Invalid (1500,None)</pre>

Table C-169 Operations that can be performed from the List of Interfaces page

Button	Description	See
Edit	Edits the configuration information for the selected interface.	Edit Interface page on page C-195
Delete	<p>Deletes the configuration information for the selected interface.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Before deleting interface and network information, make sure that the OSs are running on both nodes, and that the cluster either is running normally or was stopped without any problems. In addition, make sure that the resource groups either are running normally or were stopped without any problems. • Regardless of the protocol version that was shown in the List of Interfaces page, all the interface and network information for the selected interface is deleted. 	N/A
Add	Adds an interface used to connect to the network.	Add Interface page on page C-196
Note: N/A = Not applicable.		

Edit Interface page

You can use the **Edit Interface** page to edit the configuration information for the selected interface.



Note: If you change the value of **Fixed** in **IP address**, **Netmask**, or **Prefix length** for `mng0`, click **Close** to close the dialog box. To resume the

operation, wait a while and then open the dialog box again from the **Settings** tab.

- If you have changed the fixed IP address of the data port used for connection to the management server, re-register the new IP address in the **Edit Node** dialog box.
- When you are using the front-end LAN to manage the HDI system and you want to change the settings for the data port used for management, use the management console deployed in the management LAN to change the settings. If you use the management console deployed in the front-end LAN to change the settings, the GUI might not respond. In that case, click **X** in the title bar to close the window.

To open the **Edit Interface** page, select the target interface on the **List of Interfaces** page in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)), and then click **Edit**.

For details about the information to be specified in the **Edit Interface** page, see [Table C-170 Information specified in the Add Interface page on page C-196](#). Note that you cannot change the values set for **Port** and **Tagged VLAN** in the **Edit Interface** page.

Add Interface page

You can use the **Add Interface** page to add an interface used to connect to the network.

To open the **Add Interface** page, click **Add** on the **List of Interfaces** page in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-170 Information specified in the Add Interface page

Item	Description
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), select Use for Tagged VLAN from the options.
Tagged VLAN	Select whether to use a tagged VLAN from the options. Use Use a tagged VLAN. When you select Use , enter any VLAN ID for VLAN ID . Do not use Do not use a tagged VLAN.
Fixed in IP address ^{#1}	Enter a fixed IP address for each node. This is required for <code>mng0</code> using IPv6.
Virtual in IP address ^{#1}	Specify the virtual IP address that clients use to connect to the services of a resource group.

Item	Description
Netmask	Specify the netmask for both nodes for IPv4.
Prefix length	Specify the prefix length for both nodes for IPv6.
MTU^{#3}	Specify the MTU value of an interface from 1280 to 9216 for a GbE port and from 1280 to 16110 for a 10 GbE port. However, the maximum might be 9000 for a GbE port and 9600 for a 10 GbE port, depending on the hardware type and configuration. Changing the MTU value of the interface allows you to use the Jumbo Frame packet. The value specified here applies to both IPv4 and IPv6 environments.
<p>#1: Do not specify the IP addresses shown below. If you must specify them, contact our Technical Support Center.</p> <ul style="list-style-type: none"> For IPv4: 127.0.0.0 to 127.255.255.255 For IPv6: ::ffff:IPv4-address, ::IPv4-address, ::1/128, ::/0, ::/128, fe80::/10, and ff00::/8 IP addresses that belong to the same network as the IP address set for the private maintenance port You can use the <code>pmctl</code> command to view the IP address set for the private maintenance port. IP addresses that belong to the same network as the IP address set for the heartbeat port You can view the IP address set for the heartbeat port on the Browse Cluster Status page (for <code>Cluster / Node status</code>) in the Cluster Management dialog box. <p>You must specify IP addresses for data port interfaces according to the following rules:</p> <ul style="list-style-type: none"> For physical nodes in a cluster, all IP addresses that are assigned to the same interface must be on the same network segment but be different addresses. The IP addresses that are set for different interfaces in a cluster, must be on different network segments. <p>#2: Interfaces created without specifying a virtual IP address are excluded from the targets of resource group monitoring. Note the following when creating an interface without specifying a virtual IP address:</p> <ul style="list-style-type: none"> The CIFS, NFS, FTP, SFTP, and TFTP services provided by the HDI system cannot be used from an interface for which no virtual IP address is set. If a linkage error occurs in an interface for which no virtual IP address is set, SNMP traps and email notifications, and the error notification for maintenance personnel are not sent. <p>#3: After changing an MTU value, run the <code>ping</code> command from the client to make sure that the client can communicate with the node even when the maximum MTU value is used. If a client cannot communicate with the node although the MTU value is correctly set, the peripheral equipment or the client might have a problem. Check the settings of the peripheral equipment and the client.</p>	

DNS, NIS, LDAP Setup page

You can use the **DNS, NIS, LDAP Setup** page to set the DNS, NIS, and LDAP server information.

**Note:**

- When setting new information for **LDAP setup (for user authentication)** or deleting all the information, be aware of the following:
When performing operations from a physical node:
Before performing operations, stop the resource groups on both nodes and the cluster. After completing the settings, restart the OS on both nodes, and then the resource groups and cluster that you stopped.
- After changing the information for **LDAP setup (for user authentication)**, restart the FTP or SFTP service.
- After setting new information, changing information, or deleting all the information for **NIS setup** or **DNS setup**, restart the OS on both nodes:
- After completing the settings, make sure that each server is correctly connected from the **List of RAS Information** page (for *Server check*) in the **Check for Errors** dialog box.

To open the **DNS, NIS, LDAP Setup** page, click **DNS, NIS, LDAP Setup** on the **System Setup Menu** page (**Setting Type:** *network*) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-171 Information specified in the DNS, NIS, LDAP Setup page

Item	Description
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.
	Default domain name ^{#1} Specify the name of the domain to which the nodes belong. Enter a maximum of 255 characters. You can omit this setting if you are not using domain names.
	Search domain name(s) ^{#1} If there are domains that you want to set as name resolution search targets other than the domain specified in Default domain name , specify the names of the target domains. You can specify a maximum of 5 domain names. The search is performed in the order of the domains in the text boxes.
	Primary DNS server Specify the IP address of the DNS server to be used for normal operation.
	Secondary DNS server Specify the IP address of the DNS server to be used if the primary DNS server fails.
NIS setup ^{#2}	When you want to use the NIS server, specify information about the NIS server. The specified information is set for both nodes in the cluster.

Item	Description	
	When you do not want to use the NIS server, you can omit specification of this item.	
	NIS domain	<p>In the text box, specify the name of the domain that the NIS server belongs to. In addition, select the NIS server you want to use from the options.</p> <p>NIS server specification</p> <p>Select this when you want to use a specific NIS server. In NIS server(s), specify the IP address or server name of the NIS server you want to use (the IP address is recommended).</p> <p>Broadcast specification</p> <p>Select this when you want to use broadcasting. It does not matter which NIS server on the network is used.</p>
LDAP setup (for user authentication)	<p>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.</p> <p>When you do not want to use the LDAP server, you can omit specification of this item.</p> <p>Ask the LDAP server administrator for the information necessary to specify the values.</p>	
	LDAP server(s)	<p>In the text box, specify the IP address or server name of the LDAP server you want to use (the IP address is recommended).</p> <p>In addition, specify the port number of the LDAP server in the Port text box. When this specification is omitted, 389 is set.</p>
	LDAP server root DN	<p>Specify the root identification name of the LDAP server by using a distinguished name, as in the following example:</p> <p><code>dc=hitachi,dc=co,dc=jp</code></p>
	LDAP administrator DN^{#3}	<p>Specify the identification name of the LDAP server administrator by using a distinguished name, as in the following example:</p> <p><code>cn=Administrator,dc=hitachi,dc=co,dc=jp</code></p>
	LDAP administrator password^{#3}	<p>Specify the password of the LDAP server administrator.</p>
<p>Note: The host name can be specified using alphanumeric characters, hyphens (-), and periods (.).</p> <p>#1: The following equation must be satisfied (where n is the number of specified domains, and m is the total number of characters used in all the domain names):</p> $m + (n - 1) \leq 255$ <p>#2: If you specify an invalid value, you might not be able to set network or other information.</p> <p>#3: Make sure that you specify this item when an end user logs in to Hitachi File Services Manager and the security settings for the LDAP server to be used do not allow an anonymous user to obtain a password.</p>		

List of Routings page

You can use the **List of Routings** page to set the routing information.



Note: You can use the `routelist` command to view all the enabled routing information.

To open the **List of Routings** page, click **Routing Setup** on the **System Setup Menu** page (**Setting Type:** `network`) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)). To view specific information, select the corresponding items from the **Protocol version** and **Port** drop-down lists, and then click **Display**.

Table C-172 Information shown in the List of Routings page

Item	Description
Interface	Interface information: Port The port name. VLAN ID The VLAN ID is shown if a VLAN is used. A hyphen (-) is shown if a VLAN is not used.
Target	Routing target: The IP address, host name, or network name of the target is shown. If the default route has been specified, <code>default</code> is shown.
Netmask	For IPv4, the netmask is shown for a network, and a hyphen (-) is shown for a host. If the default route has been specified for the routing destination, <code>0.0.0.0</code> is shown.
Prefix length	For IPv6, the netmask is shown for a network, and a hyphen (-) is shown for a host. If the default route has been specified for the routing destination, <code>0</code> is shown.
Gateway	Gateway through which network data is routed. The IP address or host name of the gateway is shown.
Method of specifying route	Whether a route has been set or routing is denied for the routing target. <code>Allow</code> A route has been set for the routing target. <code>Reject</code> Routing is denied for the routing target.
MSS	Maximum segment size of the TCP connection on the route for IPv4.

Table C-173 Operations that can be performed from the List of Routings page

Button	Description	See
Delete	<p>Deletes the routing information that is set for the selected interface.</p> <p>Notes:</p> <ul style="list-style-type: none"> • If the host name specified for the routing target or gateway cannot be resolved, you might not be able to delete the routing information correctly. If a host name is specified for the routing target or gateway, make sure that the host name can be resolved before you delete routing information. • If routing information is deleted, communications between the clients that are using the routing and the HDI system cannot be performed. • If you delete the routing information of the management port, the database cache information on the management server might become inconsistent with that on the node, or it might become impossible to open dialog boxes from the Settings tab. Log on to the Hitachi File Services Manager from another management console in the same network as the nodes, and make the necessary settings for the routing information. 	N/A
Add	Adds the routing information to the interface.	Add Routing page on page C-201

Add Routing page

You can use the **Add Routing** page to add the routing information to the interface.



Note:

- Each information item set up in this page 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, regardless of protocol versions.
- Do not add multiple instances of routing information that have the same routing target. If this is done, you might not be able to delete the routing information correctly.
- Do not set routing information whose settings (except for the gateway setting) are the same as those of existing routing information. If this is done, you might not be able to delete the routing information correctly.
- The HDI system might be unable to respond to an ICMP redirect request from a gateway (request to change the route to another gateway).

Therefore, the network must be designed so that no ICMP redirect occurs. Note that multiple gateways that connect to one or more external network segments can exist in a network segment connected to an HDI port. In such an environment, set the routing information so that an appropriate gateway is used for each of the external network addresses that the HDI system must communicate with.

To open the **Add Routing** page, click **Add** on the **List of Routings** page in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-174 Information specified in the Add Routing page

Item	Description
Interface	<p>Select the target interface.</p> <p>Port Select the target port from the drop-down list.</p> <p>VLAN ID If you select a port using a VLAN for Port, select the target VLAN ID from the drop-down list. A hyphen (-) is shown if a VLAN is not used.</p>
How to specify target ^{#1}	<p>Select the method to be used to specify the routing target. 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.</p> <p>Network Specify the target by network address.</p> <p>Host Specify the target by host name or IP address.</p> <p>Default route Specify the target by the default route.</p>
Target ^{#2}	<p>Specify the routing target according to the setting How to specify target. This item shows <code>default</code> if you select Default route for How to specify target.</p>
Netmask ^{#1}	<p>For IPv4, specify one of the following according to the setting of How to specify target.</p> <p>When Network is selected: Specify the netmask.</p> <p>When Host is selected: You do not need to specify anything. The system ignores the specification.</p> <p>When Default route is selected: You do not need to specify anything. The system ignores the specification.</p>
Prefix length ^{#1}	<p>For IPv6, specify one of the following according to the setting of How to specify target.</p> <p>When Network is selected: Specify the prefix length.</p>

Item	Description
	When Host is selected: You do not need to specify anything. The system ignores the specification. When Default route is selected: You do not need to specify anything. The system ignores the specification.
Gateway ^{#2}	Enter the IP address or host name of the gateway through which network data is to be routed.
Method of specifying route	Select whether to set a route or deny routing to the routing target from the options. Allow Set a route. Reject Deny routing.
MSS	For IPv4, specify the maximum segment size of the TCP connection on the route, as a number from 64 to 65,536 (units: bytes).
<p>#1:</p> <ul style="list-style-type: none"> • If Network is selected in How to specify target, and 0.0.0.0 is specified in Netmask or 0 is specified in Prefix length, the routing information operates as the default route. • If Network is selected in How to specify target, and 255.255.255.255 is specified in Netmask or 128 is specified in Prefix length, the routing operates the same as when the host is directly specified for the routing target. <p>#2: For notes about IP addresses to be specified, see Table C-170 Information specified in the Add Interface page on page C-196.</p>	

Time Setup page

You can use the **Time Setup** page to set the NTP server information and time zone.



Note:

- For details about NTP server environment settings, see the *Installation and Configuration Guide*.
- If you are not using an NTP server and you want to set the same time for clients and nodes, you can use the `timeset` command to set the time in the nodes.
- After changing the NTP server settings, restart the OS on both nodes that make up the cluster. In addition, after the OSs are restarted, from the **List of RAS Information** page (for `List of messages`) in the **Check for Errors** dialog box, check that the message KAQM05154-I is output as a system message to make sure that the time has been correctly synchronized with the NTP server.

- After changing the time zone, restart the OS on both nodes that make up the cluster.

To open the **Time Setup** page, click **Time Setup** on the **System Setup Menu** page (**Setting Type:** *network*) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-175 Information specified in the Time Setup page

Item	Description
NTP server(s)	Specify one or two IP addresses or host names when you use an NTP server. The same value is set within a cluster. We recommend that you specify IP addresses or host names for two different NTP servers as a countermeasure against a failure. Do not specify two host names for the same NTP server.
Time zone	Select the time zone. The same value is set within a cluster. The time zone is shown in directory structure. Select a time zone from the list box, and then click Select . If lower levels are included in the selected time zone, it is expanded to the lower time zones when you click Select . To go back to the upper levels, select .. , and then click Select . For example, to set the time zone to Japan, select Asia , and then Tokyo , or select Japan . To set the time zone to Los Angeles, select America , and then Los_Angeles . Hitachi Data Systems recommends 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 shown with + for zones west of the Greenwich meridian and - for zones east of it.

Syslog Setup page

In the **Syslog Setup** page, the system administrator can set up the system log setup file (*syslog.conf*). This operation must be performed for each node in the cluster.

To open the **Syslog Setup** page, click **Syslog Setup** on the **System Setup Menu** page (**Setting Type:** *system*) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-176 Information shown in the Syslog Setup page

Item	Description
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 HDI system.

Table C-177 Operations that can be performed from the Syslog Setup page

Button	Description	See
Edit	Edits the information for the selected item. You can edit the item whose Output destination is in the format <i>@host-name</i> .	Edit Syslog Setup page on page C-205
Delete	Deletes the information for the selected item. You can delete the item whose Output destination is in the format <i>@host-name</i> .	N/A
Add	Adds a system log transfer destination.	Add Syslog Setup page on page C-205
Note: N/A = Not applicable.		

Edit Syslog Setup page

You can use the **Edit Syslog Setup** page to edit the information for the selected item. You can edit the item whose **Output destination** is in the format *@host-name*.

To open the **Edit Syslog Setup** page, from the **Syslog Setup** page in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)), select the item whose **Output destination** is in the format *@host-name*, and then click **Edit**.

For details about the information to be specified in the **Edit Syslog Setup** page, see [Table C-178 Information specified in the Add Syslog Setup page on page C-205](#).

Add Syslog Setup page

You can use the **Add Syslog Setup** page to add a system log transfer destination.

To open the **Add Syslog Setup** page, click **Add** on the **Syslog Setup** page in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-178 Information specified in the Add Syslog Setup page

Item	Description
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 <i>@host-name</i> .

Log File Capacity Setup page

You can use the **Log File Capacity Setup** page to change the number of log files that can be saved on a physical node and the file capacity. This operation must be performed for each node in the cluster.



Note: Log files that have already been output are not automatically deleted even if you reduce the number of log files to be saved. If necessary, from the **List of RAS Information** page, delete the old log files.

To open the **Log File Capacity Setup** page, click **Log File Capacity Setup** on the **System Setup Menu** page (**Setting Type:** *system*) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-179 Information shown in the Log File Capacity Setup page

Item	Description
File type	Log file type and path
Capacity (MB)	The maximum size of the log file
Number of files	Number of log files to be kept
Explanation	Description of the log file

Table C-180 Operations that can be performed from the Log File Capacity Setup page

Button	Description	See
Edit	Changes the number of log files that can be saved and the file capacity for the selected log file.	Edit File Capacity page on page C-208

Table C-181 Types of log files for which the number of log files to be kept and the size of each log file can be set

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/lvm2.log	LVM log
/var/log/lvm_display.log	LVM log
/var/log/cifs/log.smbd	CIFS log

Log file type	Description
/var/log/cifs/log.nmbd	CIFS log
/var/log/cifs/log.winbindd	CIFS log
/enas/data/em_alertfile	System messages
/var/log/failsafe/crsd_ <i>node-host-name</i>	Cluster log
/var/log/failsafe/cmsd_ <i>node-host-name</i>	Cluster log
/var/log/failsafe/failsafe_ <i>node-host-name</i>	Cluster log
/var/log/failsafe/gcd_ <i>node-host-name</i>	Cluster log
/var/log/failsafe/ifd_ <i>node-host-name</i>	Cluster log
/var/log/failsafe/srmd_ <i>node-host-name</i>	Cluster log
/var/log/failsafe/script_ <i>node-host-name</i>	Cluster log
/var/log/failsafe/cli_ <i>node-host-name</i>	Cluster log
/var/log/failsafe/cmond_ <i>node-host-name</i>	Cluster log
/var/log/failsafe/cdbd_ <i>node-host-name</i>	Cluster log
/enas/log/ebr_alertfile	Backup Restore log
/enas/log/backuprestore.trace	Backup Restore trace log
/enas/log/ndmpserver.log	NDMP server log
/enas/log/ndmpprotocol.trace	NDMP server protocol trace log
/enas/log/management.log	File Services Manager log
/enas/log/nsi_agent.log	File Services Manager log
/enas/log/management.trace	File Services Manager trace log
/enas/log/nsi_agent.trace	File Services Manager trace log
/enas/log/antivirus.log	Anti-Virus Enabler log
/enas/log/antiviruslib.trace	Anti-Virus Enabler library trace
/enas/log/antivirusmng.trace	Anti-Virus Enabler management trace log
/var/log/proftpd/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
/var/log/cifs/log.CIFSaccess	CIFS access log
/enas/log/hsmarc.log	HSM Core log
/enas/log/hsmarc.trace	HSM Core trace log

Edit File Capacity page

Changes the number of log files that can be saved and the file capacity for the selected log file.

To open the **Edit File Capacity** page, click **Edit** on the **Log File Capacity Setup** page in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-182 Information specified in the Edit File Capacity page

Item	Description
Capacity	Select a value from 1 to 6 for the maximum size of the log file (units: MB). If the log file exceeds the maximum size, the file will be switched to the next generation.
Number of files	Select a value from 1 to 14 for 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 will be deleted starting from the oldest.

Core File Auto. Deletion Setup page

In the **Core File Auto. Deletion Setup** page, the system administrator 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 ensures that there will be enough space on the OS disk for the log and core files. This operation must be performed for each node in the cluster.

To open the **Core File Auto. Deletion Setup** page, click **Core File Auto. Deletion Setup** on the **System Setup Menu** page (**Setting Type:** *system*) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-183 Information specified in the Core File Auto. Deletion Setup page

Item	Description
Period to save	Specify the core file storage period, as a number from 0 to 99 (units: days). When the storage period has elapsed, core files are deleted at the time specified with Automatic deletion time .
Automatic deletion time	Specify the time 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.

Item	Description
	<p>Click Add to add a time to the list box. You can set the checking and deletion time only by selecting it in the list box.</p> <p>To delete a time from the list box, select it and click Delete.</p> <p>You can specify a maximum of 48 automatic deletion times.</p>

Edit System File page

In the **Edit System File** page, the system administrator can directly edit system files of the HDI system.



Note:

- Host names can be specified using alphanumeric characters, hyphens (-), and periods (.).
- If necessary, configure the settings for each node so that the settings will be identical within the cluster.
- If you have edited the `/etc/hosts` file or the `/etc/cifs/lmhosts` file, you need to restart the NFS service or the CIFS service

To open the **Edit System File** page, click **Edit System File** on the **System Setup Menu** page (**Setting Type:** `system`) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)). Select a system file to be edited from the **File type** drop-down list, and then click **Display** to directly edit the system file in **Settings**.

Table C-184 Selectable system files in the Edit System File page

Item	Description
/etc/hosts	<p>Associates host names with IP addresses when host information is managed by the HDI system. Do not change or delete the values that were set in the <code>/etc/hosts</code> file when operations started.</p> <p>Note that if the values are modified on a physical node, the modified settings will be applied to both nodes in the cluster.</p> <p>If NFS file locking is used from the public destination host for an NFS share, add the following information:</p> <ul style="list-style-type: none"> • Virtual IP address and host name of the resource group to which the mounted NFS share belongs. • IP address and host name of the NFS client host that uses NFS file locks. <p>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:</p> <ul style="list-style-type: none"> • Host access restrictions in the CIFS Service Management page (Setting Type: <code>Security</code>) of the Access Protocol Configuration dialog box

Item	Description
	<ul style="list-style-type: none"> • Host/network based access restriction in the Create and Share File System dialog box • Host/network based access restriction in the Add Share dialog box • Host/network based access restriction in the Edit Share dialog box • <code>-s</code> option of the <code>cifscreate</code> command • <code>-s</code> option of the <code>cifsedit</code> command
<p>/etc/cifs/lmhosts</p>	<p>For NT domain authentication or Active Directory authentication, this file associates NT domain controllers' IP addresses with domain names for the NT domains that have trust relationships. Append the following line to this file:</p> <p><i>IP-address NetBIOS-domain-name-for-the-domain-controller-that-has-the-trust-relationship</i></p> <p>Note that if the values are modified on a physical node, the modified settings will be applied to both nodes in the cluster.</p>
<p>/etc/snmp/snmpd.conf^{#1}</p>	<p>SNMP setup file. Specify the settings for each node in the cluster.</p> <p>To enable SNMP trap notification for SNMPv2, append the following line to this file:</p> <pre>trap2sink SNMP-manager-host-name-or-IP-address [community-name [port-number]]^{#2}</pre> <p>Example: <code>trap2sink 10.213.76.194 stdDefComm1</code></p> <p>Specify a community name using no more than 32 characters. You can use the following ASCII characters: alphanumeric characters, hash mark (#), percent sign (%), plus sign (+), hyphen (-), period (.), forward slash (/), colon (:), equal sign (=), at mark (@), and underscore (_).</p> <p>A hash mark (#) cannot be used for the first character of a community name.</p> <p>In addition, if you use SNMPv2, do not directly edit <code>com2sec</code>, <code>group</code>, <code>view</code>, or <code>access</code> in Access Control. Instead, set them in the Add SNMP page or the Edit SNMP page. If you need to edit them, contact the Hitachi Data Systems Technical Support Center.</p> <p>To use SNMPv3, append the following two lines as SNMP management user information:</p> <pre>rouser user-name [security-level [OID]]^{#3} createUser user-name [authentication-type authentication-password [encryption-type encryption-password]]</pre> <p>Example:</p> <pre>rouser user1 priv createUser user1 MD5 mypassphrase DES mypassword</pre> <p>For details about the items to be specified when SNMPv3 is used, see Table 10-1 Information specified in the snmpd.conf file when SNMPv3 is used on page 10-5.</p> <p>To enable SNMP trap notification for SNMPv3, append the following line to this file:</p> <pre>trapsess -v3 -u user-name [option] SNMP-manager-host-name-or-IP-address[:port-number]^{#2#4}</pre>

Item	Description
	<p>Example: <code>trapsess -v3 -u user1 -l authPriv -a MD5 -A mypassphrase -x DES -X mypassword 10.213.76.194</code></p> <p>For details about the items to be specified when SNMPv3 is used, see Table 10-1 Information specified in the snmpd.conf file when SNMPv3 is used on page 10-5.</p>
	<p>To limit the amount of quota and subtree quota information provided, for up to a certain number of users and groups that are registered for a file system, append the following line to the end of the file. You can specify the maximum value in the range from 0 to 2,147,483,147. Specifying 0 will not limit the amount of information provided.</p> <pre>std_quota_max maximum-number std_stquota_max maximum-number</pre>
	<p>To prevent the acquisition of MIB objects from being interrupted, you can specify settings so that the SNMP agent does not restart during the following processing:</p> <ul style="list-style-type: none"> • Failovers or failbacks • Mounting of file systems <p>When specifying settings to prevent the SNMP agent from restarting, append the line below to the file. Note that the restart of the SNMP agent is not suppressed when <code>snmpd.conf</code> is updated, or when a restart operation scheduled daily at 00:01 is executed.</p> <pre>reboot_on_resource_event off</pre> <p>To obtain the most recent information about the MIB object in <code>dskEntry</code> when you have specified settings to prevent the SNMP agent from restarting, append the following line to the file:</p> <pre>Fixed-order_path on disk path-of-the-file-system-from-which-information-is-to-be-obtained unused-capacity</pre> <p>In this setting, the MIB object is applied to the file systems that are failed over to another node or unmounted, and the index is fixed. At this time, a null string is set to the device name, and "0" is set to the MIB object that indicates the capacity.</p> <p>The following is an example of obtaining the most recent information about <code>fs01</code> and <code>fs02</code> file systems by the MIB object in <code>dskEntry</code> by suppressing a restart:</p> <pre>reboot_on_resource_event off Fixed-order_path on disk /mnt/fs01 10% disk /mnt/fs02 10%</pre>
	<p>To set the file system whose status is obtained and to set the unused capacity level of the file system from which an error is sent, append the following line to the end of the file.</p> <pre>disk file-system-path unused-capacity</pre> <p>With this setting, SNMP traps are not reported. You need to use the <code>fsctl</code> command to specify that SNMP traps are to be reported whenever the usage amount of the file system exceeds a threshold.</p> <p>Example of specifying the information of the file system <code>fs01</code> so that the status is obtained and an error is sent when the unused capacity goes down to 10%: <code>disk /mnt/fs01 10%</code></p>

Item	Description
	<p>For information about file systems, quota, and subtree quota, to send information for specific objects, append the lines for each category of information as follows:</p> <p>Information only for specific file systems: <code>fspath file-system-path</code></p> <p>Quota information only for specific file systems: <code>qtpath file-system-path</code></p> <p>Subtree quota information only for specific directories: <code>stquota directory-path</code></p> <p>Example of sending information about the file systems <code>fs01</code> and <code>fs02</code>, and subtree quota information for the directories <code>dir1</code> and <code>dir2</code>:</p> <pre>fspath /mnt/fs01 fspath /mnt/fs02 stquota /mnt/fs01/dir1 stquota /mnt/fs01/dir2</pre>
<p>/enas/conf/ email_alert.conf</p>	<p>The configuration file for email error notifications. Specify the settings for each node in the cluster.</p> <p>Specify values for the entries in the configuration file as follows:</p> <pre>serveraddress=mail-server-fully-qualified-domain-name-or-IPv4-address[:port-number]</pre> <p>To use IPv6, specify a fully qualified domain name.</p> <p>To use a port number other than 25, you must specify the port number.</p> <pre>mailtoaddress=email-recipient-address</pre> <p>Up to four addresses can be specified. When specifying multiple addresses, separate the addresses with commas (,).</p> <pre>mailfromaddress=email-sender-address replytoaddress=reply-destination-address-(optional) messagelevel=message-level-(optional)</pre> <p>Specify 1 to send email notifications about errors and higher-level (fatal error) problems. Specify 2 to send email notifications about warnings and higher-level (error and fatal error) problems. 2 is the default.</p> <p>Specify email addresses in the format <code>user-name@domain-name</code>.</p> <p>If a hash mark (#) is placed at the beginning of a line, the line is treated as a comment. Use hash marks to disable definitions.</p>
<p>#1: If you configure traps, make sure that the <code>cold start</code> trap is issued after the file is updated. If the trap is not issued, check the contents of the file. If you omit the community name for <code>trap2sink</code>, <code>public</code> is set for the community name of the <code>cold start</code> and <code>nsNotifyShutdown</code> traps that are issued when <code>snmpd</code> is started and stopped.</p> <p>Note that <code>source of com2sec</code> (for IPv4) and <code>com2sec6</code> (for IPv6) in <code>Access Control</code> is set as <code>default</code>. This means that MIBs can be accessed from any host in the network. If you want to limit access, specify the name of the SNMP manager server that accesses MIBs. If you do not access MIBs, specify the local host. If you have deleted the <code>com2sec6</code> setting or commented out this setting by adding the hash symbol (#) to the beginning of the line, the initial <code>com2sec6</code> setting will be added when an update installation is performed. Revise the setting if necessary. Use the List of SNMPs page to make settings on <code>com2sec</code>. To add a local host (<code>localhost</code>), remove all the entries and then make sure that the local host is displayed at the top of the List of SNMPs page.</p>	

Item	Description
	<p>#2: If you use IPv6, specify the host name or IP address and the port number of the SNMP manager as follows (The port number is required.):</p> <pre>udp6: host-name: port-number</pre> <pre>udp6: [IP-address]: port-number</pre> <p>If you use IPv6 and want to use a specific IP address as the trap notification source, append either of the following lines:</p> <pre>sending_srcaddress SNMP-manager-host-name [notification-source-IP-address]</pre> <pre>sending_srcaddress [SNMP-manager-IP-address] [notification-source-IP-address]</pre> <p>#3: <code>rwuser</code> can be specified instead of <code>router</code>.</p> <p>#4: Do not specify options that issue SNMPv2 traps usable by <code>net-snmp</code>.</p>

Performance Tuning page

In the **Performance Tuning** page, the system administrator can tune performance of the system. For normal operation, however, there is no need to make any changes. If you wish to tune the system performance, contact Hitachi Data Systems Technical Support Center. This operation must be performed for each node in the cluster.

To open the **Performance Tuning** page, click **Performance Tuning** on the **System Setup Menu** page (**Setting Type:** `system`) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-185 Information specified in the Performance Tuning page

Item	Description
Buffer flush daemon control	<p>Specify the following control parameters for the buffer flush daemon:</p> <p>Percentage of buffer cache dirty to activate bdflush</p> <p>Specify the level of dirty cache at which to start flushing the buffer cache, using a number from 0 to 100 (units: %).</p> <p>Jiffies delay between kupdate flushes</p> <p>Specify the interval between buffer cache flushes (units: 10 ms).</p> <p>Set a number from 1 to 1,000,000. Hitachi Data Systems recommends that you specify a number that is no more than 60,000. Even if you specify a number greater than 60,000, normal operation is not affected. However, failover functionality might not work correctly when restarting the system after the system ended abnormally.</p> <p>Time for normal buffer to age before we flush it</p> <p>Specify the time to wait before starting to flush the buffer, as a number from 100 to 600,000 (units: 10 ms).</p>

Item	Description
	<p>Percentage of buffer cache dirty to activate bdflush synchronously</p> <p>Specify the level of dirty cache at which to start an urgent buffer flush process, as a number from 0 to 100 (units: %).</p> <p>This parameter activates the flush process even if the dirty cache percentage is reached before the age time elapses.</p>
Minimum count of i-nodes resident in the cache	Specify the minimum number of inodes resident on the buffer cache, from 0 to 50,000,000.
Time for buffer to age before we flush it	Specify the time to wait before starting to flush the buffer cache for meta data, as a number from 100 to 720,000 (units: 10 ms).
Interval between runs of the delayed write flush daemon	Specify the interval between flushes of the buffer cache for write-delayed meta data, as a number from 50 to 3,000 (units: 10 ms).

List of SNMPs page

In the **List of SNMPs** page, when SNMPv2 is used, the system administrator can specify a community name that is used by the SNMP manager to access the MIB values of the SNMP agent and the MIB objects that can be obtained.



Note:

- When you use the SNMP notification, Hitachi Data Systems recommends that you set the clock of the SNMP manager to that of the OS. If these clocks are different from each other, the SNMP manager clock is used to determine the SNMP trap reception time.
- To use the SNMP trap notification for SNMPv2, to use SNMPv3, or to use SNMP in an IPv6 environment, you must edit the `snmpd.conf` file in the **Edit System File** page (see [Edit System File page on page C-209](#)).

To open the **List of SNMPs** page, click **SNMP Setup** on the **System Setup Menu** page (**Setting Type:** `system`) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-186 Information shown in the List of SNMPs page

Item	Description
Source	Server name or IP address of the SNMP manager
Number of MIB objects	Number of MIB objects

Table C-187 Operations that can be performed from the List of SNMPs page

Button	Description	See
Edit	Edits the selected SNMP information.	Edit SNMP page on page C-215
Delete	Deletes the selected SNMP information.	N/A
Add	Adds the SNMP information.	Add SNMP page on page C-215
Note: N/A = Not applicable.		
Note: These operations must be performed for each node in the cluster.		

Edit SNMP page

You can use the **Edit SNMP** page to edit the selected SNMP information.

To open the **Edit SNMP** page, click **Edit** on the **List of SNMPs** page in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

For details about the information to be specified in the **Edit SNMP** page, see [Table C-188 Information specified in the Add SNMP page on page C-215](#).

Add SNMP page

You can use the **Add SNMP** page to add the SNMP information.

To open the **Add SNMP** page, click **Add** on the **List of SNMPs** page in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

Table C-188 Information specified in the Add SNMP page

Item	Description
Source	Specify the server name or IP address of the SNMP manager. The specified source SNMP manager can access and obtain information from the MIB object.
Community	Specify a community name, using no more than 32 characters. The SNMP manager uses the community name to access the MIB value of an SNMP agent. You can specify ASCII alphanumeric characters, exclamation mark (!), hash mark (#), dollar sign (\$), percent sign (%), ampersand (&), single quotation mark ('), 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 square bracket ([), backslash (\), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (), right curly bracket (}), and tilde (~). A hash mark (#) cannot be used for the first character of a community name.

Item	Description
	<p>If you use a backslash (\) or single quotation mark ('), insert a backslash as an escape character before the character that you want to use.</p> <p>The characters that can be used when specifying this community name are different from those that can be used when specifying the community name to be used when sending SNMPv2 traps. If you want to use the same community name as the one used when sending SNMPv2 traps, specify the community name that you specified in Table C-184 Selectable system files in the Edit System File page on page C-209.</p>
MIB objects	<p>Specify the MIB object name, mask, and the specification method.</p> <p>List of selectable MIB objects (MIB object name, Mask, How to specify)</p> <p>For each MIB object to be added to the SNMP setup file, set the object name, mask, and the specification method.</p> <p>Text box</p> <p>The name and mask for the MIB object selected in List of selectable MIB objects (MIB object name, Mask, How to specify) are shown.</p> <p>Drop-down list</p> <p>Select whether to include or exclude subtrees of the MIB object shown in the text box. When you want to include subtrees of the MIB object name, select Include. Otherwise, select Do not include.</p> <p>Click Select to add the MIB object to Selected MIB objects. Only the MIB objects shown in Selected MIB objects can be set as the SNMP information. When you want to delete a MIB object from Selected MIB objects, select the MIB object and click Delete.</p>

For a listing of MIB objects, see [Appendix G, MIB objects on page G-1](#).

Select User Interface page

In the **Select User Interface** page, the system administrator can select the user interface mode used for setting quotas.

The selected mode applies to both nodes in the cluster. All system administrators who operate the target nodes will operate in the selected mode.

To open the **Select User Interface** page, click **Select User Interface** on the **System Setup Menu** page (**Setting Type:** `system`) in the **Network & System Configuration** dialog box ([Network & System Configuration dialog box on page C-178](#)).

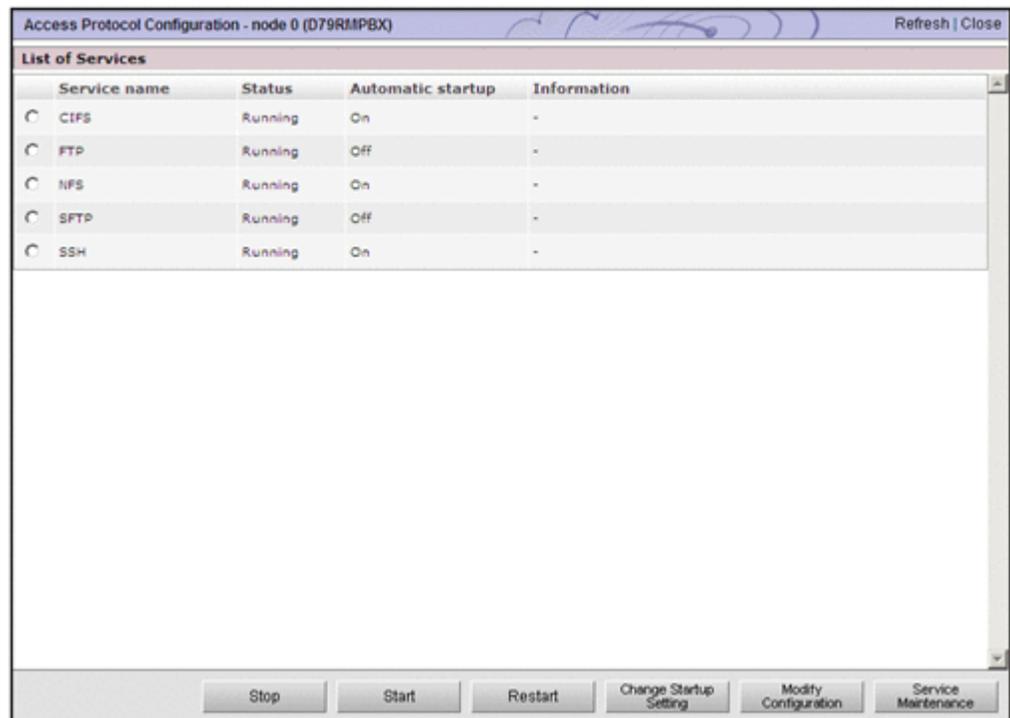
Table C-189 Information specified in the Select User Interface page

Item	Description
GUI operation mode	Select this item to operate the HDI system in GUI operation mode. In this mode, you can use all dialog boxes and commands.
Command operation mode	Select this item to operate the HDI system in command operation mode. The following operations must be performed by using commands: <ul style="list-style-type: none"> Setting quotas for users or groups for each file system Viewing quotas set for users or groups for each file system

Access Protocol Configuration dialog box

In the **Access Protocol Configuration** dialog box, the system administrator sets security and environments for access protocols including NFS and CIFS for each service provided by HDI. The services must be managed for each node in the cluster.

To open the **Access Protocol Configuration** dialog box, from the **Advanced** subtab of the **Settings** tab in the *physical-node* window ([physical-node window on page C-91](#)), click **Access Protocol Configuration**. When **Access Protocol Configuration** dialog appears, the **List of Services** page is shown.



List of Services page

You can use the **List of Services** page to view the status of the services running on a physical node.

The **List of Services** page is shown when the **Access Protocol Configuration** dialog appears.

Table C-190 Service information shown in the List of Services page

Item	Description
Service name	The service name.
Status	<p>Operating status of the service is one of the following:</p> <p>Running The service is running normally.</p> <p>Down The service is running in an incomplete state.</p> <p>Failover A failover has occurred for the resource group.</p> <p>Offline The resource group is offline.</p> <p>Stopped The service has stopped.</p>
Automatic startup	<p>Shows whether each service on a physical node automatically starts when the OS starts or restarts.</p> <p>On The service automatically starts.</p> <p>Off The service does not automatically start.</p>
Information	<p>This item is shown when the service needs to be restarted or started.</p> <p>The configuration has been modified. Make sure the file system has been unmounted from the NFS client, and then restart the service. Rebooting the OS will not apply the changes.</p> <p>This information is shown if the service was not restarted after the configuration definition of the NFS service was modified. Make sure that the file system has been unmounted from the NFS client, and then restart the service. Rebooting the OS will not apply the changes.</p> <p>The configuration has been modified. Make sure the file system has been unmounted from the NFS client, and then start the service. Rebooting the OS will not apply the changes.</p> <p>This information is shown if the service has remained stopped since the configuration definition of the NFS service was modified. Make sure that the file system has been unmounted from the NFS client, and then start the service. Rebooting the OS will not apply the changes.</p>

Item	Description
	<p>The configuration has been modified. Restart the service. Rebooting the OS will not apply the changes.</p> <p>This information is shown if the service was not restarted after the configuration definition of the NFS service, CIFS service, FTP, or SFTP service, or a setting of the LDAP server was modified. Restart the service. Rebooting the OS will not apply the changes.</p> <p>The configuration has been modified. Start the service. Rebooting the OS will not apply the changes.</p> <p>This information is shown if the service has remained stopped since the configuration definition of the NFS service, CIFS service, FTP, or SFTP service, or a setting of the LDAP server was modified. Start the service. Rebooting the OS will not apply the changes.</p> <p>The service is incomplete. Restart the service.</p> <p>This message appears if the service is running in an incomplete state. If this message appears, restart the service because a problem might have occurred. If the message continues to be shown after the restart, collect error information and contact maintenance personnel. For details about how to collect the error information, see the <i>Cluster Troubleshooting Guide</i>.</p>

Table C-191 Operations that can be performed from the List of Services page

Button	Description	See
Stop	<p>Stops the services on physical nodes.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Contact clients before stopping the services. • An error (<code>srmd executable error</code>) might occur when a resource group is started or a failover occurs while the NFS service is stopped. • When the CIFS service stops during degenerated operation, only the CIFS service running on the target node before a failover occurs stops. 	N/A
Start	<p>Starts the services on physical nodes, other than the SSH service.</p> <p>Notes:</p> <ul style="list-style-type: none"> • When the CIFS service starts during degenerated operation, only the CIFS service running on the target node before a failover occurs starts. • If you start the NFS service in an environment where the CIFS service and the NFS service share a directory, accessing a file system from the CIFS client might fail. If 	N/A

Button	Description	See
	this happens, wait a while, and then try to access the file system again.	
Restart	Restarts the services on physical nodes. Notes: <ul style="list-style-type: none"> • Contact clients before stopping the services. • After modifying the configuration definitions for the NFS, CIFS, FTP, or SFTP services, the system administrator must restart these services to apply the changes. For details about the operations that require services to be restarted, see The description of the operations that require services to be restarted on page C-221. • When the CIFS service restarts during degenerated operation, only the CIFS service running on the target node before a failover occurs restarts. • If you start the NFS service in an environment where the CIFS service and the NFS service share a directory, accessing a file system from the CIFS client might fail. If this happens, wait a while, and then try to access the file system again. 	N/A
Change Startup Setting	Specifies whether to automatically starts the services on physical nodes when physical nodes start or restart. For the current settings, verify Automatic startup .	N/A
Modify Configuration	Changes the configuration definitions of the selected service.	For CIFS: CIFS Service Management page on page C-222 For FTP: FTP Service Management page on page C-242 For NFS: NFS Service Management page on page C-248 For SFTP: SFTP Service Management page on page C-251 For SSH:

Button	Description	See
		Public Key List page on page C-256
Service Maintenance	Maintains the CIFS service environment. Services other than CIFS cannot be selected.	CIFS Service Maintenance page on page C-258
Note: N/A = Not applicable.		
Note: These operations must be performed for each node in the cluster.		

The description of the operations that require services to be restarted

After modifying the configuration definitions for the services, the services must be restarted. In addition, the following operations require services to be restarted.

If the following operations are performed, the NFS service must be restarted.

- When both the Active Directory domain controller and the KDC server are used as one server, if a name that is different from the domain name that belongs to the KDC server used by the NFS service or from the name of the KDC server is specified for the **Domain name** or **DC server name(s)** in the **Active Directory Authentication** page of the **Access Protocol Configuration** dialog box
- When editing the `/etc/hosts` file or the `/etc/cifs/lmhosts` file on the **Edit System File** page of the **Network & System Configuration** dialog box
- When specifying actions to respond to the delay time of the network environment by using the `nfsoptset` command
- When changing the port number allocation method for the NFS service by using the `nfssvset` command

If the following operations are performed, the CIFS service must be restarted.

- When using a command to modify the CIFS share settings while the CIFS service configuration definition settings do not allow the CIFS share settings to be automatically reloaded
Restart the CIFS service on the node where the command was executed.
- If the real-time scanning is enabled or disabled
After you enable or disable the real-time scanning, restart the CIFS service.
- When modifying the settings for the cache size of the scanning result on the Scan Conditions page of the Virus Scan Server Configuration dialog box while real-time scanning is enabled
Disable real-time scanning, re-enable it, and then restart the CIFS service.

- When editing the `/etc/hosts` file or the `/etc/cifs/lmhosts` file on the **Edit System File** page of the **Network & System Configuration** dialog box
The modified settings will be applied 11 minutes after the file is edited. If you want the new settings to be applied immediately, restart the CIFS service.
- When both the Active Directory domain controller and the KDC server are used as one server, if a name that is different from the Active Directory domain name used by the CIFS service or from the name of the domain controller is specified for the **Domain name** or **KDC server name(s)** in the **NFS Service Management** page of the **Access Protocol Configuration** dialog box

If the following operations are performed, the FTP or SFTP service must be restarted.

- If the FTP or SFTP service settings allow users authenticated with Active Directory to log on, and the authentication type is changed from Active Directory to another type or from another type to Active Directory.
- When modifying the settings for the **LDAP setup (for user authentication)** on the **DNS, NIS, LDAP Setup** page of the **Network & System Configuration** dialog box

CIFS Service Management page

In the **CIFS Service Management** page, the default settings for CIFS share and the settings for user mapping, in addition to CIFS service configuration definitions, can be configured.



Note:

- The **CIFS Service Management** page always shows 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 page will show the configuration information that is not applied to the service.
- 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** page click **Restart**.
- Even if the OS is restarted after the configuration definitions of the CIFS service are modified, the modified configuration definitions are not applied. Restart the service.
- When user mapping uses LDAP, change the configuration definitions of the CIFS service, and then in the **List of RAS Information** page (for `Server check`) of the **Check for Errors** dialog box, check the connection status between the LDAP server and the nodes.
- The system administrator must modify the service configuration definitions of each node in the same way to avoid inconsistency among nodes in a cluster.

- If the system administrator modifies 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 might not finish normally. The system administrator must notify users before modifying the configuration definitions.

To open the **CIFS Service Management** page, in the **List of Services** page of the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)), select **CIFS**, and then click **Modify Configuration**.

You can select an entry from **Setting Type**, and then click **Display** to view the window for the setting.

Table C-192 Targets that can be selected from the Setting Type drop-down list on the CIFS Service Management page

Item	Description	See
Basic	Specify basic settings.	CIFS Service Management page (Setting Type: Basic) on page C-223
User mapping	Specify user mapping settings.	CIFS Service Management page (Setting Type: User mapping) on page C-225
Security	Specify security settings.	CIFS Service Management page (Setting Type: Security) on page C-231
Performance	Specify performance settings.	CIFS Service Management page (Setting Type: Performance) on page C-235
Administration	Specify administrator settings.	CIFS Service Management page (Setting Type: Administration) on page C-238

CIFS Service Management page (Setting Type: Basic)

You can use the **CIFS Service Management** page (**Setting Type: Basic**) to specify basic settings for the CIFS service.

To open the **CIFS Service Management** page (**Setting Type: Basic**), select **Basic** from **Setting Type**, and then click **Display** in the **CIFS Service Management** page in the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

Table C-193 Operations performed in the CIFS Service Management page (Setting Type: Basic)

Item	Description	See
Change Authentication Mode	Sets the authentication mode used in the CIFS service.	Select Authentication Mode page on page C-240

Table C-194 Information shown in CIFS service setup in the CIFS Service Management page (Setting Type: Basic)

Item	Description
Authentication mode	<p>The specified authentication mode and the settings for user authentication used when a user accesses a CIFS share from a CIFS client.</p> <p>For details about the settings of the authentication mode, see Select Authentication Mode page on page C-240.</p>

Table C-195 Information specified in the CIFS Service Management page (Setting Type: Basic)

Item	Description
SMB protocol	<p>Specify the SMB protocol to be used for accessing from the CIFS client.</p> <p>SMB 1.0 Select this option if you use SMB 1.0.</p> <p>SMB 2.0 Select this option if you use SMB 2.0. SMB 1.0 can also be used.</p> <p>SMB 2.1 Select this option if you use SMB 2.1. SMB 1.0 and SMB 2.0 can also be used.</p> <p>SMB 3.0 Select this option if you use SMB 3.0. SMB 1.0, SMB 2.0, and SMB 2.1 can also be used.</p> <p>If you modify the setting from SMB 3.0, when you have set the CIFS service to encrypt the communication with the CIFS client, the client might not access the share. Review the encryption settings on the CIFS Service Management page (Setting Type: Security) and in the Edit Share dialog box.</p> <p>If you change this setting when real-time scanning by using Trend Micro Incorporated antivirus software is enabled, you need to restart the OS on the scanning server.</p>
Server comment	<p>Enter a comment for the server name that appears on the CIFS client, using no more than 256 characters.</p> <p>You can use any alphanumeric character, exclamation mark (!), hash mark (#), dollar sign (\$), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), forward slash (/), colon (:), left angle bracket (<), right angle bracket (>), question mark (?), at mark (@), left square bracket ([), backslash (\), right square bracket (]), carets (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (), right curly bracket (}), and tilde (~).</p>

Item	Description
	<p>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. In addition, you can specify multi-byte characters.</p> <p>This item is optional.</p>
<p>Volume Shadow Copy Service</p>	<p>Displays whether to use Volume Shadow Copy Service to make past versions of files that have been migrated to an HCP system available to CIFS clients.</p> <p>Use</p> <p>Select this to use Volume Shadow Copy Service.</p> <p>Do not use</p> <p>Select this to not use Volume Shadow Copy Service.</p>

CIFS Service Management page (Setting Type: User mapping)

You can use User mapping setup to configure the user mapping settings when the authentication mode assigned to the CIFS service is either NT domain authentication or Active Directory authentication.

Select whether to use user mapping from the options, and specify information as required.

- *When user mapping uses RIDs*
- *When user mapping uses LDAP*
- *When user mapping uses the Active Directory schema*
- *When user mapping is not used*



Note:

- To change the user mapping method that you use, you need to re-create the file systems after you migrate the data by using the Windows backup function.
- 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.
- When 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 information is 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 on the HDI system, the NIS server, or the LDAP server for user authentication.
- Even if a user registered on the domain controller is registered with the same name as for the HDI system, the NIS server, or the LDAP server for user authentication, the user ID and group ID assigned by user mapping of the RID method will be 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, Hitachi Data Systems recommends that you do not use user IDs and group IDs beyond the range set by user mapping for the HDI system, the NIS server, and the LDAP server for user authentication.
- You can use commands to view information about users and groups mapped by the RID method.

Note the following when user mapping uses LDAP:

- 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.
- Make sure that the user IDs and group IDs that you register in the LDAP server do not duplicate with the user IDs and group IDs registered on the HDI system, the NIS server, or the LDAP server for user authentication. When you use automatic ID allocation, make sure that the ID range that you specify does not include a user ID or group ID registered on the HDI system, the NIS server, or the LDAP server for user authentication.
- Even if a user registered on the domain controller is registered with the same name for the HDI system, the NIS server, or the LDAP server for user authentication, the user ID and group ID assigned by user mapping of the LDAP method will be used when the user accesses a CIFS share.
- When you use automatic ID allocation, considering the possibility that the range of user IDs and group IDs will be extended in the future, Hitachi Data Systems recommends that you do not use user IDs and group IDs beyond the range set by user mapping for the HDI system, the NIS server, and the LDAP server for user authentication.

Note the following when user mapping uses the Active Directory schema:

- Make sure that the user IDs and group IDs that you register in the domain controller do not duplicate with the user IDs and group IDs registered on the HDI system, the NIS server, or the LDAP server for user authentication.

To open the **CIFS Service Management** page (**Setting Type:** *User mapping*), select **User mapping** from **Setting Type**, and then click **Display** in the **CIFS Service Management** page in the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

Table C-196 Information specified in the CIFS Service Management page (Setting Type: User mapping) (when user mapping uses RID)

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 .

Item	Description
Range of UIDs and GIDs[#]	<p>Specify a range of user IDs and group IDs to be used for user mapping, from 70000 to 2147483147.</p> <p>Specify the minimum value in the left text box and the maximum value in the right text box.</p>
Settings for each domain	<p>Specify a range of user IDs and group IDs for each domain. You can specify a range for a maximum of 256 domains. If you have more than 20 domains to register, only register up to 20 domains at a time to avoid a timeout.</p> <p>Register all domains that have been specified in the authentication mode. If you only register domains that have trust relationships, the users on those domains are not allowed access to the CIFS share.</p> <p>Domain name (NetBIOS)</p> <p>Specify a domain name.</p> <p>Specify the name of a domain that has been specified in the authentication mode or a domain that has a trust relationship.</p> <p>Range of UIDs and GIDs[#]</p> <p>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.</p> <p>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.</p> <p>After specifying the name of a domain and the range of user IDs and group IDs for the domain, when you click Set, the specified information is added to a list box.</p> <p>To remove an entry from the list box, select the entry and then click Delete.</p> <p>The entries in the list box are sorted in ascending order based on the ID range minimum value of each domain.</p>
<p>[#]: You cannot use the user IDs and group IDs that are being used by the HDI system, 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 that the user IDs and group IDs that are being used by the HDI system, 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.</p>	

Table C-197 Information specified in the CIFS Service Management page (Setting Type: User mapping) (when user mapping uses LDAP)

Item	Description			
Use user mapping using LDAP.	Select this option when you want user mapping to use LDAP. If you select this option, specify the items from LDAP server name to Allocate manually . Ask the LDAP server administrator for the information necessary to specify the values.			
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).			
LDAP server port number	Specify an LDAP server port number in the range from 1 to 65535. Specification of this item is optional.			
LDAP server root DN	Specify the identification name of the LDAP server root by using a distinguished name, as in the following example: <code>dc=hitachi,dc=co,dc=jp</code>			
LDAP user map DN	Specify, by using a distinguished name, the identification name for which you want to add a user mapping account of the LDAP server. Specify only the relative DN from LDAP server root DN , as in the following example: <code>ou=idmap</code> 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 by using a distinguished name. Specify only the relative DN from LDAP server root DN , as in the following example: <code>cn=Administrator</code>			
LDAP administrator password	Specify the LDAP administrator password.			
Allocate automatically	Select this to allocate user IDs and group IDs automatically.			
	<table border="1"> <tr> <td data-bbox="641 1339 911 1514">Range of UIDs[#]</td> <td data-bbox="911 1339 1398 1514">Specify a range of user IDs within the range from 70000 to 2147483147. Specify the minimum value in the left text box and the maximum value in the right text box.</td> </tr> <tr> <td data-bbox="641 1514 911 1686">Range of GIDs[#]</td> <td data-bbox="911 1514 1398 1686">Specify a range of group IDs within the range from 70000 to 2147483147. Specify the minimum value in the left text box and the maximum value in the right text box.</td> </tr> </table>	Range of UIDs[#]	Specify a range of user IDs within the range from 70000 to 2147483147. Specify the minimum value in the left text box and the maximum value in the right text box.	Range of GIDs[#]
Range of UIDs[#]	Specify a range of user IDs within the range from 70000 to 2147483147. Specify the minimum value in the left text box and the maximum value in the right text box.			
Range of GIDs[#]	Specify a range of group IDs within the range from 70000 to 2147483147. Specify the minimum value in the left text box and the maximum value in the right text box.			
Allocate manually	Select this to allocate user IDs and group IDs manually. Use IDs from 200 to 2147483147 for user IDs and group IDs that you register on the LDAP server.			

Item	Description
	<p>#: 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.</p> <p>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 the HDI system, 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. If you change the minimum value of a previously set user ID or group ID, you need to perform additional tasks such as re-creating the LDAP server. 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.</p> <p>When user mapping uses LDAP and assigns IDs automatically, 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 page.</p>

Table C-198 Information shown in user mapping ID assignment information of the CIFS Service Management page (Setting Type: User mapping) when user mapping uses LDAP beforehand

Item	Description
<p>Largest currently used UID</p>	<p>The largest user ID within the range of user IDs that have already been assigned in the HDI system.</p> <p>Depending on the status of user mapping usage, the following information might be shown:</p> <p>-</p> <p> User mapping is not used.</p> <p>Not used, or less than the minimum UID used.</p> <p> No user IDs have been assigned, or the smallest assigned user ID is smaller than the minimum value set in Range of UIDs.</p> <p>Cannot be got from LDAP server. Check the LDAP server settings and CIFS service configuration in service.</p> <p> The largest user ID could not be obtained from the LDAP server for user mapping.</p> <p> Check the user mapping settings and the operating status of the LDAP server.</p>
<p>Largest currently used GID</p>	<p>The largest group ID within the range of group IDs that have already been assigned in the HDI system.</p> <p>Depending on the status of user mapping usage, the following information might be shown:</p> <p>-</p> <p> User mapping is not used.</p> <p>Not used, or less than the minimum GID used.</p>

Item	Description
	<p>No group IDs have been assigned, or the smallest assigned group ID is smaller than the minimum value set in Range of GIDs.</p> <p>Cannot be got from LDAP server. Check the LDAP server settings and CIFS service configuration in service.</p> <p>The largest group ID could not be obtained from the LDAP server for user mapping.</p> <p>Check the user mapping settings and the operating status of the LDAP server.</p>

Table C-199 Information specified in User mapping setup in the CIFS Service Management page (Setting Type: User mapping) (when user mapping uses the Active Directory schema)

Item	Description
Use user mapping using Active Directory schema.	Select this when user mapping uses the Active Directory schema. If you select Use user mapping using Active Directory schema. , specify Name service switch .
Name service switch	<p>Select the name service switch.</p> <p>Microsoft® Services for Unix</p> <p>Select this to use Microsoft services for Unix to obtain user IDs and group IDs from the domain controller.</p> <p>Using LDAP as a network information service (RFC2307)</p> <p>Select this to use the RFC2307 schema to obtain user IDs and group IDs from the domain controller.</p> <p>Select Using LDAP as a network information service (RFC2307) if you are using Windows Server 2003 R2 or later.</p>
<p>Note: Use IDs from 200 to 2147483147 for user IDs and group IDs that you register in Active Directory.</p> <p>If Domain controller: LDAP server signing requirements of the domain controller policy is Require signing, startup of the CIFS services will fail. Therefore, select None.</p> <p>Depending on the authentication server OS, the procedure for checking the domain controller policy differs slightly.</p> <p>For Windows Server 2003:</p> <p>Choose Administrative Tools and then Domain Controller Security Policy. In the window that appears, choose Security Settings, Local Policies, and then Security Options, and then check whether Domain controller: LDAP server signing requirements is specified.</p> <p>For Windows Server 2008 or Windows Server 2012:</p> <p>Choose Administrative Tools, Group Policy Management Editor, Computer Configuration, Policies, Windows Settings, and then Security Settings. In the window that appears, choose Local Policies and then Security Options, and then</p>	

Item	Description
	check whether Domain controller: LDAP server signing requirements is specified.

Table C-200 Information specified in User mapping setup in the CIFS Service Management page (Setting Type: User mapping) (when user mapping is not used)

Item	Description
Do not use user mapping.	Select this option if you do not want user mapping to be used.
<p>Note: 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 shown in User mapping setup in the CIFS Service Management page, 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 shown.</p>	

CIFS Service Management page (Setting Type: Security)

You can use the **CIFS Service Management** page (**Setting Type: Security**) to specify the security settings for the CIFS service.

To open the **CIFS Service Management** page (**Setting Type: Security**), select **Security** from **Setting Type**, and then click **Display** in the **CIFS Service Management** page in the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

Table C-201 Information specified in the CIFS Service Management page (Setting Type: Security)

Item	Description
Host access restrictions ^{#1#2}	<p>To limit the CIFS clients that can access the nodes, specify, in the text box, the host name^{#3} or IP address of each CIFS client that is to be allowed access to the CIFS share. Alternatively, specify the network address^{#4} of the network to which each CIFS client belongs. To specify multiple CIFS clients, delimit clients by using commas (,). Note that you can specify no more than 5,631 characters in total. To allow all CIFS clients access to the CIFS share, do not specify anything in the text box.</p> <p>You must also select an option to specify whether the specified CIFS clients are to be allowed or denied access to the CIFS share.</p> <p>Allow</p> <p>Allows the specified hosts or networks to access the nodes.</p> <p>Deny</p> <p>Does not allow the specified hosts or networks to access the nodes.</p>

Item	Description
Mapping to guest account ^{#5}	<p>Specify the definition of guest account users.</p> <p>Unregistered users</p> <p>Select this if users unregistered in the system can be guest account users.^{#6}</p> <p>Unregistered users or invalid passwords</p> <p>Select this if users unregistered in the system or users registered in the system who use an incorrect password can be guest account users.^{#6}</p> <p>Note:</p> <p>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.</p> <p>Never</p> <p>Select this to deny access, by guest account users, to the CIFS shares.</p> <p>Note:</p> <p>If Never is selected, access to all CIFS shares by guest account users is not permitted.</p> <p>Even if Yes is selected in Allow guest account access in the Create and Share File System, the Add Share, or the Edit Share dialog boxes, access is not permitted because the guest account setup for each CIFS share is also disabled.</p>
NetBIOS over TCP/IP	<p>Specify whether to accept access from CIFS clients that use NetBIOS over TCP/IP.</p> <p>Use</p> <p>Select this if you want the CIFS service to accept access from CIFS clients that use NetBIOS over TCP/IP.</p> <p>If Use is selected, name resolution that uses WINS, lmhosts, or broadcast, and the browsing function are available. When using the browsing function for CIFS shares, configure the network as described in the <i>Installation and Configuration Guide</i>.</p> <p>Do not use</p> <p>Select this if you do not want the CIFS service to accept access from CIFS clients that use NetBIOS over TCP/IP.</p> <p>If Do not use is selected, the load of data communication and the security risks can be reduced. However, note that the available name resolution services are only for DNS or hosts. The browsing function is not available.</p>
CIFS access log	<p>Specify whether to collect the CIFS access log.</p> <p>Use</p> <p>Select this if you want to collect the CIFS access log. To change the events that trigger the collection of the CIFS access log, click Set Up in Events logged to</p>

Item	Description
	<p>the CIFS access log, and select the desired events in the page shown (the Setting Events Logged to the CIFS Access Log page).</p> <p>If the CIFS access log file exceeds the max size, do not collect log data.</p> <p>Select this check box if the log file cannot be moved (when the move destination is not specified, or when the capacity of the file system to which the log file is to be moved has reached the maximum limit), and if you want to stop collecting the CIFS access log at the time when the capacity of the log file reaches the maximum limit.</p> <p>This check box is available when Use is selected.</p> <p>Do not use</p> <p>Select this if you do not want to collect the CIFS access log.</p> <p>Note:</p> <p>If Do not use is selected, even when the events that trigger the collection of the CIFS access log are set for each CIFS share by using the <code>cifscreate</code> command or the <code>cifsedit</code> command, the settings are invalid.</p>
Guest account access ^{#7}	<p>Specify permissions for guest account users to access the CIFS shares.</p> <p>Allow</p> <p>Select this to allow guest account users access to the CIFS service.</p> <p>Disallow</p> <p>Select this to disallow guest account users access to the CIFS service.</p>
Access Based Enumeration	<p>Specify whether to use access-based enumeration.</p> <p>Use</p> <p>Select this to use access-based enumeration.</p> <p>Do not use</p> <p>Select this to not use access-based enumeration.</p>
File timestamp changeable users	<p>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.</p> <p>Write permitted users</p> <p>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.</p> <p>Owner only</p> <p>Select this if you want to restrict timestamp updating to the file owner.</p> <p>Note that this setting is invalid in an advanced ACL file system.</p>

Item	Description
Events logged to the CIFS access log	<p>Specify the trigger conditions to collect CIFS access log information. The setting is enabled only when Use is selected in CIFS access log.</p> <p>Clicking Set Up shows the Setting Events Logged to the CIFS Access Log page. For details about how to specify trigger conditions to collect CIFS access log information, see Setting Events Logged to the CIFS Access Log page on page C-239.</p>
SMB encryption ^{#8}	<p>Specify whether communication with the CIFS client is to be encrypted.</p> <p>The setting for this item is only valid if you select SMB 3.0 for the SMB protocol in CIFS Service Management page (Setting Type: <i>Basic</i>). If you select an option other than SMB 3.0 for the SMB protocol, select Disable.</p> <p>Auto</p> <p>Select this option if communication with the client is to be encrypted only when the client supports encryption.</p> <p>Mandatory</p> <p>Select this option if communication with the client is always to be encrypted.</p> <p>Only clients that support SMB 3.0 or later can access a CIFS share. Note that clients cannot access a CIFS share by using guest accounts.</p> <p>Disable</p> <p>Select this option if communication with the client is not to be encrypted.</p>
<p>#1: If Host access restrictions is set in the CIFS Service Management page, the settings in the CIFS Service Management page are applied to all CIFS shares regardless of the settings in the Create and Share File System, the Add Share, or the Edit Share dialog boxes. If you want to specify the settings for each CIFS share, set Host/network based access restriction in the above dialog boxes, and do not set Host access restrictions in the CIFS Service Management page.</p> <p>#2: The user authentication of a CIFS client is performed even if access to the nodes is permitted in Host access restrictions.</p> <p>#3: When you specify a host name for Host access restrictions, edit the <code>/etc/hosts</code> file in the Edit System File page to add the names and IP addresses of all hosts that are specified for Host access restrictions. If the host names are not added to the <code>/etc/hosts</code> file, the specified information might not take effect when access to the nodes is permitted or denied in Host access restrictions. If you specify a host name that corresponds to an IP address and that has been added as an alias after the first host name, system behavior might not be that specified in Host access restrictions. For details about how to edit the <code>/etc/hosts</code> file, see Edit System File page on page C-209.</p> <p>You cannot specify the following names as the host name:</p> <ul style="list-style-type: none"> • ALL • FAIL • EXCEPT <p>#4: Specify the network address in the format below:</p>	

Item	Description
	<p><i>network-address/netmask</i> (example: 10.203.15.0/255.255.255.0)</p> <p>Specify a prefix length for the netmask for IPv6.</p> <p>#5: In Guest account access and Mapping to guest account, access permissions can be specified for the CIFS shares for guest account users, also guest account user definitions can be specified. The guest account is regarded as <i>nobody</i> (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 <i>nobody</i>. You cannot set an ACL that specifies a guest account.</p> <p>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, and then change the settings if necessary. You can specify the settings for each CIFS share in the Create and Share File System, the Add Share, or the Edit Share dialog boxes. Note that the guest account setup for each CIFS share is disabled when Never is specified in Mapping to guest account.</p> <p>#6: The relevant users differ depending on the authentication mode being used (the mode shown in Authentication mode), as shown below:</p> <ul style="list-style-type: none"> • When Local authentication is being used The users not registered on the HDI system • 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 <p>#7: Access permissions with guest accounts can be specified for each CIFS share in addition to CIFS service configuration definition. When changing the CIFS service settings, check the settings for each CIFS share, and then change the settings for CIFS share as necessary. Settings for each CIFS share can be configured in the Create and Share File System dialog box, the Add Share dialog box, or the Edit Share dialog box.</p> <p>#8: If Mandatory is selected in SMB encryption for some CIFS shares and Disable is selected for others, select Auto. Note that when Mandatory is selected in SMB encryption for the CIFS share, if you select Disable, the CIFS share will become inaccessible. When you select Mandatory or Disable, select Inherit CIFS service default in SMB encryption for the CIFS share.</p>

CIFS Service Management page (Setting Type: Performance)

You can use the **CIFS Service Management** page (**Setting Type: Performance**) to specify the performance settings for the CIFS service.

To open the **CIFS Service Management** page (**Setting Type: Performance**), select **Performance** from **Setting Type**, and then click **Display** in the **CIFS Service Management** page in the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

**Table C-202 Information specified in the CIFS Service Management page
(Setting Type: Performance)**

Item	Description
<p>Client time-out</p>	<p>Specify the maximum time to wait for a client response as the timeout value from 0 to 1,440 (units: minutes).</p> <p>When 0 is specified, a client is not automatically disconnected by a timeout.</p> <p>If the specified value is smaller than the default, you might not be able to connect to the file system depending on the number of CIFS clients or the status of node operations. In this case, you need to wait a while, and then connect from the CIFS client again.</p>
<p>Automatic reloading of CIFS share settings^{#1}</p>	<p>Specify whether to reload the CIFS share settings automatically when they are changed.</p> <p>Perform</p> <p>Select this if you want to reload the CIFS share settings automatically. If Perform is selected, the CIFS share settings are automatically applied to the CIFS client environment when they are changed.</p> <p>Do not perform</p> <p>Select this if you do not want to reload the CIFS share settings automatically.</p> <p>The maximum possible number of concurrent connections from clients to a CIFS share depends on whether the CIFS share settings are automatically reloaded. For details, see the <i>File System Protocols (CIFS/NFS) Administrator's Guide</i>.</p>
<p>Disk synchronization policy^{#2}</p>	<p>Specify the operations for write requests from CIFS clients to CIFS shares.</p> <p>At write and close</p> <p>Select this to write synchronously with a write request or a close request.</p> <p>At close</p> <p>Select this to write synchronously with a close request.</p> <p>Routine disk flush only</p> <p>Select this to write at a fixed interval, regardless of when write requests and close requests are made.</p>
<p>Windows® client access policy</p>	<p>Select the method for processing accesses from Windows clients.</p> <p>Parallel</p> <p>Select this to process accesses in parallel.</p> <p>Serial</p> <p>Select this to process accesses serially.</p>
<p>CIFS client cache</p>	<p>Specify whether the updated data in the CIFS share file is to be cached on the client.</p>

Item	Description
	<p>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.</p> <p>Specify Do not use for read-write-content-sharing file systems. If the updated data of the file in the CIFS share is cached on the client, the update date might not be reflected properly on other sites.</p> <p>Use</p> <p>Select this if the updated data in the CIFS share file is to be cached on the client.</p> <p>For the file systems listed below, we recommend also setting Read-only client cache for access conflicts values to Use, because there is a risk that the client cache will fail to validate.</p> <ul style="list-style-type: none"> - File systems that migrate data to an HCP system <p>Do not use</p> <p>Select this if the updated data in the CIFS share file is not to be cached on the client.</p>
<p>Read-only client cache for access conflicts</p>	<p>Specify whether to use a read-only client cache when multiple CIFS clients simultaneously attempt to access a file.</p> <p>Selecting Use improves system performance because data is cached on the client PC when a CIFS client opens a file.</p> <p>Use</p> <p>Select this to use a read-only client cache. This item can be selected if Use has been selected for CIFS client cache.</p> <p>Do not use</p> <p>Select this to not use a read-only client cache.</p> <p>Note that we recommend that you do not use the read-only client cache if you also want to use the NFS protocol to access the file shares because changes might not be applied. If you need to use the read-only client cache, we recommend implementing file sharing individually for each protocol to ensure that the NFS protocol is not used to access the share.</p>
<p>#1: If you set Do not perform, any changes made to the CIFS share settings are not automatically applied to the CIFS client environment. The CIFS share settings are applied if you perform one of the following actions:</p> <ul style="list-style-type: none"> • Restart the CIFS service • Log on again to the CIFS client machine • Disconnect all the connections to the CIFS share from the CIFS client machines, and then connect again <p>Changes to the settings are also applied when a CIFS client is automatically disconnected because the client's connection times out, and is reconnected. If you specify Do not perform, Hitachi Data Systems recommends that you specify a relatively short amount of time (about 6 minutes) for Client time-out.</p>	

Item	Description
	<p>#2: Operations when receiving requests to write to CIFS share folder from CIFS clients can be specified for each CIFS share in addition to CIFS service configuration definition.</p> <p>If you choose to write synchronously with a write request or a close request, data is immediately written to the disk drive every time a write request is received, and then the result is returned to the request source. Therefore, this setting results in lower I/O performance compared to other settings. However, if a failure occurs in the CIFS client or in the network, this setting ensures that write operations are performed to the disk drive for which the results are returned to the request source.</p> <p>If you choose to write synchronously with a close request, the result for a write request is returned to the CIFS client immediately after the HDI system receives the request, and then the data is written to the disk drive when the file is closed. Therefore, this setting results in better I/O performance than writing synchronously with a write request or a close request. However, if a failure occurs, write operations might not be performed to the disk drive for which the results are returned to the request source.</p> <p>If you select to write at a fixed interval, data is written to the disk drive regardless of when write requests and close requests are made. Therefore, this setting results in better I/O performance than any other setting. However, if a failure occurs, there is a higher probability that data might not have been written to the disk drive.</p> <p>Regardless of which setting is selected, flushing the target file causes write operations to the disk drive to be performed.</p>

CIFS Service Management page (Setting Type: Administration)

You can use the **CIFS Service Management** page (**Setting Type: Administration**) to specify the administrator settings for the CIFS service.

To open the **CIFS Service Management** page (**Setting Type: Administration**), select **Administration** from **Setting Type**, and then click **Display** in the **CIFS Service Management** page in the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

Table C-203 Information specified in the CIFS Service Management page (Setting Type: Administration)

Item	Description
CIFS administrator name(s)	<p>Specify the name of a user or group to be defined as a CIFS administrator. For group names, specify an at mark (@) in front of a name. 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.</p> <p>If you want to specify multiple names, separate them by commas (,).</p> <p>When you are using user mapping, specify a domain name with the user or group name as follows:</p> <pre>domain-name\user-name @domain-name\group-name</pre>

Item	Description
	If you use the Active Directory authentication, specify the same domain name as specified in Domain name (NetBIOS) .

Setting Events Logged to the CIFS Access Log page

The **Setting Events Logged to the CIFS Access Log** page can be used to specify an event that triggers collection of the CIFS access log.

Specified settings are applied to the whole CIFS service. However, if events that trigger collection of the CIFS access log are specified for each CIFS share by using the `cifscreate` command or the `cifsedit` command, the settings for each CIFS share are given priority over the settings for the whole CIFS service. When the settings for the CIFS service are changed, check the settings for each CIFS share as well as the settings for the entire CIFS service.

To open the **Setting Events Logged to the CIFS Access Log** page, click **Set Up** on **Events logged to the CIFS access log** in the **CIFS Service Management** page (**Setting Type:** *Security*) of the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

Table C-204 Information specified in the Setting Events Logged to the CIFS Access Log page

Item	Description
Events logged to the CIFS access log	<p>Specify the events that trigger collection of the CIFS access log.</p> <p>Successful</p> <p>Select the check boxes for desired events (from the items shown below) if you want a successful access corresponding to one of those events to trigger the collection of the CIFS access log.</p> <p>Failed</p> <p>Select the check boxes for desired events (from the items shown below) if you want a failed access corresponding to one of those events to trigger the collection of the CIFS access log.</p> <p>Each of the following items is used to specify an event (or access):</p> <ul style="list-style-type: none"> • List folder contents • Read data • Create files or write data • Create folders • Delete items • Read permissions • Change permissions

Item	Description
	<ul style="list-style-type: none"> • Change ownership • Rename items • Connect to or disconnect from shares

Select Authentication Mode page

The **Select Authentication Mode** page can be used to set the authentication mode used in the CIFS service.

To open the **Select Authentication Mode** page, click **Change Authentication Mode** option in the **CIFS Service Management** page (**Setting Type:** *Basic*) of the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)). If you select the authentication mode, and then click **OK**, the settings page is shown.

Table C-205 Information specified in the Select Authentication Mode page

Item	Description	See
Authentication mode	From the options, select the method for authenticating users accessing the CIFS share from a CIFS client.	N/A
Local authentication	Select this mode when you want to use the CIFS server function of the OS to authenticate users.	Local Authentication page on page C-241
NT domain authentication #1	Select this mode when the domain controller within the domain authenticates users. Users registered on the HDI system cannot access CIFS shares, because users are managed by the corresponding domain controller.	NT Domain Authentication page on page C-241
Active Directory authentication #1.#2	Select this mode when the Active Directory domain controller authenticates users. Users registered on the HDI system cannot access CIFS shares, because users are managed by the Active Directory domain controller.	Active Directory Authentication page on page C-241
<p>Note: N/A = Not applicable.</p> <p>#1: 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 on the HDI system, the NIS server, or the LDAP server for user authentication. Therefore, Hitachi Data Systems recommends that you use user mapping when using NT domain authentication or Active Directory authentication to authenticate users.</p> <p>#2: When the FTP or SFTP service settings permit users authenticated by Active Directory to log on, the FTP or SFTP service must be restarted if the authentication method is changed from or to Active Directory authentication.</p>		

Local Authentication page

You can use the **Local Authentication** page to set up local authentication.

Table C-206 Information specified in the Local Authentication page

Item	Description
Workgroup name	Enter the name of the work group to which the node belongs. Use a name that differs from the node host name. If you specify the same name, the group name might not be shown correctly when you set up an ACL.

NT Domain Authentication page

You can use the **NT Domain Authentication** page to set up NT domain authentication. Users registered on the HDI system cannot access CIFS shares, because users are managed by the specified domain controller.

Table C-207 Information specified in the NT Domain Authentication page

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. This item is optional.
Domain administrator name	Enter the user name of the domain administrator.
Administrator password	Enter the password of the domain administrator.

Active Directory Authentication page

You can use the **Active Directory Authentication** page to set up Active Directory authentication. Users registered on the HDI system cannot access CIFS shares, because users are managed by the Active Directory domain controller.

Table C-208 Information specified in the Active Directory Authentication page

Item	Description
Domain name[#]	Enter the DNS name of the Active Directory domain. Any lower-case letters that are entered are treated as upper-case letters. If both the Active Directory domain controller and the KDC server are used as one server, the name specified here will also be used as the name of the domain to which the KDC server belongs. If the NFS service configuration definitions are set to apply the

Item	Description
	domain name to the NFSv4 domain, the name specified here will also be used as the name of the NFSv4 domain. In addition, if the FTP or SFTP service settings permit users authenticated by Active Directory to log on, the name specified here will also be used as the domain name of the FTP or SFTP service.
Domain name (NetBIOS)	Enter the NetBIOS name of the Active Directory domain.
DC server name(s)#	Specify the server name for the Active Directory domain controller to which the node belong. Up to 5 server names can be specified. When specifying multiple names, separate each with a comma (,). You can also specify the IP address. If both the Active Directory domain controller and the KDC server are used as one server, the name specified here will also be used as the name of the KDC server. If the FTP or SFTP service settings permit users authenticated by Active Directory to log on, the name specified here will also be used as the domain name of the FTP or SFTP service.
Domain user name	Enter the name of the user for the Active Directory domain controller.
Domain user password	Enter the password of the user for the Active Directory domain controller.
# If you use both the Active Directory domain controller and the KDC server as one server, and the specified name is different from the name of the domain to which the KDC server belongs or the KDC server used by the NFS service, you need to restart the NFS service.	

FTP Service Management page

The **FTP Service Management** page can be used to change the configuration definitions of the FTP service. If a client accesses the FTP service by using the FTP protocol, the virtual IP address is used for connection.



Note:

- When the system administrator changes the configuration definitions of the FTP service, anonymous users are allowed to log on 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.
- 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 **Restart** in the **List of Services** page.

- Even if the OS is restarted after the configuration definitions of the FTP service are modified, the modified configuration definitions are not applied. Restart the service.
- If the system administrator changes the configuration definitions of the FTP service while a client is updating the file system, the client operation might not finish normally. The system administrator must contact users before changing the configuration definitions.
- When the `chmod` command is run 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.
- The system administrator must modify the service configuration definitions of each node in the same way to avoid inconsistency among nodes in a cluster.

To open the **FTP Service Management** page, select the **FTP** option, and then click **Modify Configuration** in the **List of Services** page of the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

Table C-209 Information specified in the FTP Service Management page

Item	Description
Specification method for a login directory	<p>Select the method of setting a directory to which the users can log on by using the FTP service.</p> <p>All mounted file systems can be used.</p> <p>Log on to the <code>/mnt</code> directory. This setting allows use of all file systems mounted on each node. If you select this item, both nodes can use the FTP service.</p> <p>Only the specified directory can be used.</p> <p>Log on to a specified file system or directory. This setting limits the accessible range to the specified file system or node. If you select this item, only one node can use the FTP service.</p>
Login directory	<p>Specify the directory to which the users can log on by using the FTP service.</p> <p>The system assumes <code>/mnt</code> 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 log on directory.</p> <p>Clicking Select shows the List of Mounted File Systems page. If you select, from a list of mounted file systems, an option for a file system for which the FTP service permits login, and then click OK, the mount point of the selected file system is shown in the Login directory text box. To show a directory under the file system, directly enter the directory after the mount point shown.</p> <p>When you create a login directory for the FTP service, the directory name must be unique within the cluster. Make sure that you specify an absolute path name that begins with <code>/mnt/</code>. You cannot specify a path including a symbolic link.</p>

Item	Description
	<p>You can use any alphanumeric character, exclamation mark (!), hash mark (#), dollar sign (\$), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), plus sign (+), comma (,), forward slash (/), semicolon (;), equal sign (=), at mark (@), left square bracket ([), right square bracket (]), caret (^), grave accent mark (`), left curly bracket ({), right curly bracket (}) and tilde (~). Login directory is case-sensitive. You can also specify multi-byte characters. The forward slash specified at the end of the string will be removed.</p> <p>When sharing a directory of the file system:</p> <p style="padding-left: 40px;"><i>/mnt/name-of-mounted-file-system/path-name</i></p> <p>Example: <i>/mnt/filesystem01/ftp1</i></p> <p>When sharing the whole of each file system:</p> <p style="padding-left: 40px;"><i>/mnt/name-of-mounted-file-system</i></p> <p>Example: <i>/mnt/filesystem02</i></p> <p>A mount point can be specified for a file system to which <code>On (Read/Write)</code> is selected for Content Sharing.</p> <p>You cannot specify a file system for which <code>On (Read-Only)</code> or <code>Home directory</code> is selected for Content Sharing.</p>
Directory creation/change	<p>Select whether to create a new directory from the option 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.</p> <p>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 <i>/mnt</i>.</p> <p>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:</p> <p>Owner</p> <p style="padding-left: 40px;">Specify the user name or user ID of the owner.</p> <p>Group</p> <p style="padding-left: 40px;">Specify the group name or group ID of the owner group.</p> <p>Permission mode</p> <p style="padding-left: 40px;">From the drop-down list, select the access permission for the directory owner, owner's group, and others.</p> <p>Read / Write</p> <p style="padding-left: 40px;">Select this mode to grant both read and write permissions. The directory execution permission is granted.</p> <p>Read only</p> <p style="padding-left: 40px;">Select this mode to grant read permissions only. The directory execution permission is granted.</p> <p>None</p>

Item	Description
	<p>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.</p> <p>Sticky bit</p> <p>Permit only the owner of the directory to delete or rename the files or directories under that directory.</p> <p>From the options, select whether to set a sticky bit for the directory.</p> <p>On</p> <p>Set a sticky bit.</p> <p>Off</p> <p>Do not set a sticky bit.</p> <p>When you are not using user mapping, Specify the user and the group name no more than 16 characters. You can use any alphanumeric character, hyphen (-), period (.), and underscore (_).</p> <p>When you are using user mapping, specify a domain name with the user or group name as follows:</p> <p><i>domain-name\user-name</i> <i>domain-name\group-name</i></p> <p>Specify a domain name using no more than 15 characters. The characters that can be used for the domain name are alphanumeric characters, exclamation mark (!), hash mark (#), percent sign (%), ampersand (&), left parenthesis ((), right parenthesis ()), hyphen (-), period (.), left angle bracket (<), caret (^), underscore (_), left curly bracket ({), right curly bracket (}), tilde (~), space and multi-byte characters that are encoded in UTF-8. When you are using user mapping, Specify the user name no more than 20 characters or the group name no more than 64 characters. The characters that can be used for the user name and the group name are alphanumeric characters, exclamation mark (!), hash mark (#), percent sign (%), ampersand (&), left parenthesis ((), right parenthesis ()), hyphen (-), period (.), left angle bracket (<), caret (^), underscore (_), left curly bracket ({), right curly bracket (}), tilde (~), space and multi-byte characters that are encoded in UTF-8.</p> <p>If you use Active Directory authentication, specify the same domain name as specified in Domain name (NetBIOS).</p>
Allowed users	<p>Specify the users to be allowed to log on by using the FTP service.</p> <p>All users</p> <p>Allow all users to log on by using the FTP service.</p> <p>Note that the users registered by user mapping cannot log on by using the FTP service.</p> <p>To permit users authenticated by Active Directory to log on, select the Including Active Directory users check box.</p> <p>Selected users</p>

Item	Description
	<p>Allow the specified users to log on by using the FTP service. Clicking Set Up shows the Select FTP Users page. In this page, select the users to be allowed to log on by using the FTP service. You can select a maximum of 2,000 users.</p> <p>For details about how to select the users in the Select FTP Users page, see FTP Service Management page on page C-242.</p> <p>This item name is followed by the number of users currently allowed to log on, using the Selected users(number-of-users users) format.</p>
Number of simultaneous connections	Specify the number of users who can concurrently log on by using the FTP service, from 10 to 500.
Connection timeout wait time	Specify the timeout for an automatic logoff, from 30 to 43,200 (units: seconds). If no operation is performed within the timeout period after an FTP client has logged on to the directory, the FTP client is logged off automatically.
Anonymous user settings	<p>From the options, select whether to allow anonymous users to log on by using the FTP service.</p> <p>Allow anonymous logins</p> <p>Select this to grant anonymous users permission to log on by using the FTP service. Anonymous users can use the FTP service with the ftp user (UID=97) and ftp group (GID=97) permissions.</p> <p>Allow uploads</p> <p>When you select Allow anonymous logins, use a check box to specify whether to allow anonymous users to upload data.</p> <p>Do not allow anonymous logins</p> <p>Do not allow anonymous users to log on by using the FTP service.</p>
<p>Note: Observe the following when you set a directory to which users log on by using the FTP service:</p> <ul style="list-style-type: none"> • Directories that the NFS client created by using EUC or JIS character encoding cannot be specified as a directory to which users log on by using the FTP service. • Hitachi Data Systems recommends you generally 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 a service when a failover occurs, you need to 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. <p>The List of Mounted File Systems page only shows the file system contained in the node to which you have logged on. With Only the specified directory can be used. selected, you can click Select for Login directory to show the List of</p>	

Item	Description
	<p>Mounted File Systems page. In this page, 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.</p> <p>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.</p> <ul style="list-style-type: none"> If you log on by using the FTP service and run a command, the directory specified in Login directory is used as the root directory.

Select FTP Users page

You can use the **Select FTP Users** page to permit logon by way of FTP from specific users.

To open the **Select FTP Users** page, click **Set Up** of **Allowed users** in the **FTP Service Management** page of the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

Table C-210 Information specified in the Select FTP Users page

Item	Description
<p>List of selectable users</p>	<p>From the List of selectable users list box, select the users who will use the FTP service. To narrow down the list of users, select the users from the Condition drop-down list, and then click Display.</p> <p>all All user names are shown.</p> <p>a to z, A to Z, or 0 to 9 The user names that begin with the selected alphanumeric character.</p> <p>other The user names that begin with a character other than an alphanumeric.</p> <p>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 shown 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 listed.</p> <p>Range text box The sequence number of the user who is shown 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 Display. This shows 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 Display, the value specified in the Range text box is ignored and users are shown beginning with the first user.</p>

Item	Description
	<p>Prev</p> <p>Clicking Prev shows in sequential order the users preceding the user shown at the beginning of the List of selectable users list box. If the user shown at the beginning of the List of selectable users list box is the first user, or if the total number of filtered users is 0, an error message appears when you click Prev.</p> <p>Next</p> <p>Clicking Next shows in sequential order the users following the user shown at the end of the List of selectable users list box. If the user shown at the end of the List of selectable users list box is the last user, or if the total number of filtered users is 0, an error message appears when you click Next.</p> <p>When you click ▼, the users selected in List of selectable users are added to the Selected users list box. Only users listed in the Selected users list box will be set as users with the designated access permission.</p> <p>To delete a user from the Selected users list box, select the user and click ▲.</p>

NFS Service Management page

You can use the **NFS Service Management** page to change the configuration definition of the NFS service. By modifying configuration definitions, in the **NFS Service Management** page, 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.



Note: The system administrator must note the following before modifying the configuration definitions of the NFS service:

- The system administrator must modify the service configuration definitions of each node in the same way to avoid inconsistency among nodes in a cluster.
- Even if the OS is restarted after the configuration definitions of the NFS service are modified, the modified configuration definitions are not applied. Restart the service.
- If you changed the value of **nfsd buffer size**, or disabled or changed the items for the functions that NFS clients are using in **Protocol version**, **Security flavor**, **KDC server domain name**, or **KDC server name(s)**, make sure that the file system has been unmounted from the NFS client, and then restart the NFS service.
- When you stop the NFS service, ask the NFS client host's administrator not to access NFS shares until the NFS service has started.
- When you change **Number of nfsd processes** in the NFS service configuration definition, determine the appropriate maximum number of NFS daemon processes by using the `nfsstatus` command to check the

current NFS daemon usage and memory usage. Increase the maximum number of processes if the system is running for a long time with high usage (90 to 100%) or `Number of times that all threads were in use` is more than 0. Decrease the maximum number of processes if `Retry count of buffer acquisition` is more than 0, which means retries occurred because `nfsd` processes failed to obtain an area for data transfer.

- The system administrator 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), or disabling or changing the items for the functions that NFS clients are using in **Protocol version**, **Security flavor**, **KDC server domain name**, or **KDC server name(s)** in the NFS service configuration definition. If the system administrator changes these settings 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, and restarting the NFS service, the system administrator must request the NFS client host's administrator to remount the file system that was unmounted from the NFS client.
- If Kerberos authentication is used and the times of the HDI system and an NFS client host differ, authentication might fail for an NFS client accessing the HDI system. Use the NTP server to synchronize the times of the HDI system and the NFS client hosts.

To open the **NFS Service Management** page, in the **List of Services** page of the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)), select **NFS**, and then click **Modify Configuration**.

Table C-211 Information specified in the NFS Service Management page

Item	Description
Number of nfsd processes	Enter the maximum number of <code>nfsd</code> processes that are run from 1 to 2,048. Note that the number of <code>nfsd</code> processes that are started during operation are automatically adjusted to a number that does not exceed the specified maximum according to the system status. However, if you specify less than 64 for the maximum, the actual maximum will be 64. If you specify 64 or more, the maximum will be a multiple of the number of CPUs. For example, if there are 16 CPUs and you specify 90 for this item, the actual maximum will be 96.
nfsd buffer size	Enter the maximum buffer size of data transmission from 8 to 1,024 (units: KB). 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.

Item	Description
	If NFS is mounted by using the UDP protocol, the maximum data size that can be transmitted is 56 KB, even if a value of more than 56 is specified.
Protocol version	Specify the NFS protocol version to be used. Select one or more of the following check boxes: v2 Select this to use NFSv2. v3 Select this to use NFSv3. v4 Select this to use NFSv4.
Port number allocation	Specify how the port number is assigned to the NFS service. Dynamic Select this to dynamically assign a port number. Fixed Select this to assign a fixed port number.
Security flavor	Specify the security flavor to be used. Select one or more of the following check boxes: sys Select this to use the UNIX (AUTH_SYS) authentication. krb5 Select this to use the Kerberos authentication. krb5i Select this to use the data integrity function in addition to the Kerberos authentication. krb5p Select this to use the data integrity function and privacy function in addition to the Kerberos authentication.
Domain name[#]	Specify the NFSv4 domain name or the name of the domain to which the KDC server belongs. Also, specify the domain to which the domain name is applied. Apply to an NFS v4 domain Select this to apply the name to an NFSv4 domain. Apply to a KDC server domain Select this to apply the name to a KDC server domain. If both the KDC server and the Active Directory domain controller are used as one server, the name specified here will also be used as the Active Directory domain controller name. Any lower-case letters that are entered are treated as upper-case letters.

Item	Description
KDC server name(s)#	<p>Specify the KDC server name.</p> <p>Up to 5 server names can be specified. When specifying multiple names, separate each with a comma (,). You can also specify the IP address.</p> <p>You can use an alphanumeric character for the first character, and alphanumeric character, hyphen (-), or underscore (_) for the second and subsequent characters. The default is nobody (user ID: 65534).</p>
Anonymous user name	<p>Specify a user name. This user name will be mapped to a user who belongs to a domain whose name is not set as the NFSv4 domain name for the NFS service or who is not managed by the HDI system, when an access is made by the user.</p> <p>Specify a user name that has been registered in the HDI system, NIS server, or LDAP server for user authentication.</p>
Anonymous group name	<p>Specify a group name. This group name will be mapped to a group that belongs to a domain whose name is not set as the NFSv4 domain name for the NFS service or that is not managed by the HDI system, when an access is made by the group.</p> <p>Specify a group name that has been registered in the HDI system, NIS server, or LDAP server for user authentication.</p>
<p>#: If both the KDC server and the Active Directory domain controller are used as one server, and the specified name is different from the name of the Active Directory domain or domain controller used by the CIFS service, you need to restart the CIFS service.</p>	

SFTP Service Management page

The **SFTP Service Management** page can be used to change the configuration definitions of the SFTP service. If a client accesses the SFTP service by using the SFTP protocol, the virtual IP address is used for connection.



Note:

- The service does not automatically restart even when the configuration definitions of the SFTP service have been changed. If the configuration definitions of the SFTP service have been changed, restart the service by clicking **Restart** in the **List of Services** page.
- Even if the OS is restarted after the configuration definitions of the SFTP service are modified, the modified configuration definitions are not applied. Restart the service.
- If the system administrator changes the configuration definitions of the SFTP service while a client is updating the file system, the client operation might not finish normally. The system administrator must contact users before changing the configuration definitions.

- When the `chmod` command is run 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.
- The system administrator must modify the service configuration definitions of each node in the same way to avoid inconsistency among nodes in a cluster.

The **SFTP Service Management** page is shown by selecting the **SFTP** option, and then clicking **Modify Configuration** option in the **List of Services** page of the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

Table C-212 Information specified in the SFTP Service Management page

Item	Description
Specification method for a login directory	<p>Select the method of setting a directory to which the users can log on by using the SFTP service.</p> <p>All mounted file systems can be used.</p> <p>Log on to the <code>/mnt</code> directory. This setting allows use of all file systems mounted on each node. If you select this item, both nodes can use the SFTP service.</p> <p>Only the specified directory can be used.</p> <p>Log on to a specified file system or directory. This setting limits the accessible range to the specified file system or node. If you select this item, only one node can use the SFTP service.</p>
Login directory	<p>Specify the directory to which the users can log on by using the SFTP service.</p> <p>The system assumes <code>/mnt</code> 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 log on directory.</p> <p>Clicking Select shows the List of Mounted File Systems page. If you select, from a list of mounted file systems, an option for a file system for which the SFTP service permits login, and then click OK, the mount point of the selected file system is shown in the Login directory text box. To show a directory under the file system, directly enter the directory after the shown mount point.</p> <p>When you create a login directory for the SFTP service, the directory name must be unique within the cluster. Make sure that you specify an absolute path name that begins with <code>/mnt/</code>. You cannot specify a path including a symbolic link.</p> <p>You can use any alphanumeric character, exclamation mark (!), dollar sign (\$), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), plus sign (+), comma (,), forward slash (/), semicolon (;), at mark (@), left square bracket ([), right square bracket (]), caret (^), grave accent mark (`), left curly bracket ({), right curly bracket (}) and tilde (~). Login directory is case-sensitive. You can also specify multi-byte characters.</p>

Item	Description
	<p>The forward slash specified at the end of the string will be removed.</p> <p>When sharing a directory of the file system: <code>/mnt/<i>name-of-mounted-file-system</i>/<i>path-name</i></code> Example: <code>/mnt/filesystem01/sftpl</code></p> <p>When sharing the whole of each file system: <code>/mnt/<i>name-of-mounted-file-system</i></code> Example: <code>/mnt/filesystem02</code></p> <p>A mount point can be specified for a file system to which On (Read/Write) is selected for Content Sharing.</p> <p>You cannot specify a file system for which On (Read-Only) or Home directory is selected for Content Sharing.</p>
<p>Directory creation/change</p>	<p>Select whether to create a new directory from the option 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.</p> <p>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 <code>/mnt</code>.</p> <p>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:</p> <p>Owner Specify the user name or user ID of the owner.</p> <p>Group Specify the group name or group ID of the owner group.</p> <p>Permission mode From the drop-down list, select the access permission for the directory owner, owner's group, and others.</p> <p>Read / Write Select this mode to grant both read and write permissions. The directory execution permission is granted.</p> <p>Read only Select this mode to grant read permissions only. The directory execution permission is granted.</p> <p>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.</p> <p>Sticky bit Permit only the owner of the directory to delete or rename the files or directories under that directory.</p>

Item	Description
	<p>From the options, select whether to set a sticky bit for the directory.</p> <p>On Set a sticky bit.</p> <p>Off Do not set a sticky bit.</p> <p>When you are not using user mapping, Specify the user and the group name no more than 16 characters. You can use any alphanumeric character, hyphen (-), period (.), and underscore (_).</p> <p>When you are using user mapping, specify a domain name with the user or group name as follows: <i>domain-name\user-name</i> <i>domain-name\group-name</i></p> <p>Specify a domain name using no more than 15 characters. The characters that can be used for the domain name are alphanumeric characters, exclamation mark (!), hash mark (#), percent sign (%), ampersand (&), left parenthesis ((), right parenthesis ()), hyphen (-), period (.), left angle bracket (<), caret (^), underscore (_), left curly bracket ({), right curly bracket (}), tilde (~), space and multi-byte characters that are encoded in UTF-8. When you are using user mapping, Specify the user name no more than 20 characters or the group name no more than 64 characters. The characters that can be used for the user name and the group name are alphanumeric characters, exclamation mark (!), hash mark (#), percent sign (%), ampersand (&), left parenthesis ((), right parenthesis ()), hyphen (-), period (.), left angle bracket (<), caret (^), underscore (_), left curly bracket ({), right curly bracket (}), tilde (~), space and multi-byte characters that are encoded in UTF-8.</p> <p>If you use Active Directory authentication, specify the same domain name as specified in Domain name (NetBIOS).</p>
Allowed users	<p>Specify the users to be allowed to log on by using the SFTP service.</p> <p>All users Allow all users to log on by using the SFTP service. Note that the users registered by user mapping cannot log on by using the SFTP service. To permit users authenticated by Active Directory to log on, select the Including Active Directory users check box.</p> <p>Selected users Allow the specified users to log on by using the SFTP service. Clicking Set Up shows the Select SFTP Users page. In this page, select the users to be allowed to log on by using the SFTP service. You can select a maximum of 2,000 users.</p>

Item	Description
	<p>For details about how to select the users in the Select SFTP Users page, see SFTP Service Management page on page C-251.</p> <p>This item name is followed by the number of users currently allowed to log on, using the Selected users(<i>number-of-users users</i>) format.</p>
<p>Note: Observe the following when you set a directory to which users log on by using the SFTP service:</p> <ul style="list-style-type: none"> • Directories that the NFS client created by using EUC or JIS character encoding cannot be specified as a directory to which users log on by using the SFTP service. • Hitachi Data Systems recommends you generally 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 a service when a failover occurs, you need to make sure that the SFTP service settings are the same for both nodes and that the SFTP services are running on both nodes. If you select Only the specified directory can be used., the SFTP 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. <p>The List of Mounted File Systems page only shows the file system contained in the node to which you have logged on. With Only the specified directory can be used. selected, you can click Select for Login directory to show the List of Mounted File Systems page. In this page, you select the login file system for the SFTP service. In this case, you must also directly enter a path for Login directory for the other node.</p> <p>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.</p> <ul style="list-style-type: none"> • In the SFTP service, you cannot access directories above the login directory. 	

Select SFTP Users page

You can permit logon by way of SFTP from specific users.

The **Select SFTP Users** page is shown by clicking **Set Up** of **Allowed users** in the **SFTP Service Management** page of the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

Table C-213 Information specified in the Select SFTP Users page

Item	Description
List of selectable users	<p>From the List of selectable users list box, select the users who will use the SFTP service. To narrow down the users to be shown, select the users from the Condition drop-down list, and then click Display.</p> <p>all</p> <p>All user names are shown.</p>

Item	Description
	<p>a to z, A to Z, or 0 to 9</p> <p>The user names that begin with the selected alphanumeric character.</p> <p>other</p> <p>The user names that begin with a character other than an alphanumeric.</p> <p>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 shown 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 shown.</p> <p>Range text box</p> <p>Shows initially the sequence number of the user who is shown at the beginning of the List of selectable users list box.</p> <p>Specify a value equal to or less than the total number of filtered users, and then click Display. This shows 1,000 users, beginning with the user whose sequence number you specified.</p> <p>If you then select a different filter from the Condition drop-down list and click Display, the value specified in the Range text box is ignored and users are shown beginning with the first user.</p> <p>Prev</p> <p>Clicking Prev shows in sequential order the users preceding the user shown at the beginning of the List of selectable users list box. If the user shown at the beginning of the List of selectable users list box is the first user, or if the total number of filtered users is 0, an error message appears when you click Prev.</p> <p>Next</p> <p>Clicking Next shows in sequential order the users following the user shown at the end of the List of selectable users list box. If the user shown at the end of the List of selectable users list box is the last user, or if the total number of filtered users is 0, an error message appears when you click Next.</p> <p>When you click ▼, the users selected in List of selectable users are added to the Selected users list box. Only users listed in the Selected users list box will be set as users with the designated access permission.</p> <p>To delete a user from the Selected users list box, select the user and click ▲.</p>

Public Key List page

The **Public Key List** page can be used to manage public keys used for accessing by using the SSH protocol.

**Note:**

- Before registering a public key, the system administrator must use a key creation tool to create the keys (private key and public key) that are used in the SSH authentication. For details about 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 log on password. You can skip specifying a passphrase.
- Create a public key on a machine from which the system administrator can log on to the HDI GUI.
- SSH2 is supported in HDI systems.
- Before registering a public key, the system administrator must modify the service configuration definitions of each node in the same way to avoid inconsistency among nodes in a cluster.
- The public key is registered for the SSH account `nasroot`. Make sure that there are no more than 128 public keys per node.

To open the **Public Key List** page, select **SSH**, and then click **Modify Configuration** in the **List of Services** page of the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

Table C-214 Information shown in the Public Key List page

Item	Description
SSH protocol version	Version of the SSH protocol
Comment	Comment about the public key

Table C-215 Operations that can be performed from the Public Key List page

Button	Description	See
Delete	The selected public key can be deleted.	N/A
Add	A public key can be registered.	Add Public Key page on page C-257

Note: N/A = Not applicable.
Note: These operations must be performed for each node in the cluster.

Add Public Key page

You can use the **Add Public Key** page to register a public key.

To open the **Add Public Key** page, click **Add** in the **Public Key List** page of the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

Table C-216 Information specified in the Add Public Key page

Item	Description
Public key file	Specify the path to the public key file. To select a file name through browsing, click Browse .
Comment	Enter a comment about the public key, using no more than 32 characters. You can use alphanumeric characters and hyphens (-). You can also specify spaces, but not at the beginning or end of the character string.

CIFS Service Maintenance page

The **CIFS Service Maintenance** page can be used to maintain the CIFS service in operation.



Note:

- In an environment where user mapping is being used, if you delete cached user mapping information, the CIFS service is automatically restarted. Make sure that no users are accessing CIFS shares, and then delete the user mapping information.
- In an environment where user mapping uses LDAP, if you delete cached user mapping information, a query about the user ID and group ID for an LDAP server occurs when a user first accesses a CIFS share. Such queries affect access performance. Delete the cached user mapping information only when it is no longer necessary.
- 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, and then rejoin the CIFS service to the Active Directory domain.
- Maintenance must be performed for each node in the cluster.

To open the **CIFS Service Maintenance** page, select the **CIFS** option, and then click **Service Maintenance**, in the **List of Services** page of the **Access Protocol Configuration** dialog box ([Access Protocol Configuration dialog box on page C-217](#)).

Table C-217 Information specified in the CIFS Service Maintenance page

Item	Description	See
CIFS service information	The CIFS service configuration definition.	CIFS service information on page C-259
CIFS default information	The configuration that is applied to CIFS shares by default.	CIFS default information on page C-263

Item	Description	See
User mapping information	The user mapping information.	User mapping information on page C-265

Table C-218 Operations that can be performed from the CIFS Service Maintenance page

Button	Description
Clear User Map Cache File	<p>Can be used to delete the cached user mapping information from the CIFS service environment.</p> <p>The system administrator should delete the user mapping information cached in the CIFS service environment in the following cases:</p> <ul style="list-style-type: none"> User mapping is used and there is unnecessary user information (For deleted users and users who stopped using the service, the user information remains in the cache). The range of user IDs and group IDs that has been set was changed. <p>Note: During degenerated operation, user-mapping information cannot be deleted on the failover-destination node.</p>
Rejoin Active Directory Domain	<p>Can be used to rejoin nodes to the Active Directory domain.</p> <p>When the Active Directory authentication is selected for the CIFS service authentication mode, 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 this case, rejoin the nodes to the Active Directory domain to restore the CIFS share connection.</p> <p>Note: If the selected CIFS service cannot be rejoined to the Active Directory domain, manually delete the computer account left on the Active Directory domain, and then rejoin the CIFS service to the Active Directory domain.</p>
Redefine Active Directory Domain	<p>Can be used to redefine a domain that has a trust relationship.</p> <p>When the Active Directory schema is used for user mapping and you create a new domain that has a trust relationship with the domain that the node is joined to, you can add the new domain by redefining the domain information.</p>

CIFS service information

You can use the **CIFS service information** to see the CIFS service configuration definition.

Table C-219 Information shown in CIFS service information in the CIFS Service Maintenance page

Item	Description
Service status	The status of the CIFS service. Running

Item	Description
	<p>The CIFS service is running normally.</p> <p>Down</p> <p>The service is running in an incomplete state.</p> <p>Failover</p> <p>The resource group has failed over to the other node.</p> <p>Offline</p> <p>The resource group is stopped.</p> <p>Stopped</p> <p>The CIFS service is stopped.</p>
Automatic startup of service	<p>The CIFS service on a physical node that automatically starts when the OS starts or restarts.</p> <p>On</p> <p>The CIFS service automatically starts.</p> <p>Off</p> <p>The CIFS service does not automatically start.</p>
Service information	<p>The information about the CIFS service operating status is shown.</p> <p>The configuration has been modified. Restart the service. Rebooting the OS will not apply the changes.</p> <p>The CIFS service is not stopped after the service configuration is changed. Restart the service. Rebooting the OS will not apply the changes.</p> <p>The configuration has been modified. Start the service. Rebooting the OS will not apply the changes.</p> <p>The CIFS service is stopped after the service configuration is changed. Start the service. Rebooting the OS will not apply the changes.</p> <p>The service is incomplete. Restart the service.</p> <p>The service is running in an incomplete state. If this information appears, restart the service.</p>
SMB protocol	<p>The SMB protocol to be used for gaining access from the CIFS client is displayed.</p> <p>SMB 1.0</p> <p>SMB 1.0 is being used.</p> <p>SMB 2.0</p> <p>SMB 2.0 is being used. SMB 1.0 can also be used.</p> <p>SMB 2.1</p> <p>SMB 2.1 is being used. SMB 1.0 and SMB 2.0 can also be used.</p> <p>SMB 3.0</p>

Item	Description
	SMB 3.0 is being used. SMB 1.0, SMB 2.0, and SMB 2.1 can also be used.
Server comment	A comment on the server name shown on the CIFS client.
Authentication mode	<p>Shows information about the authentication mode and authentication server.</p> <p>Local authentication</p> <p>Local authentication is being used.</p> <p>Workgroup name</p> <p>The work group name.</p> <p>NT domain authentication</p> <p>NT domain authentication is being used.</p> <p>Domain name</p> <p>The domain name.</p> <p>PDC server name</p> <p>The server name of the primary domain controller.</p> <p>BDC server name</p> <p>The server name of the backup domain controller.</p> <p>Domain administrator name</p> <p>The user name of the domain administrator.</p> <p>Active Directory authentication</p> <p>Active Directory authentication is being used.</p> <p>Domain name</p> <p>The domain name of the Active Directory domain.</p> <p>Domain name (NetBIOS)</p> <p>The NetBIOS name of the Active Directory domain.</p> <p>DC server name(s)</p> <p>The server name of the Active Directory domain controller.</p> <p>Domain user name</p> <p>The name of the user for the Active Directory domain controller.</p>
DC server connection status	The connection status of the user authentication server. When there is at least one domain controller server to which you can connect, <code>Connectable</code> is shown.
Host access restrictions	When only certain CIFS clients are allowed access to the CIFS share, the host names or IP addresses of those CIFS clients, or the network addresses of the networks to which the clients belong, are displayed after <code>Allow</code> . Alternatively, when certain CIFS clients are to be denied access to the CIFS share, the host

Item	Description
	<p>names or IP addresses of those CIFS clients, or the network addresses of the networks to which the clients belong, are displayed after <code>Deny</code>.</p> <p>When all CIFS clients are allowed access to the CIFS share, nothing is displayed.</p>
Client time-out	<p>The client timeout value (in minutes). If 0 is shown, automatic disconnection because of a timeout is not performed.</p>
Mapping to guest account	<p>Shows which users will be treated as guests.</p> <p><code>Unregistered users</code></p> <p>Users who have not been registered in the system will be treated as guests.#</p> <p><code>Unregistered users or invalid passwords</code></p> <p>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.#</p> <p><code>Never</code></p> <p>Guest access to the CIFS shares is not permitted.</p>
NetBIOS over TCP/IP	<p>Shows whether to accept access, from CIFS clients, that uses NetBIOS over TCP/IP.</p> <p><code>Use</code></p> <p>The CIFS service accepts access, from CIFS clients, that uses NetBIOS over TCP/IP.</p> <p><code>Do not use</code></p> <p>The CIFS service does not accept access, from CIFS clients, that uses NetBIOS over TCP/IP.</p>
CIFS access log	<p>Shows whether the CIFS access log is collected.</p> <p><code>Use</code></p> <p>The CIFS access log is collected.</p> <p><code>Use (If the CIFS access log file exceeds the max size, do not collect log data.)</code></p> <p>Shown if the log file cannot be moved (when the move destination is not specified, or when the capacity of the file system to which the log file is to be moved has reached the maximum limit), and if you want to stop collecting the CIFS access log at the time when the capacity of the log file reaches the maximum limit.</p> <p><code>Do not use</code></p> <p>The CIFS access log is not collected.</p>
Automatic reloading of CIFS share settings	<p>Shows whether the CIFS share settings are automatically reloaded when they are changed.</p> <p><code>Perform</code></p> <p>The CIFS share settings are automatically reloaded.</p>

Item	Description
	Do not perform The CIFS share settings are not automatically reloaded.
Max. number of CIFS clients accessible simultaneously	The maximum value of CIFS clients that can access one node at one time.
CIFS administrator name(s)	When one or more users and groups have been set as CIFS administrators, this item shows their user and group names.
Current number of CIFS login clients	The number of CIFS clients that are currently logged on.
<p>#: The users to be treated as guests differ depending on the authentication mode that is currently used (the mode shown in Authentication mode):</p> <ul style="list-style-type: none"> • When Local authentication is being used Users who are not registered on the HDI system 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. 	

CIFS default information

You can use the **CIFS default information** to see the configuration that is applied to CIFS shares by default.

Table C-220 Information shown in CIFS default information in the CIFS Service Maintenance page

Item	Description
Guest account access	Shows whether to allow users to access the CIFS shares as guests. Allow Guest access is allowed. Disallow Guest access is not allowed.
Disk synchronization policy	Shows operational settings for write requests from CIFS clients to CIFS shares. At write and close Writing is performed synchronously with a write request or a close request. At close Writing is performed synchronously with a close request. Routine disk flush only

Item	Description
	<p>Writing is performed at a fixed interval, regardless of when write requests and close requests are made.</p> <p>For details about how the system works for each setting, see the notes in Table C-202 Information specified in the CIFS Service Management page (Setting Type: Performance) on page C-236.</p>
Windows® client access policy	<p>The method for processing accesses from Windows clients.</p> <p>Parallel Accesses are processed in parallel.</p> <p>Serial Accesses are processed serially.</p>
CIFS client cache	<p>Shows whether updates to the files in CIFS shares are to be cached on the client.</p> <p>Use Updates are cached on the client.</p> <p>Do not use Updates are not cached on the client.</p>
Read-only client cache for access conflicts	<p>Indicates whether a read-only client cache is used when multiple CIFS clients simultaneously attempt to access a file.</p> <p>Use A read-only client cache is used.</p> <p>Do not use A read-only client cache is not used.</p>
Volume Shadow Copy Service	<p>Displays whether to use Volume Shadow Copy Service to make past versions of files that have been migrated to an HCP system available to CIFS clients.</p> <p>Use Volume Shadow Copy Service is used.</p> <p>Do not use Volume Shadow Copy Service is not used.</p>
Access Based Enumeration	<p>Indicates whether access-based enumeration is used.</p> <p>Use Access-based enumeration is used.</p> <p>Do not use Access-based enumeration is not used.</p>
File timestamp changeable users	<p>The users who can update the timestamps of files in CIFS shares.</p> <p>Write permitted users All users able to write to the files are permitted to update the timestamps.</p> <p>Owner only</p>

Item	Description
	<p>Only file owners are allowed to update the timestamps.</p> <p>Note that this setting is invalid for an advanced ACL file system. Only users who have write permission are permitted to update the timestamps.</p>
<p>Events logged to the CIFS access log</p>	<p>The events that trigger the collection of the CIFS access log.</p> <p>Successful</p> <p>Check marks are shown in the check boxes for the relevant events if you specified the settings so that a successful access corresponding to one of those events triggers the collection of the CIFS access log.</p> <p>Failed</p> <p>Check marks are shown in the check boxes for the relevant events if you specified the settings so that a failed access corresponding to one of those events triggers the collection of the CIFS access log.</p> <p>Each of the following items is used to specify an event (or access):</p> <ul style="list-style-type: none"> • List folder contents • Read data • Create files or write data • Create folders • Delete items • Read permissions • Change permissions • Change ownership • Rename items • Connect to or disconnect from shares
<p>SMB encryption</p>	<p>Displays whether the communication with the CIFS client is to be encrypted when you use SMB 3.0.</p> <p>Auto</p> <p>Communication with the client is to be encrypted only when the client supports encryption.</p> <p>Mandatory</p> <p>Communication with the client is always to be encrypted.</p> <p>Disable</p> <p>Communication with the client is not to be encrypted.</p>

User mapping information

You can use the **User mapping information** to see the user mapping information.

Table C-221 Information shown in User mapping information in the CIFS Service Maintenance page

Item	Description
User mapping usage type	<p>The type of user mapping being used.</p> <p>RID</p> <p>Shown when user mapping uses RIDs. For other information that is shown, see Table C-222 Information shown in User mapping information in the CIFS Service Maintenance page (when user mapping uses RIDs) on page C-266.</p> <p>LDAP</p> <p>Shown when user mapping uses LDAP. For other information that is shown, see Table C-223 Information shown in User mapping information in the CIFS Service Maintenance page (when user mapping uses LDAP) on page C-266.</p> <p>Active Directory schema</p> <p>Shown when user mapping uses the Active Directory schema. For other information that is shown, see Table C-224 Information shown in User mapping information in the CIFS Service Maintenance page (when user mapping uses the Active Directory schema) on page C-268.</p> <p>Not used</p> <p>Shown when user mapping is not used.</p>

Table C-222 Information shown in User mapping information in the CIFS Service Maintenance page (when user mapping uses RIDs)

Item	Description
Range of UIDs and GIDs	The range of user IDs and group IDs mapped by using RIDs.
Settings for each domain	<p>The range of user IDs and group IDs set for each domain.</p> <p>When two or more ranges have been set, they are shown in ascending order of the minimum value for the range of user IDs and group IDs.</p>

Table C-223 Information shown in User mapping information in the CIFS Service Maintenance page (when user mapping uses LDAP)

Item	Description
LDAP server name	The host name or IP address of the LDAP server.
LDAP server port number	The port number of the LDAP server.
LDAP server root DN	The identification name of the LDAP server root as a distinguished name.

Item	Description
LDAP user map DN	The identification name for which you added the user mapping account of the LDAP server as a distinguished name.
LDAP administrator DN	The identification name of the LDAP server administrator as a distinguished name.
Allocation method	<p>The method for allocating user IDs and group IDs.</p> <p>Automatic IDs are allocated automatically.</p> <p>Manual IDs are allocated manually.</p>
Range of UIDs[#]	The range of user IDs mapped by using LDAP.
Largest currently used UID[#]	<p>The largest user ID within the range of user IDs that have already been assigned in the HDI system.</p> <p>Depending on the status of user mapping usage, the following information might be shown:</p> <p>Not used, or less than the minimum UID used. No user IDs have been assigned, or the smallest assigned user ID is smaller than the minimum value set in Range of UIDs.</p> <p>Cannot be got from LDAP server. Check the LDAP server settings and CIFS service configuration in service. The largest ID could not be obtained from the LDAP server for user mapping. Check the user mapping settings and the operating status of the LDAP server.</p>
Range of GIDs[#]	The range of group IDs mapped by using LDAP.
Largest currently used GID[#]	<p>The largest group ID within the range of group IDs that have already been assigned in the HDI system.</p> <p>Depending on the status of user mapping usage, the following information might be shown:</p> <p>Not used, or less than the minimum GID used. No group IDs have been assigned, or the smallest assigned group ID is smaller than the minimum value set in Range of GIDs.</p> <p>Cannot be got from LDAP server. Check the LDAP server settings and CIFS service configuration in service. The largest ID could not be obtained from the LDAP server for user mapping. Check the user mapping settings and the operating status of the LDAP server.</p>
#: This item is shown only when user IDs and group IDs are allocated automatically.	

Table C-224 Information shown in User mapping information in the CIFS Service Maintenance page (when user mapping uses the Active Directory schema)

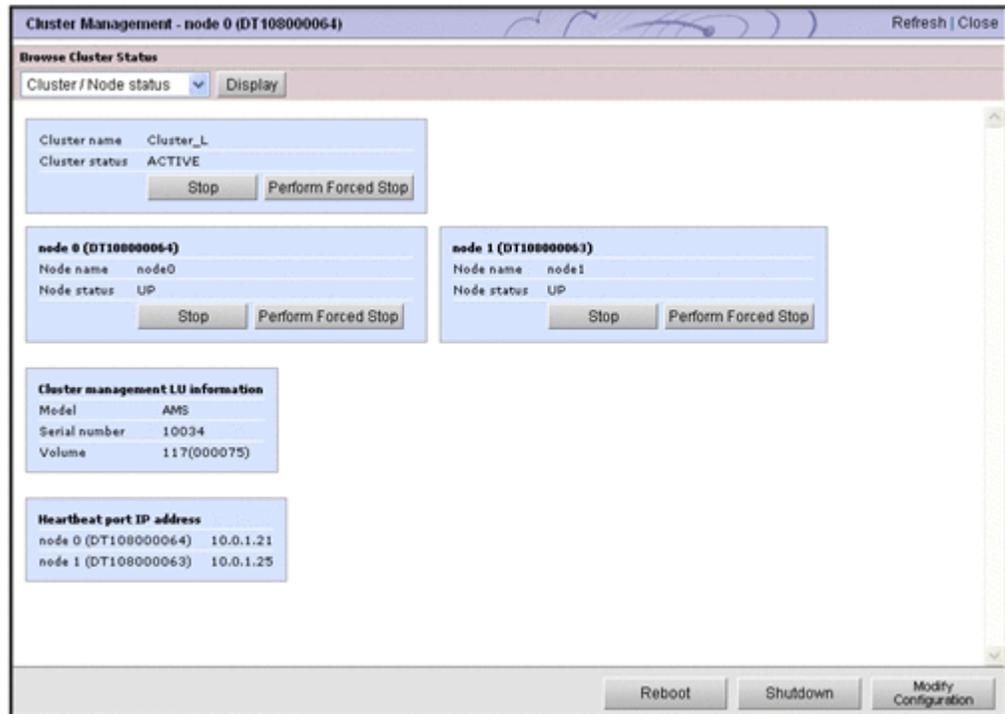
Item	Description
Name service switch	The name service switch being used. Microsoft® Services for Unix Microsoft services for Unix is used. Using LDAP as a network information service (RFC2307) The RFC2307 schema is used.
Joined domain name	The name of the domain that the node is joined to.
Trusted domain name	The names of the domains that have a trust relationship with the domain that the node is joined to. - is shown if there are no such domains.

Cluster Management dialog box

With **Cluster Management** dialog box, clusters, nodes, and resource groups can be managed.

To open the **Cluster Management** dialog box, click **Cluster Management** in the **Advanced** subtab of the **Settings** tab in the *physical-node* window ([physical-node window on page C-91](#)). If the cluster configuration is not defined in the targeted Physical Node, the **Define Cluster Configuration** page is shown initially, when the **Cluster Management** dialog box is shown.

When the cluster is configured, the **Browse Cluster Status** page (for Cluster / Node status) is shown.



Define Cluster Configuration page

You can define the cluster configuration for physical nodes.

You must complete this work before setting the information needed to start the HDI system.



Note:

- Make sure that the IP addresses shown in **Fixed IP address** in **node 0** and **node 1** match the IP addresses assigned to the nodes. If the IP address for **node 0** is shown in **node 1** and vice versa, close the **Define Cluster Configuration** page, select the other physical node from the object tree, and then show the page again.
- In the following cases, you must perform a new installation of the OS, and then newly define the cluster configuration.
 - When performing any operation on the nodes in the cluster before the processing has finished (for example, when restarting the OS or disconnecting a cable from a management port) after you click **OK**.
 - When the message KAQM06004-E, KAQM06018-E, or KAQM14101-E is shown after you click **OK**.
- When the message KAQM06107-E or KAQM06112-E is shown, newly define the cluster configuration.
- After defining the cluster configuration, implement the setup of the interface and the network with the **Network & System Configuration** dialog box.

If the cluster configuration is not defined in the targeted Physical Node, the **Define Cluster Configuration** page is shown initially, when the **Cluster Management** dialog box is shown.

Table C-225 Information specified in the Define Cluster Configuration page

Item	Description
Cluster name	<p>Specify the name of the cluster that consists of two nodes. The specified name is used as the processing node name. When multiple processing nodes are managed by the management server, make sure that names are not duplicated.</p> <p>You can use a maximum of 22 characters. You can use any alphanumeric character, hyphen (-), period (.), forward slash (/), colon (:), at mark (@), and underscore (_). However, you cannot use an underscore (_) as the first character.</p> <p>Note that you cannot specify the name 0 or words reserved by the system.#</p>
Node name	<p>Specify the node name. A <i>node name</i> is the name of an element that corresponds to each node in the cluster. This node name is different from the host name.</p> <p>You can use a maximum of 22 characters. You can use any alphanumeric character, hyphen (-), period (.), colon (:), at mark (@), and underscore (_). You cannot use the hyphen (-) and underscore (_) as the first character.</p> <p>Note that you cannot specify the name 0 or words reserved by the system.#</p>
Network address	<p>Select the network address of the heartbeat port from the addresses shown in the drop-down list (10.0.1.0, 192.168.1.0, 192.168.234.0, 172.23.212.0, or 10.197.182.0).</p>
LUs	<p>Select the LU to be used as the cluster management LU. The model and serial number of the storage system in which a usable LU exists, and the LDEV number and capacity (units: GB) of the LU are shown. Select one LU with a capacity of approximately 70 GB, and then click Select. Note that the cluster management LU must have a capacity of at least 70 GB.</p> <p>Note that the LU capacities are rounded down to the nearest three decimal places.</p> <p>Also note that the following LUs are not shown:</p> <ul style="list-style-type: none"> • An LU for which an error has occurred on the FC path • A blocked LU <p>Enable the mapping guard for the cluster management LU. For the LU to be used as the cluster management LU, if you change the mapping of the LUN (host LU number) and the LDEV number to be set for the storage system, the HDI system will not function correctly. Do not change this mapping. You can set the mapping guard by using Storage Navigator, or version 6.5 or later of Hitachi Storage Navigator Modular 2.</p>

Item	Description
	To use a virtual LU as a cluster management LU, confirm with the storage system administrator whether full allocation or full capacity mode for Dynamic Provisioning is enabled.
#: For details about reserved words, see List of reserved words on page F-2 .	

Browse Cluster Status page

On the **Browse Cluster Status** page, you can view error information about the cluster, nodes, resource groups.

When the cluster is configured, the **Browse Cluster Status** page is shown initially, when the **Cluster Management** dialog box is shown.

Select the information to be viewed with the drop-down list, and click **Display**.

Table C-226 Information selected with the drop-down list on Browse Cluster Status page

Item	Description	See
Cluster / Node status	You can manage the clusters and nodes that make up the clusters.	Browse Cluster Status page (for Cluster / Node status) on page C-271
Resource group status	You can manage a resource group that is running on the nodes.	Browse Cluster Status page (for Resource group status) on page C-278

Browse Cluster Status page (for Cluster / Node status)

On the **Browse Cluster Status** page (for `Cluster / Node status`), you can start, stop or perform a forced stop on the cluster or the node, or you can restart or shut down the OS.

Before starting or stopping the cluster

In the initial status after installation, the cluster is stopped. A system administrator must set up the network and interface information, and then start the cluster by using the **Browse Cluster Status** page (for `Cluster / Node status`) of the **Cluster Management** dialog box.

Also, you 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.

When a cluster is stopped while resource groups are running, the resource groups will be in `Online Ready/No error` status. When a cluster is started while resource groups are in this status, the resource groups will automatically start. After processing finishes, it might take a while before you

can perform resource group related operations (until the `Online/No error` status is reached).

The system administrator needs to make sure that no partial blockage has occurred in a resource group during the resource group startup process. On the **List of RAS Information** page (for `List of messages`) of the **Check for Errors** dialog box, check whether the message KAQG72006-E or KAQM35001-E has been output to the system messages. For the action to take if the message has been output, see the *Error Codes* manual.

Do not stop and start a cluster repeatedly. If you perform these operations repeatedly, the KAQM06018-E message might be output when you stop the cluster. In this case, stop the cluster again.



Note: If you work with maintenance personnel to perform maintenance, make sure that the maintenance personnel have started the OSs on both nodes, and then start the cluster.

If you start a cluster when either of the OSs has not completed startup, startup processing for that OS might be canceled (reset), and a dump file might be output. If startup processing for an OS is stopped, the message KAQG72010-E is output, the resource group is failed over, and then services start.

Before starting or stopping the node

During normal operation, a resource group run on each node. When a failover occurs, the resource group that were running on the failed over node are switched to the alternate node. The resource group run on the alternate node in addition to the resource group that were running on that node before the failover.

When a node is started while a resource group is in the `Online Ready/No error` status, the resource group is automatically started. After processing finishes, it might take a while before you can perform resource group related operations (until the `Online/No error` status is reached).

The system administrator needs to make sure that no partial blockage has occurred in a resource group during the resource group start-up process. On the **List of RAS Information** page (for `List of messages`) of the **Check for Errors** dialog box, check whether the message KAQG72006-E has been output to the system messages. For the action to take if the message has been output, see the *Error Codes* manual.

Do not stop and start a node repeatedly. If you perform these operations repeatedly, the KAQM06018-E message might be output when you stop the node. In this case, forcibly stop the node.

To open the **Browse Cluster Status** page (for `Cluster / Node status`), select **Cluster / Node status** in the drop-down list of the **Browse Cluster Status** page in the **Cluster Management** dialog box ([Cluster Management dialog box on page C-268](#)), and then click **Display**.

Table C-227 Cluster and node information shown in the Browse Cluster Status page (for Cluster / Node status)

Item	Description
Cluster name	Name of the cluster
Cluster status	Status of the cluster:#1 ACTIVE The cluster is running normally. INACTIVE The cluster is stopped. UNKNOWN#2#3 The status cannot be determined. DISABLE The failover functionality is disabled because of an error.
Node name	Name of the nodes in the cluster
Node status	Status of the nodes in the cluster:#1 UP The node is running normally. INACTIVE The node is stopped. DOWN The OS ended abnormally and the node is stopped. UNKNOWN#2#3 The status cannot be determined.
Cluster management LU information	The cluster management LU information. Model The model of the storage system in which the LU exists. Serial number The serial number of the storage system in which the LU exists. Volume The LDEV number of the LU.
Heartbeat port IP address	The IP address of the heartbeat port for each node.
<p>#1: If an error occurs in the system, the status of clusters and nodes might not be shown. In this case, collect the error information and contact the maintenance personnel. For details about how to collect error information, see the <i>Cluster Troubleshooting Guide</i>.</p> <p>#2: After performing a stop or forced stop for a node, if you select the stopped node (physical node) in the navigation area, and then show the Browse Cluster Status page (for Cluster / Node status), the status of the cluster and the other node is shown as UNKNOWN. In this state, you cannot check the status of the cluster and the other node. To</p>	

Item	Description
	<p>check the status of the cluster and the other node, select the operating node (the other physical node) in the navigation area, and then show the Browse Cluster Status page (for <i>Cluster / Node status</i>).</p> <p>#3: UNKNOWN is also shown when a cluster starts up. Note that, when a cluster starts up, UNKNOWN is shown until both OSs on the nodes making up the cluster complete startup (for up to 10 minutes).</p>

Table C-228 Operations that can be performed from the Browse Cluster Status page (for Cluster / Node status)

Button	Description	See
Stop	<p>It is shown, when a cluster or a node has been started.</p> <p>If you click Stop for a cluster, it stops all the nodes in the cluster, and the resource group active on each node.</p> <p>When you click Stop for a node, it stops the node, and begins failover for the resource group active on the different node. Depending on the usage status of the node where the resource group that you want to fail over is operating (for example, the number of file systems, usage status of the volume manager, or the number of NFS shares), the processing time until failover finishes might vary between 10 minutes and 50 minutes.</p> <p>When the processing has finished, make sure that the operations have finished normally with Cluster status and Node status in the Browse Cluster Status page (for <i>Cluster / Node status</i>). For details about the actions to take if an error occurs, see the <i>Cluster Troubleshooting Guide</i>.</p>	N/A
Perform Forced Stop	<p>It is shown, when a cluster or a node has been started.</p> <p>When you click Perform Forced Stop 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 the resource group active on each node.</p> <p>When you click Perform Forced Stop for a node, the system ignores any errors that occurred during processing, performs a forced stop for the node, and begins failover for the resource group active on the node. Depending on the usage status of the node where the resource group that you want to fail over is operating (for example, the number of file systems, usage status of the volume manager, or the number of NFS shares), the processing time until failover finishes might vary between 10 minutes and 50 minutes.</p> <p>Some services might remain running after a forced stop 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 might start. Therefore, after performing a forced stop for a cluster, reboot the OS on both nodes before starting the cluster. Also, if the resource group has not been moved to the other node when one</p>	N/A

Button	Description	See
	<p>node is forcibly stopped, reboot the OS before you start the node.</p> <p>Performing a forced stop for a cluster might take an extended period of time. When stop processing does not finish within 30 minutes, an uncorrectable error might have occurred. In this case, contact maintenance personnel.</p> <p>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 about the actions to take if an error occurs while stopping or starting a cluster or node, see the <i>Cluster Troubleshooting Guide</i>.</p>	
Start	<p>It is shown when a cluster or a node has been stopped.</p> <p>If you click Start for a cluster, it starts all the nodes in the cluster. When a node starts, its resource group can be activated.</p> <p>If you click Start for a node, the node starts, and makes the resource group available for starting.</p> <p>When the processing has finished, make sure that the operations have finished normally with Cluster status and Node status in the Browse Cluster Status page (for <i>Cluster / Node status</i>). For details about the actions to take if an error occurs, see the <i>Cluster Troubleshooting Guide</i>.</p>	N/A
Reboot	<p>You can reboot the OS of the physical node selected in the navigation area.</p> <p>Normally, the system administrator needs to reboot the OS for the following operations:</p> <ul style="list-style-type: none"> • Setting new information for the LDAP server for user authentication, or deleting all information for the LDAP server for user authentication • Setting, changing, or deleting information for the NIS server • Setting or changing the NTP server or the time zone • Changing the node time <p>If the OS needs to be rebooted for any other reason, contact maintenance personnel first.</p> <p>Before the OS is rebooted, the node must be stopped. In the Browse Cluster Status page (for <i>Cluster / Node status</i>) of the Cluster Management dialog box, verify that the node at which the OS is to be rebooted is inactive.</p> <p>If you click Reboot, the Reboot page is shown. Select Start the node after a reboot or Do not start the node after a reboot. If you select Start the node after a reboot, specify whether you start the resource group (and fail back if the resource group is failed over), and then click Reboot.</p>	N/A

Button	Description	See
	<p>If you did not start the node or fail back a resource group, in 5 minutes after rebooting the OS, open the Cluster Management dialog box again, start the node, and then fail back the resource group.</p> <p>If the host name specified for the routing target or gateway cannot be resolved, the routing information might not be restored after rebooting the OS. If a host name is specified for the routing target or gateway, make sure that the host name can be resolved before rebooting the OS. If the routing information cannot be restored, see the <i>Cluster Troubleshooting Guide</i>, and take appropriate action.</p>	
Shutdown	<p>You can shut down the OS of the physical node selected in the navigation area.</p> <p>Notes:</p> <ul style="list-style-type: none"> To start the OS, press the power switch on the node chassis. For details about how to shut down both OSs on the processing node at the same time, see File Servers tab on page C-79. 	N/A
Modify Configuration	Cluster configuration definition can be changed.	Modify Cluster Configuration page on page C-276

Modify Cluster Configuration page

You can use the **Modify Cluster Configuration** page to change the cluster configuration definition.



Note: Save the system configuration in case the attempt to change the cluster configuration definition fails. When you change a cluster configuration definition, the cluster and all resource groups in it must be stopped. If you want to change a cluster configuration definition while operating, you must first stop the resource groups, and then stop the cluster. Next, change the cluster configuration definition, and then start the cluster and resource groups.

Depending on the usage status of the nodes in the cluster (for example, the number of file systems, usage status of the volume manager, or the number of NFS shares), the processing time to save the setting contents might vary between 10 minutes and 50 minutes. After you click **OK**, do not perform any operation on the nodes in the cluster until the processing has finished (for example, do not restart the OS or disconnect a cable from a management port). If you perform any operation on a node before this processing is completed, you must perform either of the following operations:

- Perform a new installation of the OS, and then re-define the cluster configuration
- Restore the system by using a system configuration file

If you move to the **Modify Host Name** page by clicking **Modify Host Name** without clicking **OK**, the cluster configuration will not be changed.

To open the **Modify Cluster Configuration** page, click **Modify Configuration** of the **Browse Cluster Status** page (for *Cluster / Node status*) in the **Cluster Management** dialog box ([Cluster Management dialog box on page C-268](#)).

Table C-229 Information changed in the Modify Cluster Configuration page

Item	Description
Cluster name	Specify the name of the cluster that consists of two nodes. The specified name is used as the processing node name. When multiple processing nodes are managed by the management server, make sure that names are not duplicated.
Node name	Specify the node name. A <i>node name</i> is the name of an element that corresponds to each node in the cluster. This node name is different from the host name.

Table C-230 Operations that can be performed from the Modify Cluster Configuration page

Button	Description	See
Modify Host Name	Host name of the node can be changed.	Modify Host Name page on page C-277

Modify Host Name page

You can use the **Modify Host Name** page to change the host names of the nodes.



Note: Save the system configuration in case the attempt to change the host name fails. Notify the maintenance personnel and other administrators not to operate both nodes in the cluster until the tasks are completed.

Until you make sure that you can show the **Cluster Management** dialog box from the **Settings** tab, do not perform any operation on the nodes in the cluster (for example, do not restart the OS or disconnect a cable from a management port). If you perform any operation on a node before you make sure that you can show the **Cluster Management** dialog box again, or if an error occurs while setting a host name, you must perform either of the following operations:

- Perform a new installation of the OS, and then re-define the cluster configuration definition.
- Restore the system by using a system configuration file.

Table C-231 Information specified in the Modify Host Name page

Item	Description
Host name	<p>Specify a host name for the node. The host name of each node must be unique. Note that upper-case and lower-case letters are set exactly as specified, but names that differ only in case are assumed to be the same.</p> <p>The specified name is also used as the host name of the physical node.</p> <p>The host name can have a maximum of 15 characters. You can use alphanumeric characters including hyphens (-). The host name must begin with an alphabetic letter, and must not end with a hyphen (-).</p> <p>Note that you cannot specify system-reserved words in upper case or lower case. For details about reserved words, see List of reserved words on page F-2.</p>

Browse Cluster Status page (for Resource group status)

You can use the **Browse Cluster Status** page (for `Resource group status`) to manage a resource group that is running on the nodes.

To open the **Browse Cluster Status** page (for `Resource group status`), select **Resource group status** in the drop-down list of the **Browse Cluster Status** page in the **Cluster Management** dialog box ([Cluster Management dialog box on page C-268](#)), and then click **Display**.

Table C-232 Resource group information shown in the Browse Cluster Status page (for Resource group status)

Item	Description		
Resource group	Name of a resource group Automatically allocated by the system.		
Resource group status	<p>Status and error information about a resource group, shown in the following format:</p> <p><i>resource-group-status/error-information</i></p> <table border="1"> <tbody> <tr> <td><i>resource-group-status</i></td> <td> <p>Online Ready#</p> <p>The resource group cannot start because the cluster is inactive, or an error was detected when the cluster was stopping.</p> <p>Initializing</p> <p>The resource group is initializing.</p> <p>Discovery (exclusivity)</p> <p>Online processing is being performed for the resource group before operations begin.</p> <p>Online Pending</p> <p>The resource group is starting.</p> <p>Online</p> </td> </tr> </tbody> </table>	<i>resource-group-status</i>	<p>Online Ready#</p> <p>The resource group cannot start because the cluster is inactive, or an error was detected when the cluster was stopping.</p> <p>Initializing</p> <p>The resource group is initializing.</p> <p>Discovery (exclusivity)</p> <p>Online processing is being performed for the resource group before operations begin.</p> <p>Online Pending</p> <p>The resource group is starting.</p> <p>Online</p>
<i>resource-group-status</i>	<p>Online Ready#</p> <p>The resource group cannot start because the cluster is inactive, or an error was detected when the cluster was stopping.</p> <p>Initializing</p> <p>The resource group is initializing.</p> <p>Discovery (exclusivity)</p> <p>Online processing is being performed for the resource group before operations begin.</p> <p>Online Pending</p> <p>The resource group is starting.</p> <p>Online</p>		

Item	Description	
		<p>The resource group is active.</p> <p>Online Maintenance</p> <p>Automatic failover is impossible because monitoring is disabled.</p> <p>Offline Pending</p> <p>The resource group is stopping.</p> <p>Offline#</p> <p>The resource group is stopped.</p> <p>Internal Error</p> <p>An internal error was detected. Contact the maintenance personnel.</p>
	<p><i>error-information</i></p>	<p>No error</p> <p>No errors occurred.</p> <p>Internal error - not recoverable</p> <p>An unrecoverable internal error occurred. Contact the maintenance personnel.</p> <p>Monitor activity unknown</p> <p>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.</p> <p>No available nodes OR No available nodes in failure domain after monitor failure</p> <p>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.</p> <p>Node not available (exclusivity)</p> <p>Failover is impossible because the Node status of the alternate node is not UP. 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.</p> <p>Node unknown</p> <p>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.</p> <p>Split resource group (exclusivity)</p> <p>A duplicate resource group is active in the cluster. Perform a forced stop for the</p>

Item	Description
	<p>cluster, and then request the maintenance personnel to shut down and restart the OSs of the nodes in the cluster.</p> <p>srmd executable error</p> <p>An error occurred during start or stop processing. Perform a forced stop and fix the problem.</p>
Running node	Name of the node on which the resource group is running
<p>#: This status is shown even when the cluster status is <code>DISABLE</code>. When <code>Online Ready</code> or <code>Offline</code> is shown, also check the cluster status in the Browse Cluster Status page (for <code>Cluster / Node status</code>).</p>	

Table C-233 Operations that can be performed from the Browse Cluster Status page (for Resource group status)

Button	Description
Start	<p>Selected resource groups can be started.</p> <p>Note:</p> <p>When you start a resource group, make sure that the data port can communicate with the List of Data Ports page of Network & System Configuration dialog box.</p> <p>After starting a resource group, check whether a partial blockage has occurred in the resource group. On the List of RAS Information page (for <code>List of messages</code>) of the Check for Errors dialog box, check whether the message <code>KAQG72006-E</code> has been output to the system messages. For the action to take if the message has been output, see the <i>Error Codes</i> manual.</p>
Stop	Selected resource groups can be stopped.
Perform Forced Stop	<p>A forced stop is performed for the selected resource group, while ignoring all the errors occurring during processing.</p> <p>Note:</p> <p>Some services might 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 might 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.</p> <p>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 retrying this operation, you must determine the cause of the problem from the error information and take appropriate action. For details about the actions to take if an error occurs while stopping or starting a resource group, see the <i>Cluster Troubleshooting Guide</i>.</p>
Monitor	Monitoring of selected resource groups can be restarted.

Button	Description
Cancel Monitoring	Selected resource groups can be excluded from the monitoring target. If a LAN cable is handled incorrectly during normal operation, the HDI system assumes that an error has occurred and automatically fails over. By temporarily excluding resource groups from the monitoring target when performing maintenance of services provided by the resource group, failover can be prevented.
Change Execution Node	<p>Selected resource groups can be moved to other nodes (failover or failback).</p> <p>Note:</p> <ul style="list-style-type: none"> • When performing a failover as instructed by maintenance personnel for recovery from a port error, you need to perform operations from the management LAN even when the HDI system is managed from the management console located on the front-end LAN. • Make sure that the Node status of the node to which the resource group is moving is UP in the Browse Cluster Status page (for <code>Cluster / Node status</code>). • Make sure that the Resource group status of the resource group being moved is Online / No error or Online Maintenance / No error in the Browse Cluster Status page (for <code>Resource group status</code>). • The selected resource group moves to the other node. Depending on the usage status of the node 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 shares), the processing time until failover finishes might vary between 10 minutes and 50 minutes. • When failover or failback occurs, the system administrator needs to check whether a partial blockage has occurred in the resource group. On the List of RAS Information page (for <code>List of messages</code>) of the Check for Errors dialog box, check whether message KAQG72006-E has been output to the system messages. For the action to take if the message has been output, see the <i>Error Codes</i> manual.



Note: When the processing has finished, make sure that the operations have finished normally with **Resource group status** in the **Browse Cluster Status** page (for `Resource group status`). For details about the actions to take if an error occurs, see the *Cluster Troubleshooting Guide*.

Proxy Server Settings window

You can use the Proxy Server Settings window to view proxy server information in the Proxy Server Settings window.

To open the Proxy Server Settings window, click **Proxies** in the **Advanced** subtab of the **Settings** tab in the *physical-node* window ([physical-node window on page C-91](#)).

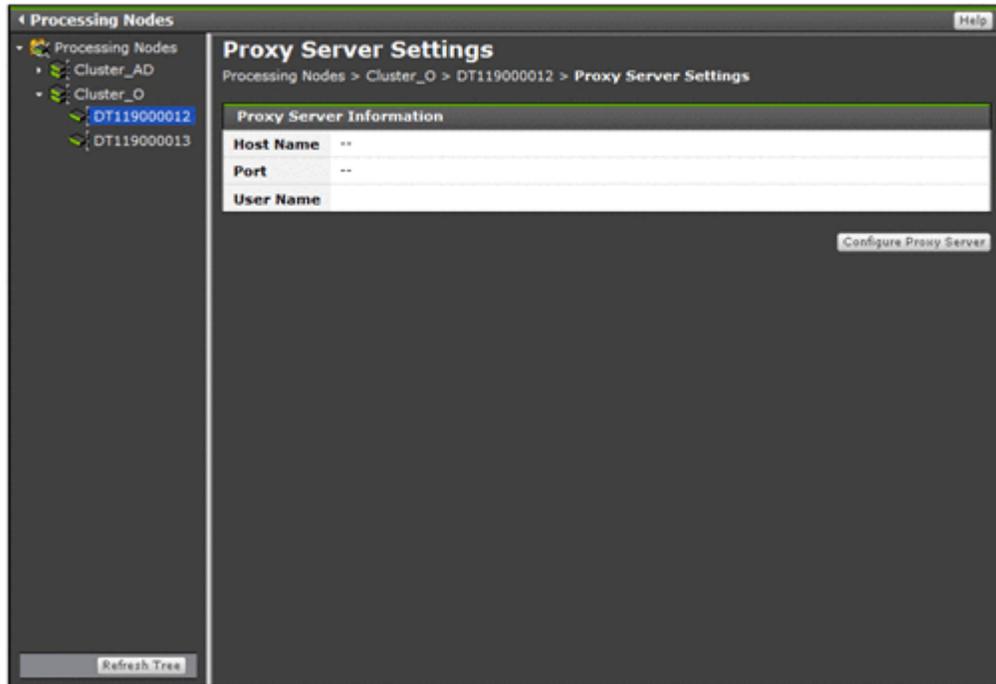


Table C-234 Proxy server information shown in the Proxy Server Settings window

Item	Description
Host Name	The proxy server host name.
Port	The port number used in the proxy server.
User Name	The user name used for authentication on the proxy server.

Table C-235 Operations that can be performed from the Proxy Server Settings window

Button	Description	See
Configure Proxy Server	Sets proxy server information.	Configure Proxy Server dialog box on page C-282

Configure Proxy Server dialog box

You can use the **Configure Proxy Server** dialog box to set information for the proxy server that is used for communication between an HDI system and an HCP system.

To open the **Configure Proxy Server** dialog box in the Proxy Server Settings window ([Proxy Server Settings window on page C-281](#)), click **Configure Proxy Server**.

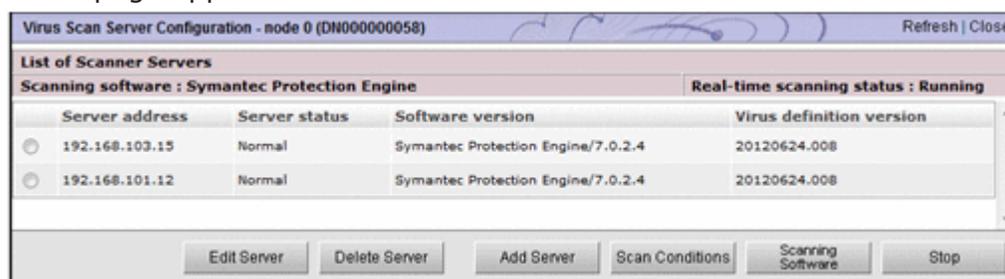
Table C-236 Proxy server information specified in the Configure Proxy Server dialog box

Item	Description
Proxy server	When setting up the proxy server, select the Use check box. When deleting proxy server information, clear the Use check box.
Host name	Specify the proxy server host name. An IP address can be specified instead of a host name.
Port	Specify the port number used for the proxy server.
User authentication	When users are authenticated by the proxy server, select the Use check box. When deleting user information, clear the Use check box.
User name	Specify the user name used for authentication by the proxy server.
Password	Specify the user password used for authentication by the proxy server.

Virus Scan Server Configuration dialog box

You can use the **Virus Scan Server Configuration** dialog box to manage the real-time virus scanning functionality. This functionality must be managed for each node in the cluster.

To open the **Virus Scan Server Configuration** dialog box, click **Virus Scan Server Configuration** in the **Advanced** subtab of the **Settings** tab in the *physical-node* window ([physical-node window on page C-91](#)). After the **Virus Scan Server Configuration** dialog box is shown, the **List of Scanner Servers** page appears.



List of Scanner Servers page

You can use the **List of Scanner Servers** page to view information about real-time scanning that is set for physical nodes.

The **List of Scanner Servers** page appears first when the **Virus Scan Server Configuration** dialog box is shown.

Table C-237 Information shown in the List of Scanner Servers page

Item	Description
Scanning software	The name of the scan software that is used. If a scan software is not set, - is shown.
Real-time scanning status	<p>The real-time scanning status.</p> <p>Running Real-time scanning is enabled.</p> <p>Stopped Real-time scanning is disabled.</p>
Server address	Shows either the IP address, domain name, or host name of the scan server. Shows the content of the Server address specified in the Add Scanner Server page.
Server status	<p>The status of the scan server.</p> <p>- Real-time scanning is disabled.</p> <p>Normal The scan server is functioning normally.</p> <p>Blocked (Server not found) The scan server could not be found. Make sure that the IP address, domain name, or host name of the scan server is correct.</p> <p>Blocked (Access is impossible) The port numbers set at the HDI system and the scan server are different, the real-time virus scanning service is not available, or the scanning software that is specified for the HDI system is different from the software on the scan server. Verify that the IP address, domain name, 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. Verify that the scanning software settings for the HDI system are correct.</p> <p>Blocked (Time-out) The scan server timed out. Make sure that no network failure has occurred.</p> <p>Blocked (Version conflict) The protocol versions for the HDI and the scan server are not compatible. Obtain all the log data, and then inform maintenance personnel.</p> <p>Blocked (License expired) The scan software license that was installed at the scan server is invalid. Verify that the scanning software license has been set up.</p> <p>Blocked (Scanner server error) A failure occurred in the scan server. Recover the scan server from the failure.</p>

Item	Description
	<p>Blocked (Under registration)</p> <p>The information about the registered scan server is being applied to an HDI system.</p> <p>Wait for several minutes, and then click Refresh to update the information shown.</p> <p>Blocked (Invalid protocol)</p> <p>The communication protocol is different from the one used by Hitachi Server Protect Agent that is installed on the scan server.</p> <p>Check the version of the installed Hitachi Server Protect Agent, and then install the correct version.</p> <p>Blocked (Scanning software is not installed)</p> <p>Scan software is not installed on the scan server. Install scan software.</p> <p>Blocked (Scanning software service has stopped)</p> <p>The service of the scan software on the scan server is stopped. Start the service.</p> <p>Blocked (Access user info. is not registered)</p> <p>The information of the user for accessing CIFS shares is not registered on the scan server. Register the information.</p> <p>Blocked (Access user info. is invalid)</p> <p>The information of the user for accessing CIFS shares registered on the scan server is incorrect. Correct the information.</p> <p>Deleting</p> <p>Operation for deleting the scan server is performed, but some CIFS clients are using the scan server. The scan server will be deleted when the CIFS clients finish using the scan server.</p> <p>Error (System failure)</p> <p>A failure occurred in the HDI system, or an attempt to update the status failed. Wait for the time specified for Server monitoring interval on the Scan Conditions page to pass, and then check the status again.</p> <p>If the status still cannot be updated, obtain all the log data, and then inform maintenance personnel.</p>
Software version	<p>Shows the version of the scan software that is installed on the scan server.</p> <p>If the scan software being used is a Trend Micro product, or if this information cannot be obtained, a hyphen (-) is displayed.</p>
Virus definition version	<p>Shows the version of the virus definition file used on the scan server.</p> <p>If the scan software being used is a Trend Micro product, or if this information cannot be obtained, a hyphen (-) is displayed.</p>



Note: The status of the scan server is periodically monitored. When recovery of a blocked scan server is confirmed, the connection is unblocked automatically.

Table C-238 Operations that can be performed from the List of Scanner Servers page

Button	Description	See
Edit Server	Edits the information for a scan server.	Edit Scanner Server page on page C-286
Delete Server	Deletes a scan server. Select the server you want to delete in the options, and then click Delete Server .	N/A
Add Server	Registers a scan server.	Add Scanner Server page on page C-287
Scan Conditions	Sets the conditions for real-time scanning to be requested to a scan server.	Scan Conditions page on page C-287
Scanning Software	Sets the scan software to use.	Scanning Software page on page C-293
Start/Stop	Enables or disables real-time scanning. In the HDI system, when real-time virus scanning is enabled, scanning is performed on the files targeted by a read or write request from a CIFS client. The system administrator needs to enable or disable real-time virus scanning for each node to ensure that all nodes within a cluster are configured in the same way. Before enabling or disabling real-time virus scanning, note the following: <ul style="list-style-type: none"> • After you enable or disable the real-time scanning, restart the CIFS service. • If you disable real-time virus scanning during scan processing, the scan processing might end with an error. 	N/A
Note: N/A = Not applicable.		
Note: These operations must be performed for each node in the cluster.		

Edit Scanner Server page

You can change the scan server information registered in the physical nodes. Note that you need to install the same version of the same virus scan software product on all scan servers registered within a cluster, and configure the software in the same way.

To open the **Edit Scanner Server** page, select a scan server, and then click **Edit Server** in the **List of Scanner Servers** page of the **Virus Scan Server Configuration** dialog box ([Virus Scan Server Configuration dialog box on page C-283](#)).

Table C-239 Information specified in the Edit Scanner Server page

Item	Description
Server address	Specify the IP address, domain name, or host name of the scan server.
Port number	Specify a port number of the scan server.

Add Scanner Server page

You can use the **Add Scanner Server** page to register a scan server for each physical node.



Note:

- Make sure that the scan server to be registered has been prepared in the network. For details about how to set up the scan server environment, see the *Installation and Configuration Guide*.
- In the HDI system, you do not need to register the same scan server in each node within a cluster, but you can register different scan servers in the same cluster. However, you need to install the same version of the same virus scan software product on all scan servers registered within a cluster, and configure the software in the same way.

To open the **Add Scanner Server** page, click **Add Server** on the **List of Scanner Servers** page in the **Virus Scan Server Configuration** dialog box ([Virus Scan Server Configuration dialog box on page C-283](#)).

Table C-240 Information specified in the Add Scanner Server page

Item	Description
Server address	Specify the IP address, domain name, or host name of the scan server.
Port number	Specify a port number of the scan server, from 1024 to 65535.

Scan Conditions page

You can use the **Scan Conditions** page to set the conditions for real-time scanning to be requested to a scan server.



Note:

- Set the scanning conditions for each node so that each node within the cluster has the same settings.
- At the scan server, scan requests are received from the HDI, and real-time virus scanning is run in accordance with the scan server settings. For example, if the extension of a file for which a scan request was received from the HDI is not set as a scan target, real-time virus scanning will not

be run. For details about how to set up the scan server environment and scan software configuration, see the *Installation and Configuration Guide*.

To open the **Scan Conditions** page, click **Scan Conditions** on the **List of Scanner Servers** page in the **Virus Scan Server Configuration** dialog box ([Virus Scan Server Configuration dialog box on page C-283](#)).

Table C-241 Information specified in the Scan Conditions page

Item	Description
Scan timing ^{#1}	<p>Select the timing of scans in the options.</p> <p>Read and write Runs a scan when the CIFS client has read or written files.</p> <p>Read only Runs a scan when the CIFS client has read files.</p> <p>Write only Runs a scan when the CIFS client has written files.</p>
Extension for scanning ^{#2}	<p>Select the files to be scanned in the options.</p> <p>Scan all files regardless of extension Scans all the files for viruses.</p> <p>Scan all files except these extensions Runs a scan on files other than those whose extensions were specified in the Extensions list box.</p> <p>Scan files with these extensions Runs a scan on files whose extensions were specified in the Extensions list box.</p>
Extensions ^{#2}	<p>Specify the extensions to be used when you selected either the Scan all files except these extensions or Scan files with these extensions options in the Extension for scanning field, using no more than 16 characters.</p> <p>You can use any alphanumeric character, exclamation mark (!), hash mark (#), dollar sign (\$), percent sign (%), ampersand (&), single quotation mark ('), 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 square bracket ([), backslash (\), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (), right curly bracket (}), and tilde (~).</p> <p>Specify a maximum of 255 characters for each compatible option.</p> <p>When the Scan all files except these extensions option is selected, the default setting will appear in the list box as follows:</p> <pre>.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</pre>

Item	Description
	<p>When the Scan files with these extensions option is selected, there is no default settings in the list box.</p> <p>Enter an extension and click Add to add an extension in the list box. Information that has not been added to the list box cannot be set.</p> <p>To delete an extension from the list box, select it and click Delete.</p> <p>The settings corresponding to the selected in the option will be saved by the system. To discard the settings information saved to the system and restore the default settings, click Default Extensions.</p> <p>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.</p>
<p>Maximum size for scanning^{#2#3}</p>	<p>Select whether or not to specify an upper limit for the size of files to be scanned in the options.</p> <p>Specify</p> <p>Select this option to perform a scan on all files whose size is the same as or smaller than the size specified in Maximum file size.</p> <p>In the Maximum file size field, specify the upper size limit (in megabytes) of the file to be scanned within the range from 1 to 9,999 MB.</p> <p>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 storage system.</p> <p>Do not specify</p> <p>Select this option when not limiting the size of the file to be scanned.</p>
<p>Method of dealing with infected file^{#2}</p>	<p>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.</p> <p>Delete the file</p> <p>Select this option to delete infected files.</p> <p>Deny access</p> <p>Select this option to deny access from the client to infected files.</p> <p>Allow access</p> <p>Select this option to allow access from the client to infected files.</p> <p>Depending on the method of dealing with infected files, the operation result for the client accessing the infected file differs.</p> <p>When the client creates the target file, the operation result is as follows: An error is not reported to the operation result.</p> <p>When selecting Delete the file</p> <p>The target file is deleted and therefore cannot be created newly.</p>

Item	Description
	<p>When selecting Deny access The target file is deleted and therefore cannot be created newly.</p> <p>When selecting Allow access The target file can be created newly.</p> <p>When the client views the target file, the operation result is as follows:</p> <p>When selecting Delete the file The target file is deleted and therefore cannot be viewed.</p> <p>When selecting Deny access The target file access is denied. The target file cannot be viewed.</p> <p>When selecting Allow access The target file can be viewed.</p> <p>When the client updates the target file, the operation result is as follows: An error is not reported to the operation result.</p> <p>When selecting Delete the file The target file is deleted and therefore cannot be updated.</p> <p>When selecting Deny access The target file status returns to the status before the update and therefore the target file cannot be updated.</p> <p>When selecting Allow access The target file can be updated.</p>
<p>Notification when infection is detected^{#2}</p>	<p>When SNMP or email error notifications are used, from the radio buttons, select whether you want to receive notifications regarding the results of infected files via the KAQV10022-E message.</p> <p>For details about messages other than KAQV10022-E that are output, and about message IDs that are sent via notifications by SNMP traps or email notifications (including message IDs that need to be set by the <code>avaconfedit</code> command in order to be sent by SNMP traps or email notifications), see the manual <i>Error Codes</i>.</p> <p>Notify Select this option to send the KAQV10022-E message when infected files are detected.</p> <p>Do not notify Select this option if you do not want to be notified when infected files are detected.</p>
<p>Connection time-out period</p>	<p>Specify the interval from the time the connection request is sent from the HDI to the scan server until timeout, within the range from 1 to 600 seconds.</p> <p>Scan servers that do not respond during the timeout will be blocked, and the scan will be requested from another scan server.</p>
<p>Scanning time-out period</p>	<p>Specify the interval from the time a scan request is sent from the HDI to the scan server until timeout, within the range from 1 to 1,800 seconds.</p>

Item	Description
	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.
Stub file scanning time-out period	Specify the interval from the time a stub file scan request is sent from the HDI system to the scan server until the scanning times out. Specify a value in the range from 1 to 1,800 seconds. 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.
Retry other server count	Specify the number of times to switch the scan server in the event of a timeout or error during processing for connecting to the scan server. Specify a value from 0 to 32 that is no larger than the number of scan servers registered in the HDI. Specifying 0 will cause scans to fail when a timeout or error occurs during processing for connecting to the scan server.
Procedure if scanning fails	Select the response method you want to use, in the options, in the event that the scan fails. Allow access Specify this to permit access to files that could not be scanned for viruses. Deny access Specify this to refuse access to files that could not be scanned for viruses. Select the check box Permit read files if all scan server closed and scan conditions are not satisfied if all scan server connections are closed and you only want to give a client permission to read files that are excluded from being scanned (that is, folders and files with a folder or file size of zero and files that do not meet a scan condition). If this check box is not selected, any client access to read a file is denied. Even if all scan server connections are closed, files that are excluded from being scanned can also be stored in the storage system. Depending on the method of dealing with files that could not be scanned, the operation result for the client accessing such a file differs. When the client creates the target file, the operation result is as follows: An error about the operation result is not reported. When selecting Allow access The target file can be created newly. When selecting Deny access The target file is deleted and therefore cannot be created newly. When the client views the target file, the operation result is as follows: When selecting Allow access

Item	Description
	<p>The target file can be viewed.</p> <p>When selecting Deny access</p> <p>The target file access is denied. The target file cannot be viewed.</p> <p>When the client updates the target file, the operation result is as follows: An error about the operation result is not reported.</p> <p>When selecting Allow access</p> <p>The target file can be updated.</p> <p>When selecting Deny access</p> <p>The target file status returns to the status before the update and therefore the target file cannot be updated.</p>
Server monitoring interval	Specify the polling interval to confirm the status of the scan server, from 1 to 86,400 seconds.
Cache size of scanning result^{#2}	<p>Specify the size of the cache that stores the information on files that were determined to be free of infection as the result of a scan, from 1 to 64 MB.</p> <p>1 MB stores an amount of information equivalent to approximately 430 files. Files whose contents have not been changed from the information that is stored in the cache can be directly accessed without a scan.</p> <p>When changing this setting, make sure that real-time scanning is disabled. If you change the setting while real-time scanning is enabled, you need to perform the following to apply the change: disable real-time scanning, enable it again, and then restart the CIFS service.</p>
<p>Note: For details about how to exclude files and paths in a CIFS share from a scan, see the <i>CLI Administrator's Guide</i>.</p> <p>#1: If virus scan software from Trend Micro Inc. is used, when a CIFS client modifies a file, virus scanning is performed asynchronously after the modification processing is complete. Therefore, opening or renaming a file might fail because of contention between the processing for accessing modified files and for virus scanning. If an application (such as Microsoft Office) is used that sometimes reopens or renames a file right after it is modified, saving of the files might fail or unnecessary files might remain in the system. Therefore, in this environment, we recommend that you select Read only for Scan timing.</p> <p>#2: These items are not shown for some scanning software.</p> <p>#3: Symantec scan software returns an error for files that are 2 GB or larger in size. In Maximum size for scanning, perform the following settings:</p> <ul style="list-style-type: none"> • Select Specify in the options. • In the Maximum file size text box, specify a value no greater than 2,047. • Select the check box Permit access to files that have exceeded the maximum size. <p>If you set scan conditions other than the above, CIFS clients will be unable to access files that are 2 GB or larger in size. Also, the scan server will be blocked as soon as the scan fails.</p>	

Scanning Software page

You can use the **Scanning Software** page to set the scan software to use.



Note: Set the same scan software on both nodes. Note that all the registered scan server information is deleted and the scan condition is initialized when the scan software is changed.

To open the **Scanning Software** page, click **Scanning Software** on the **List of Scanner Servers** page in the **Virus Scan Server Configuration** dialog box ([Virus Scan Server Configuration dialog box on page C-283](#)).

Table C-242 Information specified in the Scanning Software page

Item	Description
Select scanning software	Select the scanning software to be used from the options.

Activate License dialog box

You can use the **Activate License** dialog box to set up licenses for the software.



Note: There are three types of licenses that can be set for the software:

- Permanent license
- Temporary license
- Emergency license

To use the software on a trial basis, the system administrator sets up a temporary license with a valid-use period. If the software needs to be used after the temporary license has expired, you need to start using the software in official-user mode. If, however, the temporary license has expired before shifting to the official-user mode, set up an emergency license.

To start using the software in official-user mode, you must set up a permanent license. After you have set up a permanent license for the software, you cannot change the license to a temporary or emergency license.

A license is set for each physical node. To set up a license, you can either specify a prepared license key file or type a license key string directly into a dialog box. When you use a license key file, you must obtain the license key file on the management console by transferring it by way of FTP, or by transporting recording media containing its copy.

To open the **Activate License** dialog box, click **Activate License** in the Configuration Wizard ([Configuration Wizard on page C-317](#)).

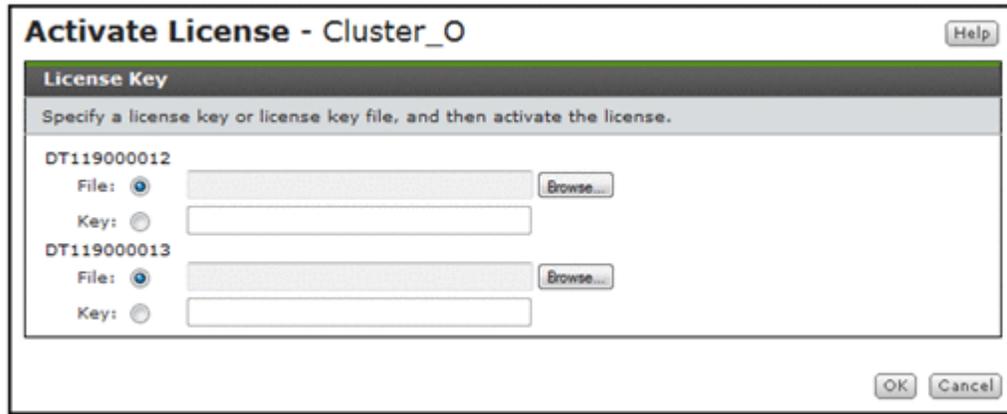


Table C-243 Information specified in the Activate License dialog box

Item	Description
File	Select this option if you want to use a license key file. Specify the path for the license key file in the text box. To specify a file name by browsing, click Browse .
Key	Select this option if you want to manually enter a license key. Enter the license key in the text box.

HCP-name window

You can use the *HCP-name* window to view specific HCP information.

To open the *HCP-name* window, select **Resources - Processing Nodes** in the **Explorer** menu of the Hitachi File Services Manager main window ([Explorer menu on page B-5](#)), and then select a desired HCP system in the object tree.

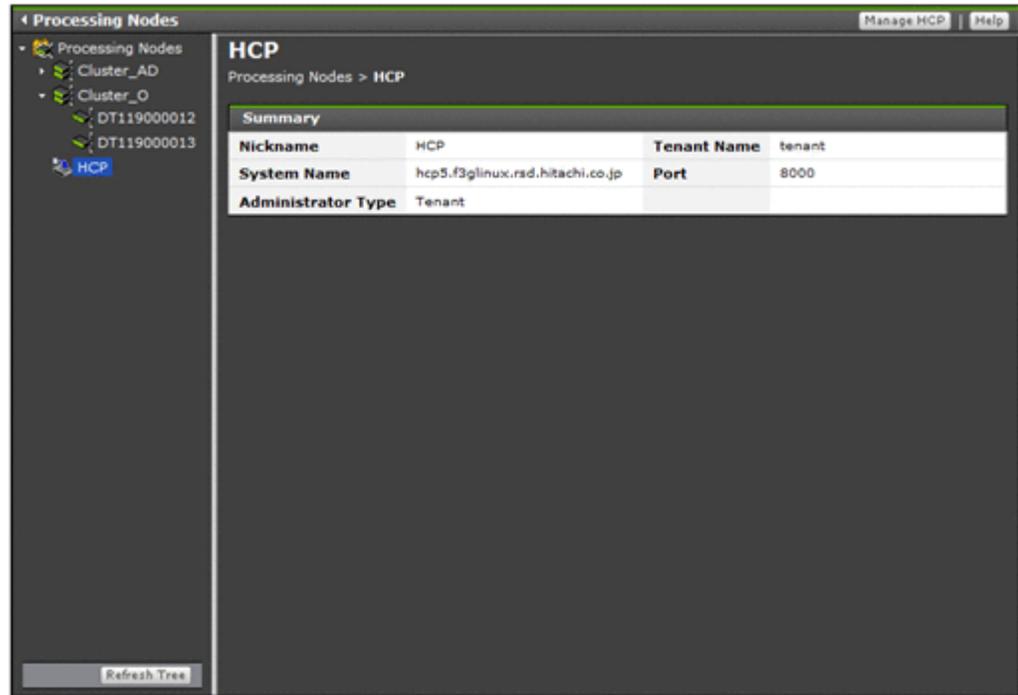


Table C-244 Information shown in the HCP-name window

Item	Description
Nickname	The HCP nickname.
System Name	The HCP system name.
Administrator Type	The administrator type. Cluster A cluster administrator. Tenant A tenant administrator.
Tenant Name	The tenant name is shown when the Administrator Type is Tenant . -- is shown when the Administrator Type is Cluster .
Port	The port number used by the management console to communicate with the HCP system.

storage-system-name window

When Hitachi Storage Navigator Modular 2 is linked to, you can view storage system information in the *storage-system-name* window.

To open the *storage-system-name* window, select **Resources - Processing Nodes** in the **Explorer** menu of the Hitachi File Services Manager main window ([Explorer menu on page B-5](#)), and then select **Processing Nodes - storage-system-name** in the object tree.

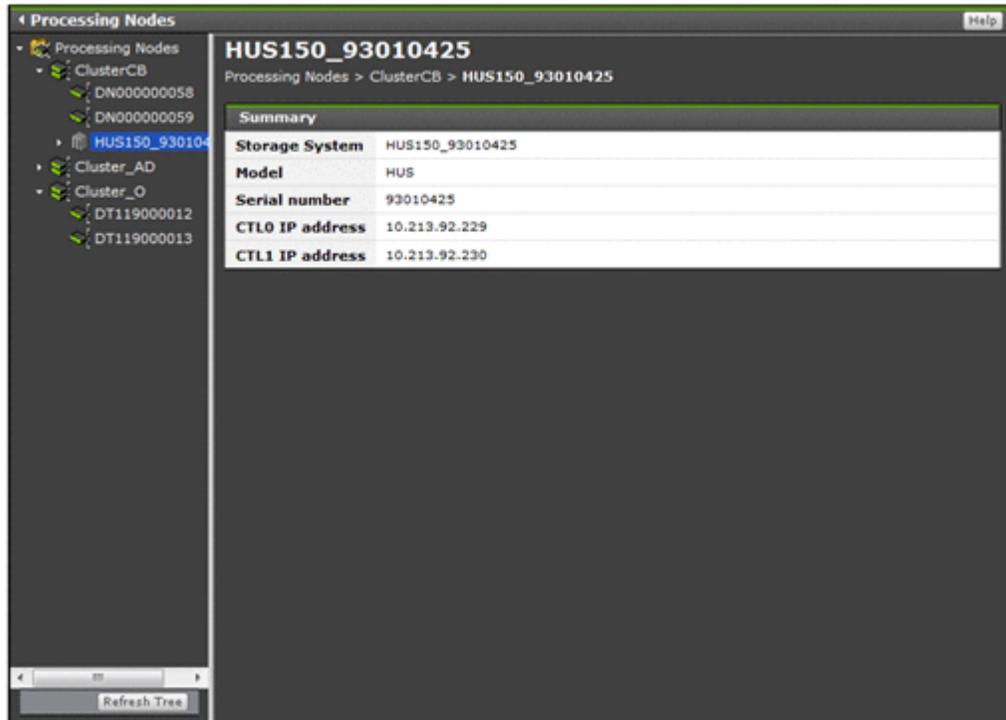


Table C-245 Information shown in the storage-system-name window

Item	Description
Storage System	The storage system name.
Model	The model of the storage system.
Serial number	The serial number of the storage system.
CTL0 IP address	The IP address of the controller 0 for the storage system.
CTL1 IP address	The IP address of the controller 1 for the storage system.

If Hitachi Storage Navigator Modular 2 is linked to, the functions of Hitachi Storage Navigator Modular 2 are shown under the object indicated by the storage system name in the object tree. For details about using these functions, see the applicable Hitachi Storage Navigator Modular 2 documentation.

Users and Permissions window

This is the menu window for managing system administrator accounts. This window is shown only for users who have the Admin permission for user management.

To open the Users and Permissions window, select **Administration**, and then **Users and Permissions** in the **Explorer** menu of the Hitachi File Services Manager main window ([Explorer menu on page B-5](#)).

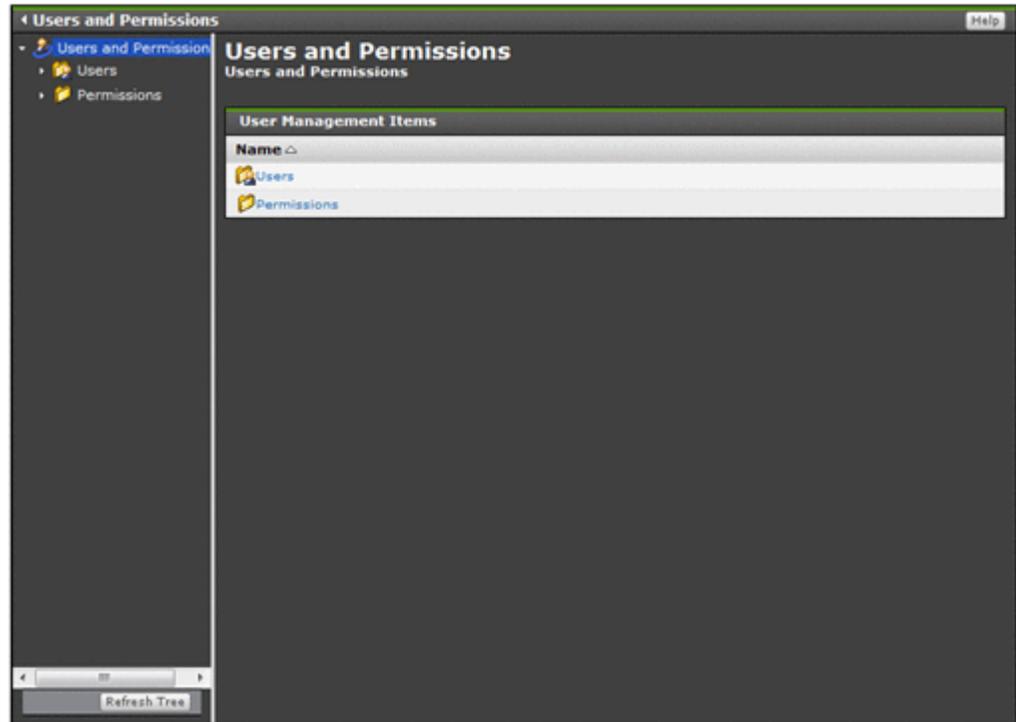


Table C-246 Information specified in the Users and Permissions window

Item		Description	See
Name	Users	Select Users to view or set user (system administrator) profiles and permissions.	Users window on page C-297
	Permissions	Select Permissions to view the number of system administrators granted operating permissions, and the specific permissions each holds.	Permissions window on page C-306

Users window

A system administrator who has Admin (user management) permission can view, in the Users window, information about the system administrators of Hitachi File Services Manager and all Hitachi Command Suite products installed on the management server.

During installation, a *built-in account* that can use all functions of Hitachi File Services Manager and Hitachi Command Suite products is set up. The user ID of this account is fixed to `System`. The user ID and permissions for this account cannot be changed or deleted.

To open the Users window, click **Users** in the object tree from the Users and Permissions window ([Users and Permissions window on page C-296](#)).

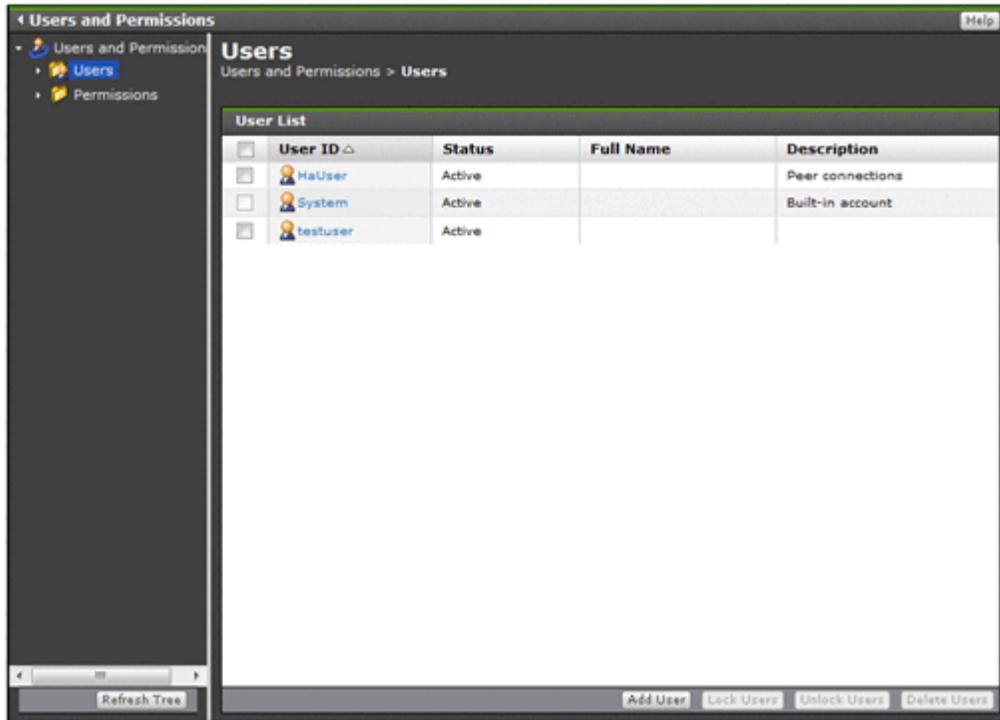


Table C-247 Information shown in the Users window

Item	Description
User ID	Lists the system administrator IDs.
Status	The lock status of each system administrator account. Active The account is not locked. Locked The account is locked.
Authentication	Shows how system administrators are authenticated. Shown only if Hitachi File Services Manager and all Hitachi Command Suite products are set to link with an external authentication server. Internal System administrators are authenticated by Hitachi File Services Manager and Hitachi Command Suite products. RADIUS System administrators are authenticated by a RADIUS server. LDAP System administrators are authenticated by an LDAP server. Kerberos System administrators are authenticated by a Kerberos server.
Full Name	The full name of each system administrator.

Item	Description
Description	The other system administrator information, such as department or contact details.

Table C-248 Operations that can be performed from the Users window

Button	Function	See
Add User	Add a system administrator.	Add User dialog box on page C-300
Lock Users	<p>Lock a system administrator account. By locking a specific system administrator's account, you can prevent that system administrator from logging on to the GUI.</p> <p>If you lock the account of a system administrator who is currently logged on, he or she will be unable to continue operations. Make sure that the system administrator is not logged on before you lock the account.</p> <p>Note:</p> <ul style="list-style-type: none"> You cannot lock your own account. To lock the System account, you need to set the <code>account.lock.system</code> property in the <code>user.conf</code> file so that you can lock the System account. For details about lock settings for the System account, see the <i>Installation and Configuration Guide</i>. You cannot log on to the GUI by using a locked account. 	N/A
Unlock Users	Unlock a system administrator account. Unlocking an account allows that system administrator to log on to the GUI. You can use either the GUI or commands to unlock an account.	N/A
Change Auth	Change how to authenticate system administrators. Shown only if Hitachi File Services Manager and all Hitachi Command Suite products are set to link with an external authentication server.	Change Authentication Method dialog box on page C-301
Delete Users	<p>Select and delete accounts of system administrators from the list.</p> <p>If you delete the account of a system administrator who is currently logged on, that system administrator will be unable to continue operations. Make sure that the system administrator is not logged on before you delete his or her account. If you want to delete your own account, log on again using another system administrator's account or the System account.</p>	N/A
Note: N/A = Not applicable.		

Button	Function	See
Only a system administrator who has Admin (user management) permission can perform these operations.		

Add User dialog box

In the **Add User** dialog box, a system administrator who has Admin (user management) permission can add a system administrator (user) account to Hitachi File Services Manager and Hitachi Command Suite products.



Note: After you add an account, you must set permissions for that system administrator. For details about how to set permissions, see [Change Authentication Method dialog box on page C-301](#).

To open the **Add User** dialog box, click **Add User** in the Users window ([Users window on page C-297](#)).

Table C-249 Information specified in the Add User dialog box

Item	Description
User ID	<p>Specify a user ID, using from 1 to 256 characters.</p> <p>You can use alphanumeric characters and the following symbols: exclamation marks (!), hash marks (#), dollar signs (\$), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), asterisks (*), plus signs (+), hyphens (-), periods (.), equal signs (=), at marks (@), backslashes (\), carets (^), underscores (_), and vertical bars ().</p> <p>User IDs are not case sensitive.</p> <p>If system administrator accounts are authenticated by a RADIUS server, and you want to register a user who is authenticated by a RADIUS server that is not the connection-destination RADIUS server, specify the realm the user belongs to along with the user name. For example, if the user name is <i>user1</i>, the realm is <i>example.com</i>, and the delimiter is @, specify <i>user1@example.com</i>.</p>
Password	<p>Enter a password, using no more than 256 characters.</p> <p>When system administrators are authenticated by an external authentication server, a password is not necessary. However, if a password is not specified, and the authentication settings are changed so that external authentication servers are no longer used, user accounts registered as such will be locked.</p> <p>You can use alphanumeric characters and the following symbols: Exclamation marks (!), hash marks (#), dollar signs (\$), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), asterisks (*), plus signs (+), hyphens (-), periods (.), equal signs (=), at marks (@), backslashes (\), carets (^), underscores (_), and vertical bars ().</p> <p>Passwords are case sensitive.</p> <p>Conditions regarding the minimum length and combination of characters that can be specified as a password might be set. If so,</p>

Item	Description
	you cannot specify a password that does not meet the set conditions.
Verify Password	Re-enter the password you specified in Password .
Full Name	Specify the system administrator's full name. This name is shown in the global tasks bar area when the system administrator you are adding logs on. Enter no more than 80 characters. You cannot use two or more dollar signs (\$) in succession. Also, you cannot use Unicode characters in the range from U+10000 to U+10FFFF.
E-mail	Specify the system administrator's email address, using no more than 255 characters.
Description	Specify the system administrator's department, contact details, or other particulars, using no more than 80 characters. Note that you cannot use Unicode characters in the range from U+10000 to U+10FFFF.

Change Authentication Method dialog box

When using an external authentication server to authenticate system administrators in the **Change Authentication Method** dialog box, a system administrator with Admin (user management) permission can change how to authenticate system administrators.

To open the **Change Authentication Method** dialog box, click **Change Auth** in the Users window ([Users window on page C-297](#)).

Table C-250 Information specified in the Change Authentication Method dialog box

Item	Description
The following user IDs will be authenticated by <i>method-name</i> method.	Select the authentication method for system administrators from the drop-down list. Internal Select this option to authenticate system administrators by using Hitachi File Services Manager and Hitachi Command Suite products. RADIUS Select this option to authenticate system administrators by using a RADIUS server. LDAP Select this option to authenticate system administrators by using an LDAP server. Kerberos Select this option to authenticate system administrators by using a Kerberos server.

user-ID window

A system administrator who has Admin (user management) permission can use the *user-ID* window to view his or her own profile and the profiles of other system administrators.

To open the *user-ID* window, in the Users and Permissions window ([Users and Permissions window on page C-296](#)), select **Users and Permissions**, **Users**, and then *user-ID* in the object tree.

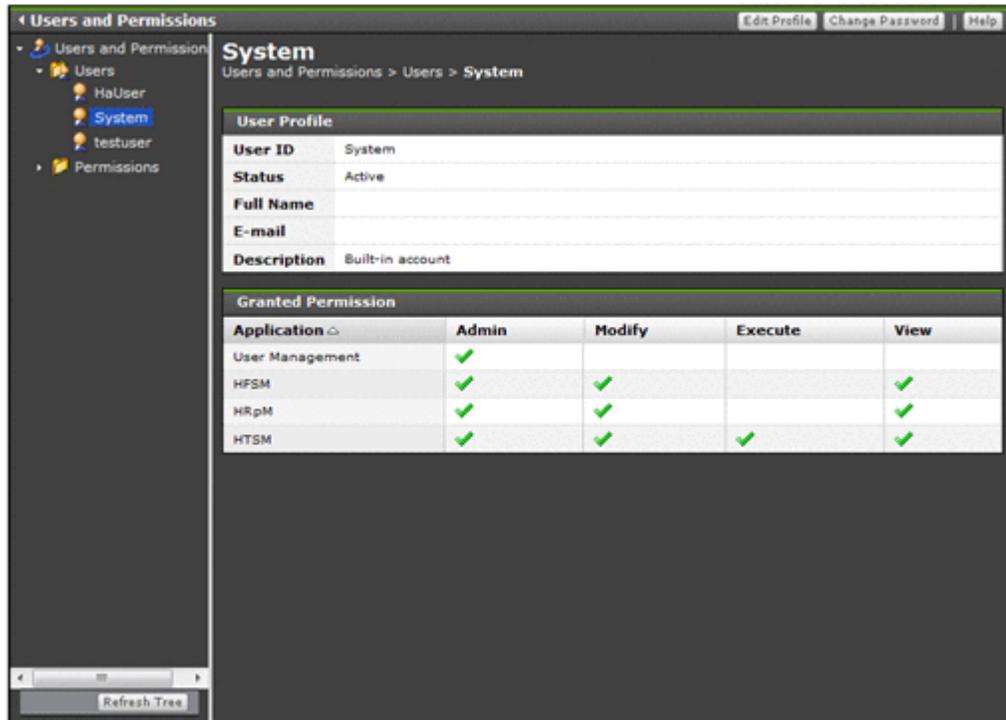


Table C-251 Information shown in the User Profile of the user-ID window

Item	Description
User ID	The ID of the system administrator.
Status	The lock status of the system administrator account. Active The account is not locked. Locked The account is locked.
Full Name	The full name of the system administrator.
E-mail	The email address of the system administrator.
Description	The other system administrator information, such as department or contact details.

Table C-252 Operations that can be performed from the user-ID window

Button	Function	See
Edit Profile	Edit your own profile, or the profiles of other system administrators.	Edit Profile dialog box on page C-303
Change Password	Change your own password or the passwords of other system administrators.	Change Password dialog box on page C-304
Change Permission	Change the permissions of the system administrator. This button is not displayed when you view the profile of the System account or your own profile.	Change Permission dialog box on page C-305
Delete User	Delete the account of the system administrator. This button is not displayed when you view the profile of the System account or your own profile. If you delete the account of a system administrator who is currently logged on, that system administrator will be unable to continue operations. If you want to delete your own account, log on again using another system administrator's account or the System account.	N/A
<p>Note: N/A = Not applicable.</p> <p>Only a system administrator who has Admin (user management) permission can perform these operations.</p>		

Edit Profile dialog box

In the **Edit Profile** dialog box, you can edit your own profile. An administrator who has Admin (user management) permission can edit profiles of other system administrators.

To open the **Edit Profile** dialog box for editing your own profile, click **Edit Profile** in the User Profile window ([User Profile window on page C-316](#)). To open this dialog box for editing the profile of another system administrator, click **Edit Profile** in the *user-ID* window ([user-ID window on page C-302](#)).

Table C-253 Information specified in the Edit Profile dialog box

Item	Description
Full Name	Specify your full name. This name is shown in the global tasks bar area when you log on.

Item	Description
	Enter no more than 80 characters. You cannot use two or more dollar signs (\$) in succession. Also, you cannot use Unicode characters in the range from U+10000 to U+10FFFF.
E-mail	Specify your email address, using no more than 255 characters.
Description	Specify your department, contact details, or other particulars, using no more than 80 characters. Note that you cannot use Unicode characters in the range from U+10000 to U+10FFFF.

Change Password dialog box

In the **Change Password** dialog box, you can change your own password. A system administrator who has Admin (user management) permission can also change the passwords of other system administrators.



Note: If the management server is operated in a cluster configuration, perform the operation on both the executing node and standby node if you want to change the System account password.

To open the **Change Password** dialog box for changing your password, click **Change Password** in the User Profile window ([User Profile window on page C-316](#)). To open this dialog box for changing the password of any other system administrator, click **Change Password** in the *user-ID* window ([user-ID window on page C-302](#)).

Table C-254 Information specified in the Change Password dialog box

Item	Description
Old Password	Enter your own current password. This item is displayed when you open the dialog box by clicking the Change Password button in the User Profile window.
New Password	Enter the new password, using no more than 256 characters. You can use alphanumeric characters and the following symbols: Exclamation marks (!), hash marks (#), dollar signs (\$), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), asterisks (*), plus signs (+), hyphens (-), periods (.), equal signs (=), at marks (@), backslashes (\), carets (^), underscores (_), and vertical bars (). Passwords are case sensitive. Conditions regarding the minimum length and combination of characters that can be specified as a password might have been set. If so, you cannot specify a password that does not meet the set conditions. To find out about the set conditions, consult a system administrator who has Admin (user management) permission.
Verify Password	Re-enter the password you specified in New Password .

Change Permission dialog box

In the **Change Permission** dialog box, a system administrator who has Admin (user management) permission can change the permissions of system administrators other than the System account and his or her own account.



Note:

- If you want to change the permissions for your own account, log on again using another system administrator's account or the System account.
- To run and manage an HDI system using the Hitachi File Services Manager GUI, the system administrator must be granted Admin permission for Hitachi File Services Manager.

To open the **Change Permission** dialog box, click **Change Permission** in the *user-ID* window ([user-ID window on page C-302](#)).

Table C-255 Information specified in the Change Permission dialog box

Item	Description
Application	<p>Select the permissions you want to set.</p> <p>Use the User Management check box to set or clear the permission required for user management.</p> <p>Admin permission for user management allows you to log on to all Hitachi Command Suite products, manage system administrators, and enhance the security of the GUI for system administrators.</p> <p>To set the same permissions for Hitachi File Services Manager and all Hitachi Command Suite products in one operation, select the All Applications check box.</p> <p>To set permissions for a specific Hitachi Command Suite product, select the check box for that product.</p> <p>Admin</p> <p>Select this option to set Admin permission. Modify and View permissions will be set automatically.</p> <p>Admin permission allows all operations other than those of user management. This provides access permissions for all resources of the target product.</p> <p>Modify</p> <p>Select this option to set Modify permission. View permission will be set automatically.</p> <p>Modify permission allows management of resources specified by a system administrator who has Admin permission for the target product.</p> <p>View</p> <p>Select this option to set View permission.</p> <p>View permission allows viewing of resource information for resources specified by a system administrator who has Admin permission for the target product.</p> <p>Peer</p> <p>Select this option to set Peer permission. Peer permission is the permission set for the Device Manager agent.</p>

Permissions window

A system administrator who has Admin (user management) permission can use the Permissions window to view the number of system administrators who have been granted operating permissions for Hitachi File Services Manager and all Hitachi Command Suite products installed on the management server.

To open the Permissions window, click **Permissions** in the object tree from the Users and Permissions window ([Users and Permissions window on page C-296](#)).

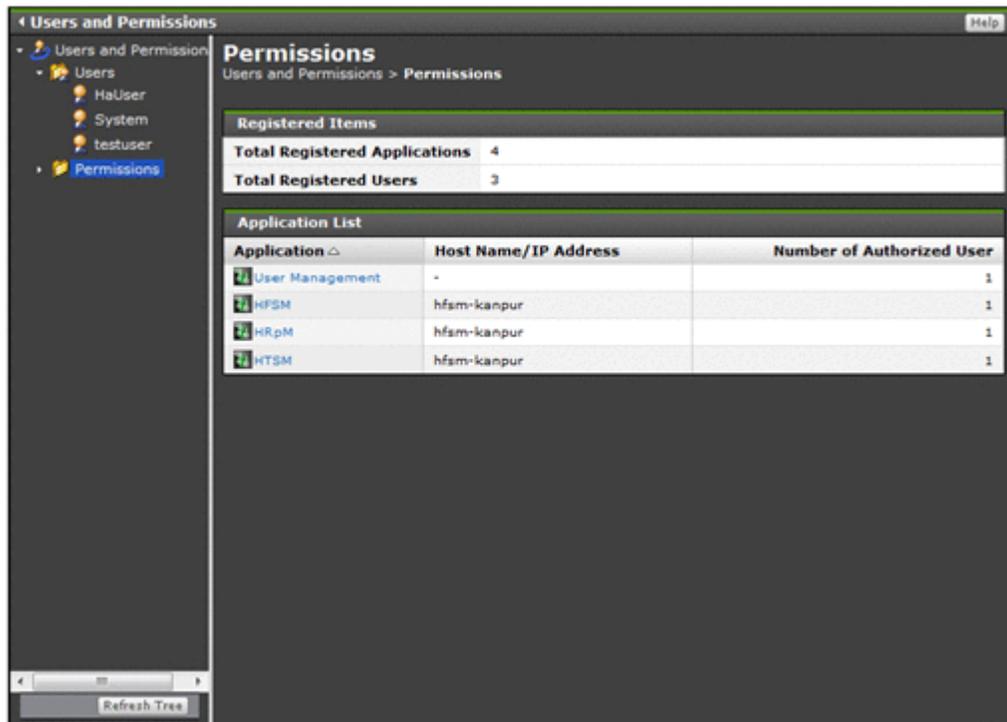


Table C-256 Information shown in the Registered Items of the Permissions window

Item	Description
Total Registered Applications	The total number of products installed on the management server.
Total Registered Users	The total number of system administrators registered for the installed products.

Table C-257 Information shown in the Application List of the Permissions window

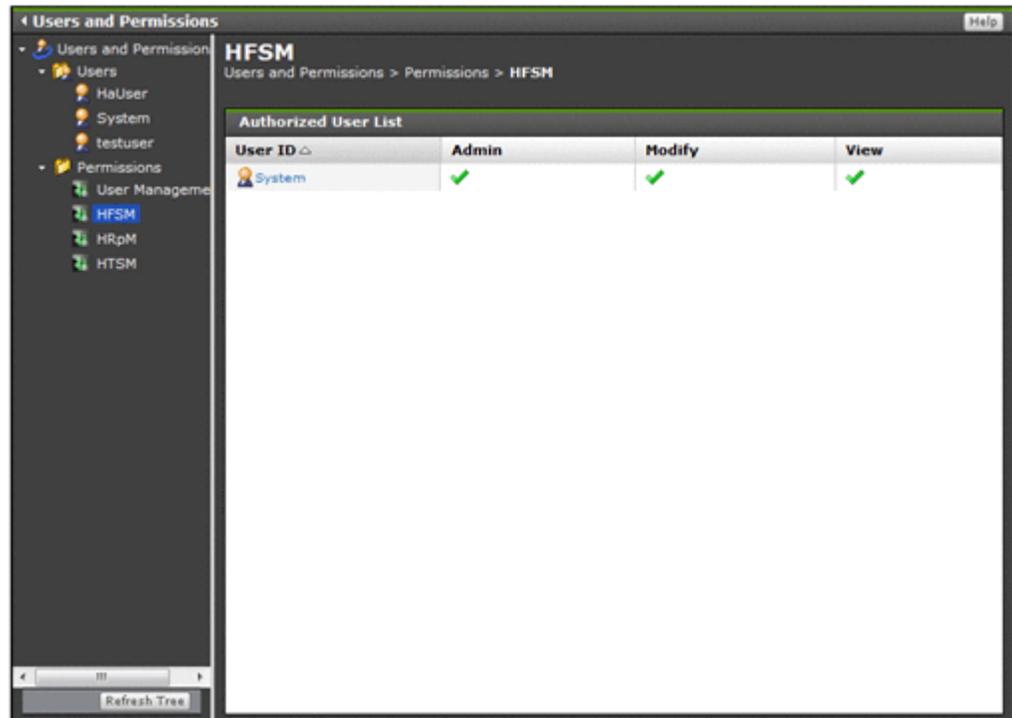
Item	Description
Application	The abbreviations of the products installed on the management server. Hitachi File Services Manager is shown as HFSM.

Item	Description
Host Name/IP Address	The host name or IP address of the server on which each product is installed. A hyphen (-) is shown for Hitachi File Services Manager (HFSM) and User Management.
Number of Authorized User	The number of system administrators who have operating permissions for each product.

application window

A system administrator who has Admin (user management) permission can view, in the *application* window, information about the system administrators of Hitachi File Services Manager.

To open the *application* window, in the Users and Permissions window ([Users and Permissions window on page C-296](#)), select **Users and Permissions**, and then an application name from the object tree.



To view information about the system administrators who have operating permissions for Hitachi File Services Manager, select **HFSM** in the object tree.

Table C-258 Information shown in the Authorized User List of the application window

Item	Description
User ID	The user ID and permissions set for each system administrator.

Item	Description
	<p>Admin A check mark is shown if the user has Admin permission.</p> <p>Modify A check mark is shown if the user has Modify permission.</p> <p>View A check mark is shown if the user has View permission.</p> <p>Peer A check mark is shown if the user has Peer permission. Peer permission is the permission set for the Device Manager agent.</p>

Security window

The Security window is the menu window for the login security settings. This window is shown only for users that have Admin permission for user management.

To open the Security window, select **Administration**, and then **Security** from the **Explorer** menu of the Hitachi File Services Manager main window ([Explorer menu on page B-5](#)).

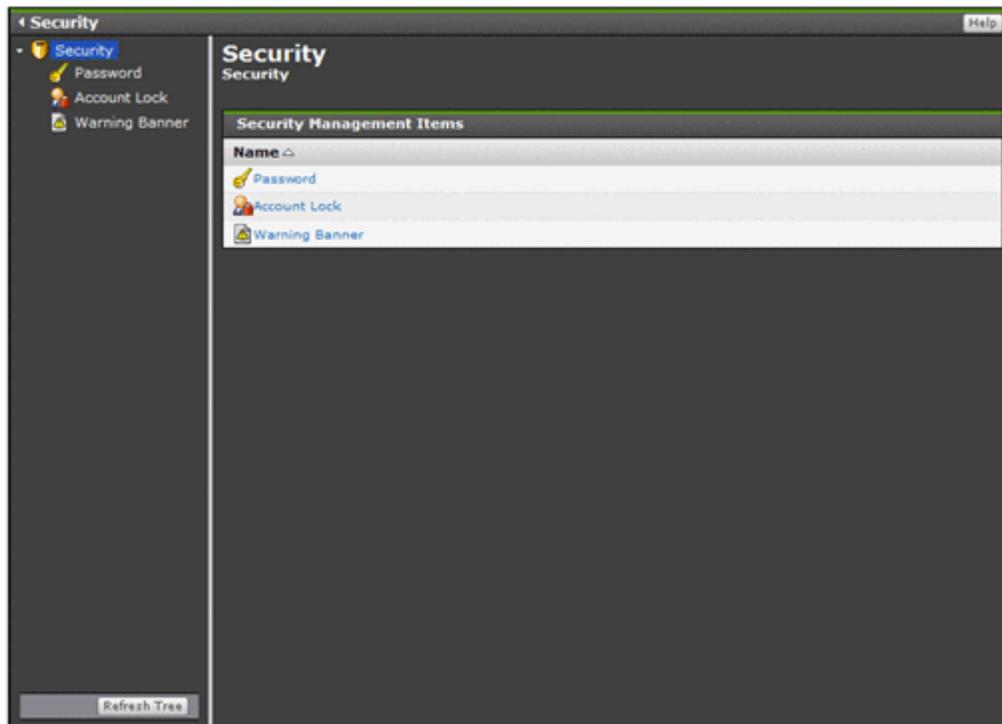


Table C-259 Information specified in the Security window

Item		Description	See
Name	Password	Select this item to view or set the system administrator password policy.	Password window on page C-309
	Account Lock	Select this item to view or specify the auto-lock settings for system administrator accounts.	Account Lock window on page C-311
	Warning Banner	Select this item to view or set the message shown in the Login window warning banner.	Warning Banner window on page C-313

Password window

A system administrator who has Admin (user management) permission can use the Password window to view the system administrator password policy.

To open the Password window, click **Password** in the object tree from the Security window ([Security window on page C-308](#)).

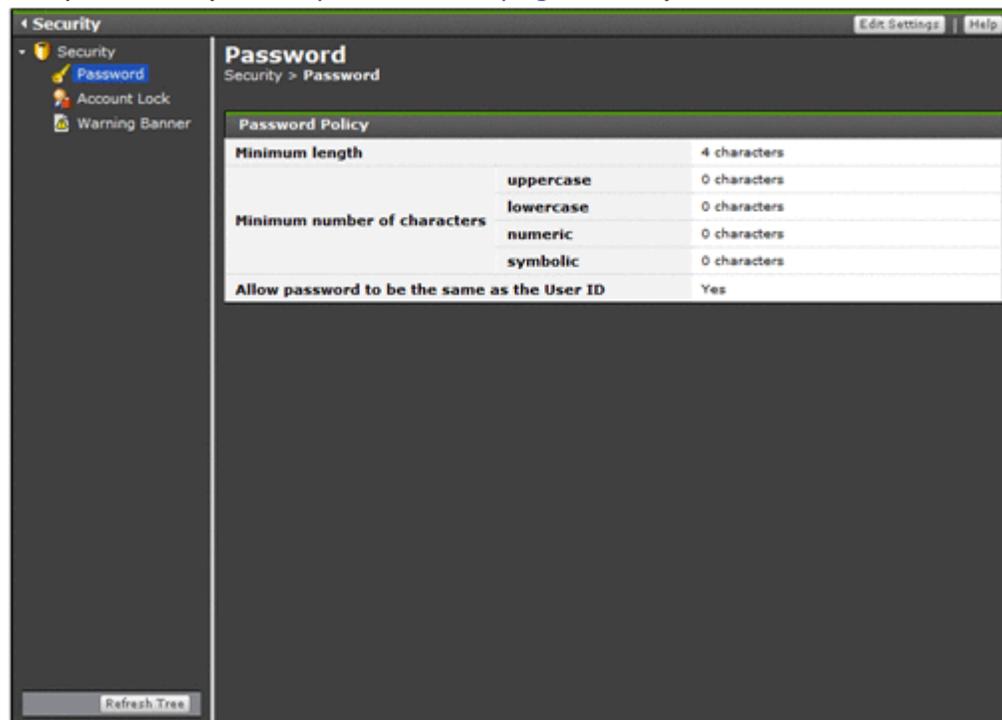


Table C-260 Information shown in the Password window

Item	Description
Minimum length	The minimum number of characters that can be set as a password.

Item		Description
Minimum number of characters	uppercase	The minimum number of upper-case characters that the password must contain.
	lowercase	The minimum number of lower-case characters that the password must contain.
	numeric	The minimum number of numeric characters that the password must contain.
	symbolic	The minimum number of symbols that the password must contain.
Allow password to be the same as the User ID		<p>Indicates whether the same character string as the user ID can be used as the password.</p> <p>Yes</p> <p>Allows the password to be the same character string as the user ID.</p> <p>No</p> <p>Does not allow the password to be the same character string as the user ID.</p>

Table C-261 Operations that can be performed from the Password window

Button	Function	See
Edit Settings	Set the system administrator password policy.	Password dialog box on page C-310

Password dialog box

In the **Password** dialog box, a system administrator who has Admin (user management) permission can set conditions about the minimum length and combination of characters that can be set as the password of a system administrator. Hitachi Data Systems recommends that you set a password policy so that third parties cannot easily guess a system administrator's password.



Note:

- The set password policy applies when a system administrator account is added or a system administrator's password is changed. If a system administrator's existing password does not match the set conditions, that system administrator can still log on to the GUI.
- If the management server is operated in a cluster configuration, specify the password policy setting on both the executing node and standby node.

To open the **Password** dialog box, click **Edit Settings** in the Password window ([Password window on page C-309](#)).

Table C-262 Information specified in the Password dialog box

Item		Description
Minimum length		Specify the minimum number of characters contained in the password.
Minimum number of characters	uppercase	Specify the minimum number of upper-case characters contained in the password. If you specify 0, there is no limit on the number of upper-case characters.
	lowercase	Specify the minimum number of lower-case characters contained in the password. If you specify 0, there is no limit on the number of lower-case characters.
	numeric	Specify the minimum number of numeric characters contained in the password. If you specify 0, there is no limit on the number of numeric characters.
	symbolic	Specify the minimum number of symbols contained in the password. If you specify 0, there is no limit on the number of symbols.
Allow password to be the same as the User ID		<p>Select whether the same character string as the user ID can be used as the password.</p> <p>Yes</p> <p>Allow the password to be the same character string as the user ID.</p> <p>No</p> <p>Do not allow the password to be the same character string as the user ID.</p>

Account Lock window

A system administrator who has Admin (user management) permission can use the Account Lock window to view the auto-lock settings for system administrator accounts.

To open the Account Lock window, click **Account Lock** in the object tree from the Security window ([Security window on page C-308](#)).

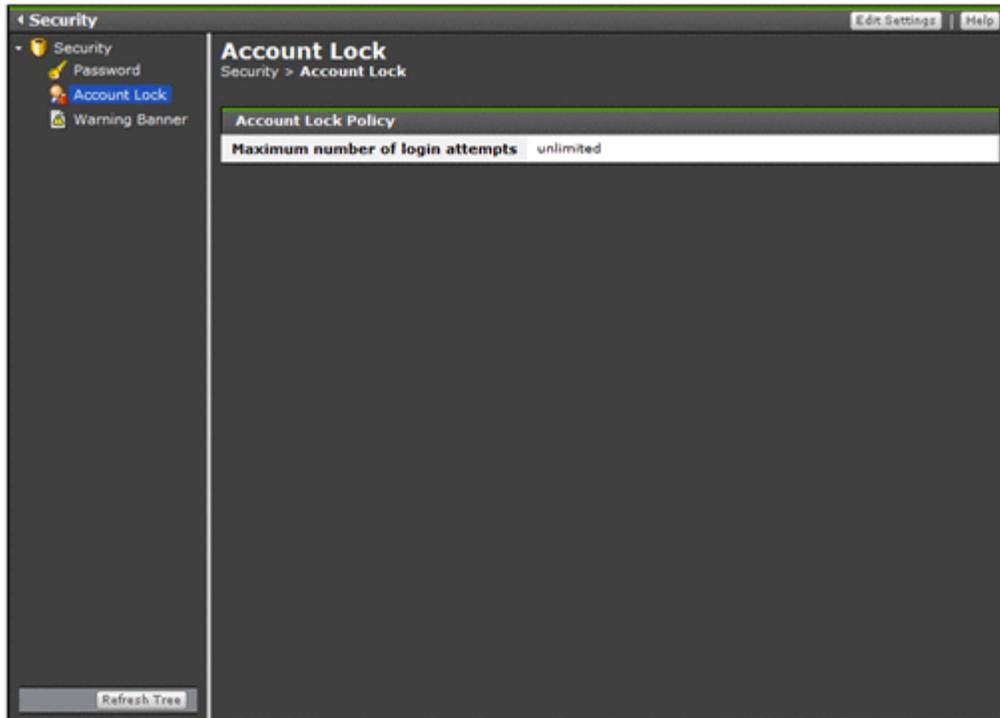


Table C-263 Information shown in the Account Lock window

Item	Description
Maximum number of login attempts	The number of consecutive unsuccessful log on attempts allowed before an account is locked. If no upper limit has been set, <code>unlimited</code> appears.

Table C-264 Operations that can be performed from the Account Lock window

Button	Function	See
Edit Settings	Sets the number of unsuccessful log on attempts allowed before an account is locked when the system administrator fails to log on.	Account Lock dialog box on page C-312

Account Lock dialog box

In the **Account Lock** dialog box, a system administrator who has Admin (user management) permission can enter settings so that an account will be locked automatically after a number of consecutive unsuccessful log on attempts. Automatically locking an account after repeated unsuccessful log on attempts reduces the risk of unauthorized access to the GUI.



Note:

- You cannot log on to Hitachi File Services Manager or a Hitachi Command Suite product by using an account locked by another system administrator who has Admin (user management) permission.
- If the system administrator account that has logged on is locked automatically, the account can continue operation until it logs off.
- If the management server is operated in a cluster configuration, specify the automatically locking an account setting on both the executing node and standby node.

To open the **Account Lock** dialog box, click **Edit Settings** in the Account Lock window ([Account Lock window on page C-311](#)).

Table C-265 Information specified in the Account Lock dialog box

Item	Description
Lockout a user account after number of failed attempts	Select this check box to enable auto-locking of accounts. An account will be locked when the number of consecutive unsuccessful log on attempts exceeds the number specified in Maximum number of log on attempts .
Maximum number of login attempts	Specify the number of consecutive unsuccessful log on attempts allowed before an account is locked. The maximum number of unsuccessful log on attempts is applied for log on authentication. For example, if the number of unsuccessful attempts is changed from 5 to 2, three consecutive log on attempt failures will not result in the account being locked. If the password is set correctly at the next attempt (the fourth time), log on is allowed. If the fourth log on attempt fails, the account is locked.

Warning Banner window

In the Warning Banner window, a system administrator who has Admin (user management) permission can view the message shown in the warning banner of the Login window.

To open the Warning Banner window, click **Warning Banner** in the object tree from the Security window ([Security window on page C-308](#)).

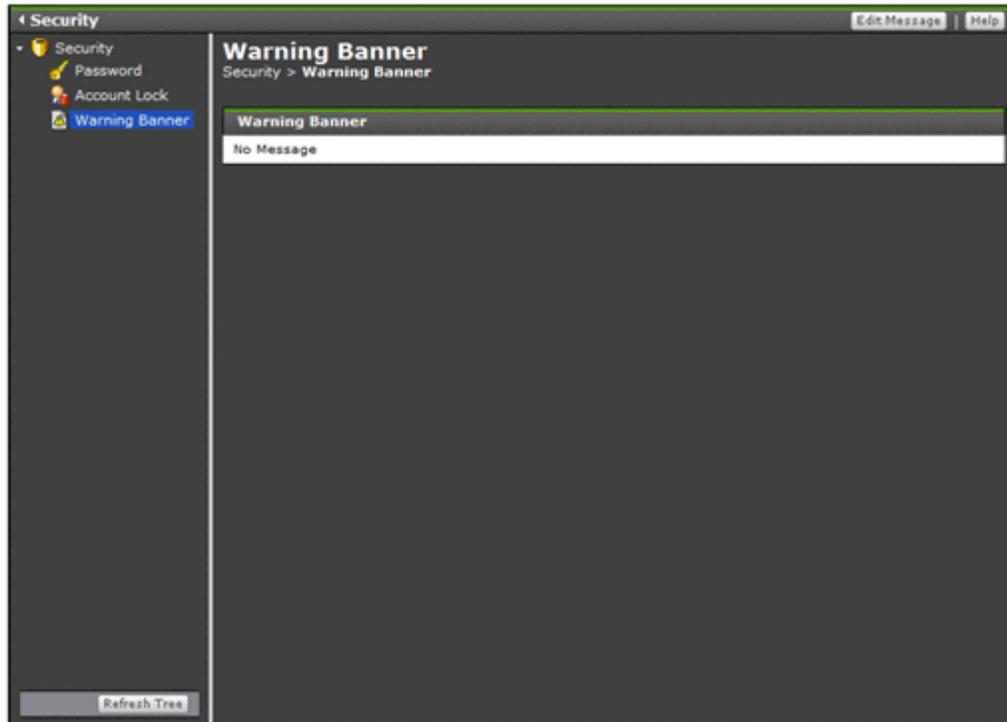


Table C-266 Information shown in the Warning Banner window

Item	Description
Warning Banner	The message shown in the warning banner of the Login window in HTML format. If no message has been set, <code>No Message</code> appears.

Table C-267 Operations that can be performed from the Warning Banner window

Button	Function	See
Edit Message	Set the message to be shown in the warning banner of the Login window.	Edit Message dialog box on page C-314

Edit Message dialog box

As a log on security measure, in the **Edit Message** dialog box, a system administrator who has Admin (user management) permission can set a message to be shown as a warning banner in the Login window. By issuing a warning in advance to a third party attempting unauthorized access, you can reduce the risk of data destruction or disclosure.



- When the message is registered, the HTML syntax is neither checked nor corrected. Edit the message correctly in accordance with HTML syntax rules. If there is a problem with the HTML syntax in the message, the message might not show correctly in the log on window.
- A different message cannot be set for each Web browser's locale by using the GUI.
- There are restrictions on the HTML tags you can use by using the GUI.
- If a message registered by specifying the locale by using the `hcmdsbanner` command exists, that message is shown in the Login window, instead of the message set by using the GUI.
- Messages registered by specifying the locale by using the `hcmdsbanner` command cannot be edited by using the GUI.
- By using the `hcmdsbanner` command, you can set a different message for each locale. In addition, you can use any HTML tags.
For details about how to set a message by using the `hcmdsbanner` command, see the *Installation and Configuration Guide*.
- To delete the message from the warning banner of the log on window, clear the **Message** field in the **Edit Message** dialog box, and then click **OK**.
- If the management server is operated in a cluster configuration, specify the message to be shown as a warning banner setting on both the executing node and standby node.
- When a Hitachi Command Suite product that supports the warning banner functionality is installed on the management server, the registered message is also shown in the Login window of that product.

To open the **Edit Message** dialog box, click **Edit Settings** in the Warning Banner window ([Warning Banner window on page C-313](#)).

Table C-268 Information specified in the Edit Message dialog box

Item	Description
Message	<p>Write the message to be shown in the warning banner using HTML tags.</p> <p>You can specify a maximum of 1,000 characters, including the HTML tags. HTML tags are not case sensitive. Line breaks used in the text box are included in the character count.</p> <p>Use HTML escape sequences to show, as ordinary characters, the following characters used in HTML tags: left angle brackets (<), right angle brackets (>), ampersands (&), single quotation marks (') and double quotation marks ("). For example, to show an ampersand (&) in the message, write <code>&amp;</code>.</p> <p>Click Preview > to check the message in HTML format in the Preview field.</p>

User Profile window

You can view your own profile in the User Profile window.

To open the User Profile window, in the **Explorer** menu of the Hitachi File Services Manager main window ([Explorer menu on page B-5](#)), select **Settings**, and then **User Profile**.

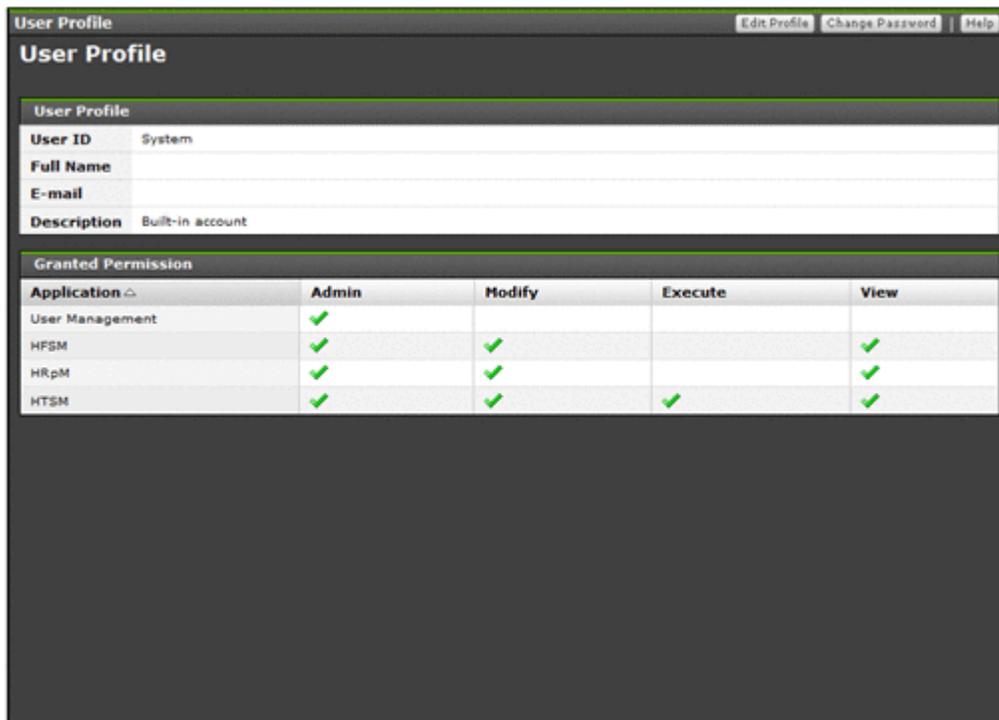


Table C-269 Information shown in the User Profile of the User Profile window

Item	Description
User ID	The ID of the system administrator.
Full Name	The full name of the system administrator.
E-mail	The email address of the system administrator.
Description	The other system administrator information, such as department or contact details.

Table C-270 Information shown in the Granted Permission of the User Profile window

Item	Description
Application	The permissions granted to the system administrator for each product. Permissions related to user management are shown in the User Management field. Permissions related to Hitachi File Services Manager are shown in the HFSM field.

Item	Description
	<p>Admin A check mark is shown if Admin permission is set.</p> <p>Modify A check mark is shown if Modify permission is set.</p> <p>View A check mark is shown if View permission is set.</p> <p>Peer A check mark is shown if Peer permission is set. Peer permission is the permission set for the Device Manager agent.</p>

Table C-271 Operations that can be performed from the User Profile window

Button	Function	See
Edit Profile	Edit your own profile.	Edit Profile dialog box on page C-303
Change Password	Change your own password.	Change Password dialog box on page C-304

Configuration Wizard

You can set up nodes and licenses, and configure clusters by using the Configuration Wizard.



Tip: Note that some existing processing node settings cannot be changed in the Configuration Wizard, although they are shown. To change a setting that cannot be changed in the Configuration Wizard, click the relevant menu on the **9. Completion** page shown when setup is completed or on the **Settings** tab in the *physical-node* window.

The Configuration Wizard sometimes temporarily stops the cluster and resource groups that are running, depending on the settings you perform. If you set HCP information in the Configuration Wizard, the system configuration file will be periodically saved to the HCP.

You can start the Configuration Wizard by using either of the following operations:

When registering a new processing node:

In the global tasks bar area of the Hitachi File Services Manager main window ([Global tasks bar area on page B-4](#)), click **Go**, and then select **Configuration Wizard**.

If no processing nodes have been registered and you log on to the Hitachi File Services Manager GUI, the Configuration Wizard starts automatically.

When changing the settings for a registered processing node:

In the *processing-node* window or *physical-node* window, click **Reconfigure Processing Node** (see [processing-node window on page C-86](#) or [physical-node window on page C-91](#)).

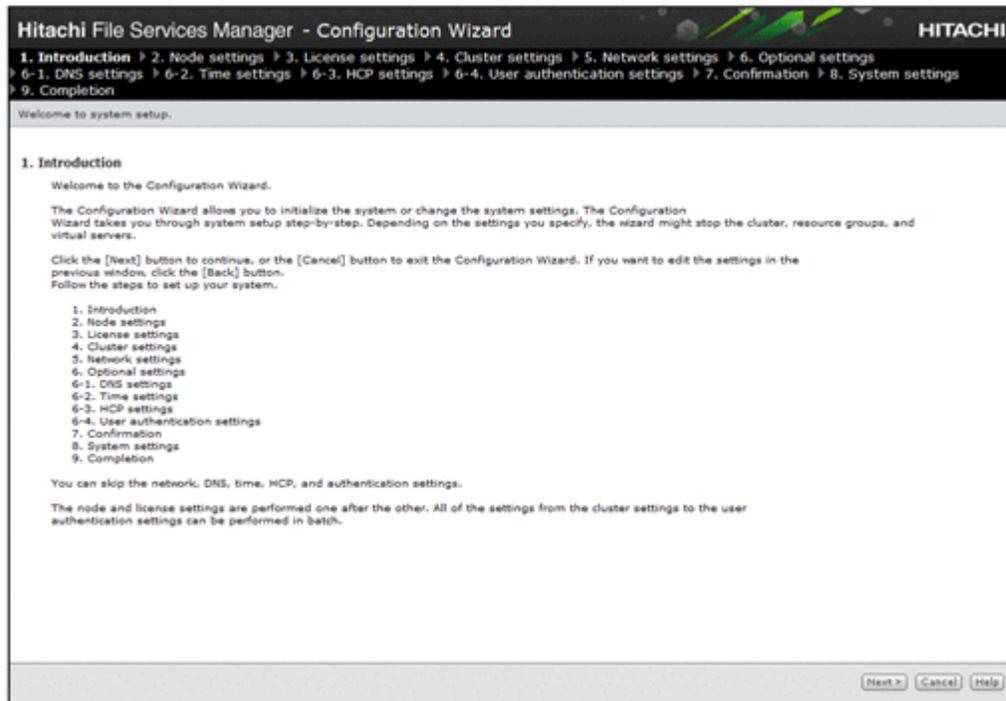


Table C-272 Pages shown for the Configuration Wizard

Page	Description	See
1. Introduction	Check the information shown, and then click Next > .	N/A
2. Node settings	Specify the necessary information in the settings page, and then click Next > . Check the specified processing node information in the confirmation page, and then click Next > .	2. Node settings page on page C-319
3. License settings	Specify the necessary information, and then click Next > . Click Activate License to view the Activate License dialog box, where you can specify the license settings. When you click OK to close the Activate License dialog box, the license information you specified is shown on the 3. License settings page. If you want to continue setup with different license settings between the nodes, before clicking Next , select the Keep the license settings between the physical nodes different, and continue with setup check box.	Activate License dialog box on page C-293

Page	Description	See
4. Cluster settings	Specify the necessary information, and then click Next > .	4. Cluster settings page on page C-320
5. Network settings	Specify the necessary information, and then click Next > .	5. Network settings page on page C-322
6. Optional settings	Specify the necessary information, and then click Next > . The window that is shown depends on the selected option.	6. Optional settings page on page C-322
6-1. DNS settings	Specify the necessary information, and then click Next > . The window that is shown depends on the option selected in the 6. Optional settings page.	6-1. DNS settings page on page C-323
6-2. Time settings	Specify the necessary information, and then click Next > . The window that is shown depends on the option selected in the 6. Optional settings page.	6-2. Time settings page on page C-323
6-3. HCP settings	Specify the necessary information, and then click Next > .	6-3. HCP settings page on page C-324
6-4. User authentication settings	Specify the necessary information, and then click Next > .	6-4. User authentication settings page on page C-326
7. Confirmation	Check the information shown, and if there is no problem, click Confirm . The 8. System settings page is shown and the setup is performed.	N/A
8. System settings	The progress of the setup is shown until processing is completed. After processing has been completed, the 9. Completion page is shown.	N/A
9. Completion	Check the processing result, and then click Close .	9. Completion page on page C-333
Note: N/A = Not applicable.		

2. Node settings page

You can use the **2. Node settings** page of the **Configuration Wizard** to set the processing node information.

Table C-273 Information specified on the 2. Node settings page of the Configuration Wizard

Item	Description
Target node settings	<p>Specify the settings for the node that will be connected to the management server.</p> <p>Mgmt. IP address first node Specify the IP address or host name of node 0 in the cluster.</p> <p>Mgmt. IP address second node Specify the IP address or host name of node 1 in the cluster.</p> <p>Password Specify the management server's authentication password set in the node. The initial password is <code>manager</code>.</p>
Storage system settings	<p>Specify the settings for the controllers of the storage system to be managed.</p> <p>CTL0 IP address Specify the IP address or host name of the management port for controller 0.</p> <p>CTL1 IP address Specify the IP address or host name of the management port for controller 1.</p>

4. Cluster settings page

You can use the **4. Cluster settings** page of the **Configuration Wizard** to set the information for configuring a cluster. If you change the settings (except for when you only change the cluster name), the OS is restarted on the **8. System settings** page.

Table C-274 Information specified on the 4. Cluster settings page of the Configuration Wizard

Item	Description
Cluster name	<p>Specify the name of the cluster that consists of two nodes. The specified name is used as the processing node name. When multiple processing nodes are managed by the management server, make sure that names are not duplicated.</p> <p>You can use a maximum of 22 characters.</p> <p>You can use any alphanumeric character, hyphen (-), period (.), forward slash (/), colon (:), at mark (@), and underscore (_). However, you cannot use an underscore (_) as the first character.</p> <p>Note that you cannot specify the name 0 or words reserved by the system. For details about reserved words, see List of reserved words on page F-2.</p>

Item	Description
Physical node host name	<p>Specify the physical node host name. The host name of each physical node must be unique. Note that upper-case and lower-case letters are set exactly as specified, but names that differ only in case are assumed to be the same.</p> <p>The host name set here is also used as the host name of the node that is set on the Modify Host Name page.</p> <p>The host name can have a maximum of 15 characters. You can use alphanumeric characters including hyphens (-). The host name must begin with an alphabetic letter, and must not end with a hyphen (-).</p> <p>Note that you cannot specify system-reserved words in upper case or lower case. For details about reserved words, see List of reserved words on page F-2.</p> <p>Also note that in the initial settings, a unique name is assigned to each physical node.</p>
Optional setting	<p>If you want to specify the network address of the heartbeat port, select Change. Select an address from the Network address of the heartbeat port drop-down list (10.0.1.0, 192.168.1.0, 192.168.234.0, 172.23.212.0, or 10.197.182.0).</p>
Cluster management LU#	<p>Information about the LU to be used as the cluster management LU is shown. To change the LU, click Change LU.</p> <p>If Change LU is clicked, the Change Cluster Management LU dialog box opens.</p> <p>Select the option for the LU you want to use, and then click OK. Note that the LU size must be about 70 GB. After clicking OK, the information about the selected LU is shown in the Selected LU table on the 4. Cluster settings page. Note that the shared LU must have a capacity of at least 70 GB.</p> <p>Note that the following LUs are not shown:</p> <ul style="list-style-type: none"> • An LU for which an error has occurred on the FC path • A blocked LU <p>To use a virtual LU as a cluster management LU, confirm with the storage system administrator whether full allocation or full capacity mode for Dynamic Provisioning is enabled.</p>
Encryption settings#	<p>When an encryption license is set, select whether to encrypt the local data or the data to be stored in the HCP system.</p> <p>Enable local data encryption</p> <p>Select the Yes check box to encrypt the local data (user LUs).</p> <p>If the common key used for encryption is corrupted or cannot be obtained, user data will no longer be available. We recommend that you use the <code>encdisplaykey</code> command to display the key, and save the key on external media.</p> <p>Enable HCP payload encryption</p> <p>Select the Yes check box when encrypting the data to be stored in the HCP system.</p>

Item	Description
	If the common key used for encryption is corrupted or cannot be obtained, you will not be able to migrate data to the HCP system or to recall data from the HCP system. Be sure to use the <code>hcpdisplaykey</code> command to display the key, and then save the key on external media.
#: These items cannot be changed if they have been set up.	

5. Network settings page

Specify an `mnq0` virtual IP address in the **IPv4** or **IPv6** tab.

Table C-275 Information specified on the 5. Network settings page of the Configuration Wizard

Item	Description
Fixed IP address	Specify a fixed IP address.
Virtual IP address	Specify a virtual IP address.
Netmask	For IPv4, specify a netmask.
Prefix length	For IPv6, specify a prefix length.
Default gateway	Specify the default gateway. You can edit the default gateway that has already been set if Hitachi File Services Manager and the processing node are in the same network segment.
Note: Settings and editable items differ depending on the protocol used for network configuration or communication.	

6. Optional settings page

You can use the **6. Optional settings** page of the **Configuration Wizard** to select whether to use the default settings or custom settings.

Table C-276 Information specified on the 6. Optional settings page of the Configuration Wizard

Item	Description
Default settings	<p>Select this option if you want to create a temporary environment for testing operations such as access to a file share. If this option is selected, a test file share (<code>MyShare</code>) and a test user (name: <code>testuser</code>, password: <code>password789</code>) are created.</p> <p>Note that you cannot select this option in the following cases:</p> <ul style="list-style-type: none"> The settings for a registered processing node are being changed. The virtual IP addresses are not specified on the 5. Network settings page. There are no LUs that have enough space to set up a test file system.

Item	Description
Custom settings	<p>Select this option if you want to specify an external server and the user authentication settings necessary for the actual start of operation. If you select this option, select the check boxes of the settings you want to specify:</p> <p>DNS settings</p> <p>Select this check box if you want to specify DNS server settings.</p> <p>Time settings</p> <p>Select this check box if you want to specify NTP server and time zone settings.</p> <p>HCP settings</p> <p>Select this check box if you want to specify the information about HCP that is used for migrating data.</p> <p>User authentication settings</p> <p>Select this check box if you want to specify user authentication settings.</p>

6-1. DNS settings page

You can use the **6-1. DNS settings** page of the **Configuration Wizard** to set up the DNS server. After the settings are changed, the OS is restarted in the **8. System settings** page.

Table C-277 Information specified on the 6-1. DNS settings page of the Configuration Wizard

Item	Description
Skip these settings	Select this option if you do not want to specify DNS server settings.
DNS settings	<p>If you want to specify DNS server settings, select this option, and then specify the following items:</p> <p>Primary DNS server</p> <p>Specify the IP address of the primary DNS server used during normal operation.</p> <p>Secondary DNS server</p> <p>Specify the IP address of the secondary DNS server used when the primary DNS server has failed.</p> <p>Default domain name</p> <p>Specify the name of the domain to which the node belongs.</p>

6-2. Time settings page

You can use the **6-2. Time settings** page of the **Configuration Wizard** to configure time settings. After the settings are changed, the OS is restarted in the **8. System settings** page.

Table C-278 Information specified on the 6-2. Time settings page of the Configuration Wizard

Item	Description
Skip these settings	Select this option if you do not want to specify NTP server and time zone settings.
Time settings	<p>If you want to specify NTP server and time zone settings, select this option, and then specify the following items:</p> <p>Time zone</p> <p>Specify a time zone. Select a region from the Region drop-down list and a time zone from the Time zone drop-down list.</p> <p>NTP server</p> <p>Specify one or two IP addresses or host names when you use an NTP server.</p> <p>We recommend that you specify IP addresses or host names for two different NTP servers as a countermeasure against a failure. Do not specify two host names for the same NTP server.</p>

6-3. HCP settings page

You can use the **6-3. HCP settings** page of the **Configuration Wizard** to set up HCP information.

Table C-279 Information specified on the 6-3. HCP settings page of the Configuration Wizard

Item	Description
Skip these settings	Select this option if you do not want to specify HCP settings.
HCP settings	If you want to specify HCP settings, select this option, and then specify information in the HCP tab and the Proxy tab.
HCP tab	<p>Specify HCP information.</p> <p>Specify the following information for Primary.</p> <p>System name</p> <p>Specify the HCP system name as a fully qualified domain name.</p> <p>Tenant name</p> <p>Specify the name of the HCP tenant.</p> <p>External HCP host name</p> <p>If the HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the HCP system.</p> <p>Tenant admin account</p>

Item	Description
	<p>Specify the user name and password of the HCP tenant administrator.</p> <p>Select Yes in the Change password when changing the password for the tenant administrator specified in the Tenant admin account.# If the password is changed from HDI, the change is also applied in HCP. Make this change only if you want to change the settings in HCP.</p> <p>New password</p> <p>Enter a new password by using 64 or fewer characters.</p> <p>Only alphabetic characters, numeric characters, and symbols can be used in passwords. Of these three types of characters, use at least two to specify the password. In addition, multibyte Unicode (UTF-8) characters can also be used. The password can contain space characters, but cannot consist of space characters only.</p> <p>The specified password of a tenant administrator user account must meet all of the password requirements, including the minimum number of characters and the combination of characters. For information about the password requirements for a tenant administrator user account, check with the HCP administrator.</p> <p>Confirm new password</p> <p>Enter the character string you entered for New password.</p> <p>The entered password is displayed by using asterisks (*).</p> <p>If you are using the HCP replication functionality, select the Use checkbox for Replica, and then specify the replica HCP information.</p>
Proxy tab	<p>If you want to use a proxy server to communicate with HCP, select Use, and then specify the proxy server information.</p> <p>Host name</p> <p>Specify the host name of the proxy server. An IP address can be specified instead of a host name.</p> <p>Port</p> <p>Specify the port number that is used on the proxy server.</p> <p>User authentication</p> <p>If you want to use user authentication on the proxy server, select Use, and then specify the user name and password that are used for authentication.</p>
	<p>#: Take note of the following before changing the password for the tenant administrator.</p> <ul style="list-style-type: none"> • The specified password is necessary to connect to HCP tenants. Do not forget this password. • Change the tenant administrator password when no migration or recall is taking place. If a migration or recall takes place when a password change is in progress, the migration or recall processing might fail. • If you specify a password that includes invalid characters, after the processing to change the password fails, the original password might become unusable. In such a case, ask the HCP administrator to issue a new password. After receiving a new password from the HCP administrator, reconfigure the tenant administrator user account.

Item	Description
	<ul style="list-style-type: none"> • If a tenant or tenant administrator user account is shared with another HDI system, it is necessary to update the appropriate setting on the HDI system, so that the changed password is also used on the system. If such a password change is made, report the new password to the administrator of the other HDI system, and then ask the administrator to update the relevant HCP information registered in the HDI system. • If a tenant or tenant administrator user account is shared with another HDI system, make a password change after verifying that no migration or recall is taking place on the other HDI system. <p>If an HDI system exists where a migration or recall cannot be stopped, ask the HCP administrator to create and configure a new user account for the tenant administrator. After changing the password of the new user account, report the new user name and password to the administrator of the HDI system by using the same user account. When the tenant administrator user account is configured for each relevant HDI, ask the HCP administrator to delete the old user account.</p>

If a DNS server is set or **External HCP host name** is specified, click the **Test Connection** button to check if the connection with HCP is established.

6-4. User authentication settings page

You can use the **6-4. User authentication settings** page of the **Configuration Wizard** (for selecting the protocol) to set up user authentication.

Selecting the protocol

You can select the protocol to be used.

Table C-280 Information specified on the 6-4. User authentication settings page of the Configuration Wizard (for selecting the protocol)

Item	Description
Skip these settings	Select this option if you do not want to specify user authentication settings.
Protocol	<p>If you want to specify user authentication settings, select this option, and then select the check boxes for the protocols to be used:</p> <p>CIFS</p> <p>Select this check box if CIFS user settings are to be specified.</p> <p>If you select this option and then click Next, the 6-4. User authentication settings pages (for selecting the CIFS user authentication method, specifying local authentication settings, and specifying Active Directory authentication settings) is shown.</p> <p>NFS</p> <p>Select this check box if NFS user settings are to be specified.</p>

Item	Description
	If you select this option and then click Next , the 6-4. User authentication settings page (for selecting the external server) is shown.

Selecting the CIFS user authentication method

You can set up the CIFS user authentication method.

Table C-281 Information specified on the 6-4. User Authentication Settings page of the Configuration Wizard (for selecting the CIFS user authentication method)

Item	Description
Local authentication	Select this option if you want to use the CIFS server functionality of the OS for user authentication. If you select this option and then click Next , the 6-4. User authentication settings page (for specifying local authentication settings) is shown.
Active Directory authentication	Select this option if you want to use the Active Directory domain controller for user authentication. If this option is selected, users registered in HDI cannot access CIFS shares because the Active Directory domain controller manages users. If you select this option and then click Next , the 6-4. User authentication settings page (for specifying Active Directory authentication settings) is shown.
Others	Select this option if you want to use the domain controller in the domain for user authentication. If this option is selected, you will specify the authentication settings in the Access Protocol Configuration dialog box after setup with the Configuration Wizard has been completed.

Specifying local authentication settings

You can set up local authentication.

Table C-282 Information specified on the 6-4. User authentication settings page of the Configuration Wizard (for specifying local authentication settings)

Item	Description
Workgroup name	Specify the name of the workgroup to which the node belongs. Use a name that differs from the node host name. If you specify the same name, the group name might not be shown correctly when you set up an ACL.
Create a test user	Select this check box if you want to create an operation test user. If you select the check box, specify the user information.

Item	Description	
	User name	<p>Specify a user name. You cannot specify a user name that has already been registered on the HDI system, the NIS server, or the LDAP server for user authentication. You cannot specify a name that is the same as that of an existing group configured to use the ACL functionality.</p> <p>Enter a maximum of 16 characters. The first character must be an alphanumeric character. You can use any alphanumeric character, hyphen (-), and underscore (_) after the first character. 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. Also, you cannot specify a user name already reserved in the OS.#</p>
	UID	<p>Specify the user ID. Specify a value from 200 to 2147483147.</p> <p>You cannot specify 65534 or any other value that has already been registered on the HDI system, 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.</p>
	Group name	<p>Specify the name of the group to which the user belongs. You cannot enter any group name that has already been registered on the HDI system, the NIS server, or the LDAP server for user authentication. Enter a maximum of 16 characters. The first character must be an alphanumeric character. You can use any alphanumeric character, hyphen (-), and underscore (_) after the first character. 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. Also, you cannot specify a group name already reserved in the OS.#</p>
	GID	<p>Specify the ID of the group to which the user belongs. Specify a value from 200 to 2147483147.</p> <p>You cannot specify 65534 or any other value that has already been registered on the HDI system, 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.</p>
	Password	<p>Enter the user password, using from 6 to 20 characters.</p> <p>You can use any alphanumeric character, exclamation mark (!), double quotation mark ("), hash mark (#), dollar sign (\$), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.),</p>

Item	Description
	forward slash (/), colon (:), semicolon (;), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left square bracket ([), backslash (\), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (), right curly bracket (}), and tilde (~).
Confirm password	Re-enter the password you set in Password .

#: For details about reserved words, see [List of reserved words on page F-2](#).

Specifying Active Directory authentication settings

You can set up Active Directory authentication. After the settings are changed, the CIFS service is restarted in the **8. System settings** page.

Table C-283 Information specified on the 6-4. User authentication settings page of the Configuration Wizard (for specifying Active Directory authentication settings)

Item	Description
Domain name	Specify the DNS name of the Active Directory domain. Any lower-case letters that are entered are treated as upper-case letters. If the computer used as an Active Directory domain controller is also used as a KDC server, the name specified here is also used as the domain name for the KDC server.
Domain name (NetBIOS)#	Specify the NetBIOS name of the Active Directory domain.
DC server name(s)#	Specify the names of the Active Directory domain controller servers to which the node belongs. You can specify a maximum of 5 server names. If you specify multiple server names, separate them with a comma (,). You can also specify IP addresses. If the computer used as an Active Directory domain controller is also used as a KDC server, the name of an Active Directory domain controller server specified here is also used as the name of the KDC server.
Domain user name	Specify the name of the user for the Active Directory domain controller.
Domain user password	Specify the password of the user for the Active Directory domain controller.
User mapping#	Select the option corresponding to the user mapping method used. RIDs

Item	Description
	<p>Select this option if you want to base user mapping on relative identifiers (RIDs).</p> <p>If you select this option and then click Next, the 6-4. User authentication settings page used when RIDs is selected as the user mapping method is shown.</p> <p>Active Directory schema</p> <p>Select this option if you want to base user mapping on the Active Directory schema.</p> <p>If you select this option and then click Next, the 6-4. User authentication settings page used when Active Directory schema is selected as the user mapping method is shown.</p> <p>Others (LDAP, or if user mapping will not be used)</p> <p>Select this option if you want to base user mapping on LDAP or if you do not want to use user mapping.</p> <p>For LDAP user mapping, after setup with the Configuration Wizard has been completed, specify settings on the CIFS Service Management page in the Access Protocol Configuration dialog box. For details, see CIFS Service Management page on page C-222.</p>
	<p>#: Shown when Custom settings is selected or the current settings are changed. If Custom settings is not selected, a domain name (NetBIOS) and up to five DC servers based on the specified domain name are automatically searched for and set. When only the CIFS protocol is used, RID user mapping is selected and an ID range from 70000 through 4069999 (4,000,000 IDs) is set for the domain name (NetBIOS) that was automatically searched for. When both the CIFS and NFS protocols are used, Active Directory user mapping is selected and LDAP is used for the network information service (RFC 2307).</p>

When RIDs is selected as the user mapping method

You can set up RID user mapping.

Table C-284 Information specified on the 6-4. User Authentication Settings page of the Configuration Wizard (when RIDs is selected as the user mapping method)

Item	Description
Range of UIDs and GIDs	Specify the range of user IDs and group IDs that will be used for RID-based user mapping.
Settings for each domain	<p>Specify a range of user IDs and group IDs for each domain. You can specify a range for a maximum of 256 domains. If you have more than 20 domains to register, only register up to 20 domains at a time to avoid a timeout.</p> <p>Register all domains that have been specified as Active Directory domains. If you only register domains that have</p>

Item	Description
	<p>trust relationships, the users on those domains are not allowed access to the CIFS share.</p> <p>Domain name (NetBIOS)</p> <p>Specify a domain name.</p> <p>Specify the name of a domain that has been specified as an Active Directory domain or a domain that has a trust relationship.</p> <p>Range of UIDs and GIDs</p> <p>Specify the range of user IDs and group IDs for the domain. Make sure that you specify a range within the range of user IDs and group IDs that can be used for user mapping.</p> <p>Note that the ranges for the domains must not overlap. However, they need not be contiguous.</p> <p>When you specify the above items and then click Add, the settings for the domain are added to the Selected Domains table. To delete the settings for a domain, select the check box for the domain in the table, and click Delete.</p>

When Active Directory schema is selected as the user mapping method

You can set up Active Directory schema user mapping.

Table C-285 Information specified on the 6-4. User authentication settings page of the Configuration Wizard (when Active Directory schema is selected as the user mapping method)

Item	Description
Microsoft® Services for Unix	<p>Select this option to use Microsoft services for Unix to obtain user IDs and group IDs from the domain controller.</p> <p>Select Using LDAP as network information service (RFC2307) if you are using Windows Server 2003 R2 or later.</p>
Using LDAP as network information service (RFC2307)	<p>Select this option to use the RFC2307 schema to obtain user IDs and group IDs from the domain controller.</p>

Selecting an external server

You can select an external server that is used for user authentication.

Table C-286 Information specified on the 6-4. User authentication settings page of the Configuration Wizard (for selecting the external server)

Item	Description
NIS	<p>Select this check box if you want to use an NIS server.</p>

Item	Description
LDAP	Select this check box if you want to use an LDAP server.

When using an NIS server

You can set up an NIS server. After the NIS server information is set or changed, the OS is restarted in the **8. System settings** page.

Table C-287 Information specified on the 6-4. User authentication settings page of the Configuration Wizard (when NIS is selected)

Item	Description
NIS domain	Specify the name of the domain to which the NIS server belongs.
NIS server specification	<p>If you want to use a specific NIS server, select this option, and then specify the following items:</p> <p>Primary NIS server Specify the IP address or server name of the primary NIS server used during normal operation. (An IP address specification is recommended.)</p> <p>Secondary NIS server Specify the IP address or server name of the secondary NIS server used if the primary NIS server has failed. (An IP address specification is recommended.)</p>
Broadcast specification	Select this option if you want to use a network NIS server in broadcast mode.

When using an LDAP server

You can set up an LDAP server that is used for user authentication. After the LDAP server information is changed, the OS is restarted in the **8. System settings** page.

Table C-288 Information specified on the 6-4. User authentication settings page of the Configuration Wizard (when LDAP is selected)

Item	Description
Primary LDAP server	<p>Specify the IP address or server name of the primary LDAP server used during normal operation.</p> <p>In addition to the IP address or server name, you can specify the port number in the Port text box. If you do not specify a port number, the default value (389) is used.</p>
Secondary LDAP server	Specify the IP address or server name of the secondary LDAP server used if the primary LDAP server has failed.

Item	Description
	In addition to the IP address or server name, you can specify the port number in the Port text box. If you do not specify a port number, the default value (389) is used.
LDAP server root DN	Specify the root ID of the LDAP server by using a distinguished name, as in the following example: dc=hitachi,dc=co,dc=jp
LDAP administrator DN	Specify the ID of the LDAP server administrator by using a distinguished name, as in the following example: cn=Administrator,dc=hitachi,dc=co,dc=jp
LDAP administrator password	Specify the password of the LDAP server administrator.
Note: Ask the LDAP server administrator for the information necessary to specify the values.	

9. Completion page

This page completes the setup.

Table C-289 Operations that can be performed on the 9. Completion page of the Configuration Wizard

Button	Function	See
Network & System Configuration	Manage information about interfaces, networks, and external servers.	Network & System Configuration dialog box on page C-178
Cluster Management	Manage clusters, nodes, and resource groups.	Cluster Management dialog box on page C-268
Access Protocol Configuration	Control the operating status or change the configuration definitions of the NFS service, CIFS service, or other services.	Access Protocol Configuration dialog box on page C-217
Create and Share File System	Create and share a file system.	Create and Share File System dialog box on page C-103
Close	Close the Configuration Wizard window.	N/A
Note: N/A = Not applicable.		

HDvM Connection Management dialog box

You can manage the information about Device Manager to which Hitachi File Services Manager is linked in the **HDvM Connection Management** dialog box.

By registering Device Manager information in Hitachi File Services Manager, you can view information about HDI file systems and launch the Hitachi File Services Manager GUI from the Device Manager GUI.

To open the **HDvM Connection Management** dialog box, select **HDvM Connection Management** from the **Go** menu in the global tasks bar area of the Hitachi File Services Manager main window ([Global tasks bar area on page B-4](#)).

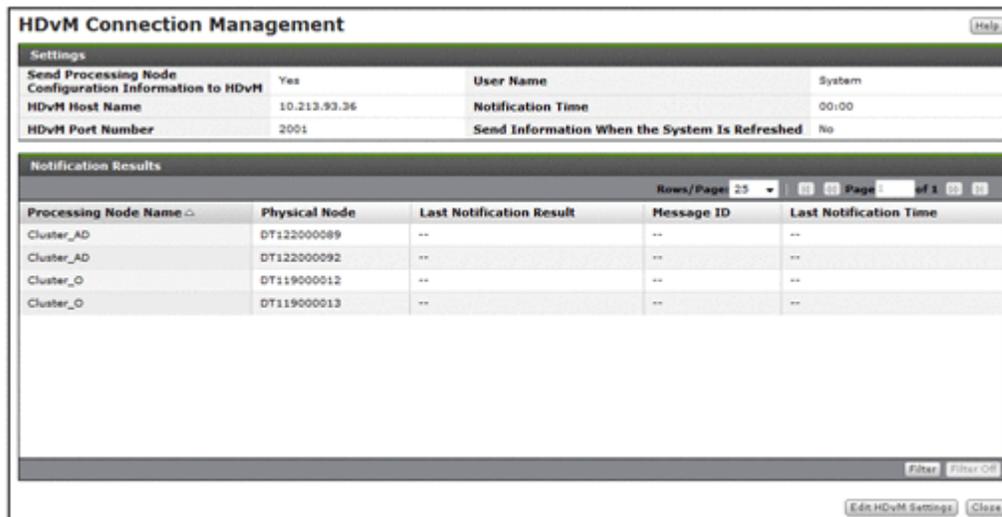


Table C-290 Device Manager information shown in Settings in the HDvM Connection Management dialog box

Item	Description
Send Processing Node Configuration Information to HDvM	Shows whether the configuration information of the processing node is sent to Device Manager. Yes The information is sent. No The information is not sent. If this item is No, -- is shown for the following items.
HDvM Host Name	The Device Manager host name.
HDvM Port Number	The port number used by Device Manager.
User Name	The user name used for authentication on Device Manager.
Notification Time	The time that the configuration information is sent to Device Manager.

Item	Description
Send Information When the System Is Refreshed	Shows whether the configuration information is sent to Device Manager every time the processing node information is refreshed. Yes The information is sent. No The information is not sent.

Table C-291 Information shown in Notify Result in the HDvM Connection Management dialog box

Item	Description
Processing Node Name	The name of the processing node for which the configuration information is sent to Device Manager.
Physical Node	The name of the physical node for which the configuration information is sent to Device Manager.
Last Notification Result	The last result of sending the configuration information. Success The information was sent successfully. Error The information was not sent because of an error. -- is shown if no attempt to send the information has been made.
Message ID	The message that was output for the last attempt to send the configuration information. -- is shown if no message was output.
Last Notification Time	The last time that the configuration information was sent. -- is shown if no attempt to send the information has been made.
Note: Information about nodes with an OS version earlier than 03-00-00-00-00 is not shown.	

Table C-292 Operations that can be performed from the HDvM Connection Management dialog box

Button	Description	See
Edit HDvM Settings	Edits Device Manager information.	Edit HDvM Settings dialog box on page C-335

Edit HDvM Settings dialog box

You can edit Device Manager information in the **Edit HDvM Settings** dialog box.



Note: When you finish entering the required information, click **Test Connection** to check whether you can connect to Device Manager.

Note that, if the management server locale differs from the Web browser locale, the following information is shown according to the management server locale:

- Error information that is returned from Device Manager when an attempt to send configuration information failed
- Information that is shown when you click an error ID in the **Edit HDvM Settings** confirmation dialog box

To open the **Edit HDvM Settings** dialog box, click **Edit HDvM Settings** in the **HDvM Connection Management** dialog box ([HDvM Connection Management dialog box on page C-334](#)).

Table C-293 Device Manager information specified in the Edit HDvM Settings dialog box

Item	Description
Send Processing Node configuration information to HDvM	To send the configuration information of the processing node to Device Manager, select the Yes check box.
HDvM host name	Specify the Device Manager host name.
HDvM port number	Specify the port number used for Device Manager.
User name	Specify the user name used for authentication by Device Manager. Specify a user who has the Peer permission.
Password	Specify the user password used for authentication by Device Manager.
Notification time	Specify the time that the configuration information is sent to Device Manager. Select the hour and minute from the drop-down lists. The information will be sent at the specified time daily.
Send information when the system is refreshed	To send the configuration information to Device Manager every time the processing node is refreshed, select the Yes check box.

Migration Tasks dialog box

You can manage migration tasks as units for which migration is performed.

To open the **Migration Tasks** dialog box, select **Migration Tasks** from the **Go** menu in the global tasks bar area of the Hitachi File Services Manager main window ([Global tasks bar area on page B-4](#)).



Note:

- Do not change or delete the namespace set for a file system for which a migration has already been started. Changing or deleting the namespace for a file system that migrated files rely on might cause migrated files to become inaccessible or might cause subsequent migrations to fail.

- The `.arc` directory, which is used for storing management information, is created directly under a file system for which migration operations have started. Do not delete the `.arc` directory or any files under the directory. If the directory or any files under the directory are deleted, use the `arccorrection` command to restore them.
 - Increasing the number of migration tasks to be executed concurrently puts a heavier load on the system. If too many migration tasks are executing concurrently, putting a heavy load on the system, adjust the schedule so that fewer migration tasks execute concurrently.
 - Migration tasks cannot be set for file systems that reference other HDI data as read-only via the linked HCP. Furthermore, tasks other than the default migration tasks cannot be set for home-directory-roaming file systems or read-write-content-sharing file systems.
-



Tip: Task management information is recorded when a file is accessed or updated in a file system for which migration is set up. The task management information is used to determine whether files are migrated. If a failure occurs, or a migration task is set for a file system for which migration is set, the task management information is rebuilt. If a failure occurs or a migration task is set for a file system for which migration is currently being performed, processing to reconstruct the task management information is executed in the background. If this happens, set a migration task so that the migration is performed again, after the task management information has finished being rebuilt. In order to confirm whether task management information is being or has been rebuilt, check for the KAQM37137-I system message, which is output when rebuild processing starts, and the KAQM37139-I system message, which is output when rebuild processing finishes. For details about how to check system messages, see [List of RAS Information page on page C-164](#).

If a migration task is set up for the first time for a file system on which files have been created and the schedule is set up to perform only one migration, the migration might not be performed. If the migration was not performed, set up another migration task after the KAQM37139-I message has been output.

Some files might not be migrated depending on the status of the system during a migration. To ensure that all files are correctly migrated, set up a migration task schedule so that migrations are performed on a regular basis.

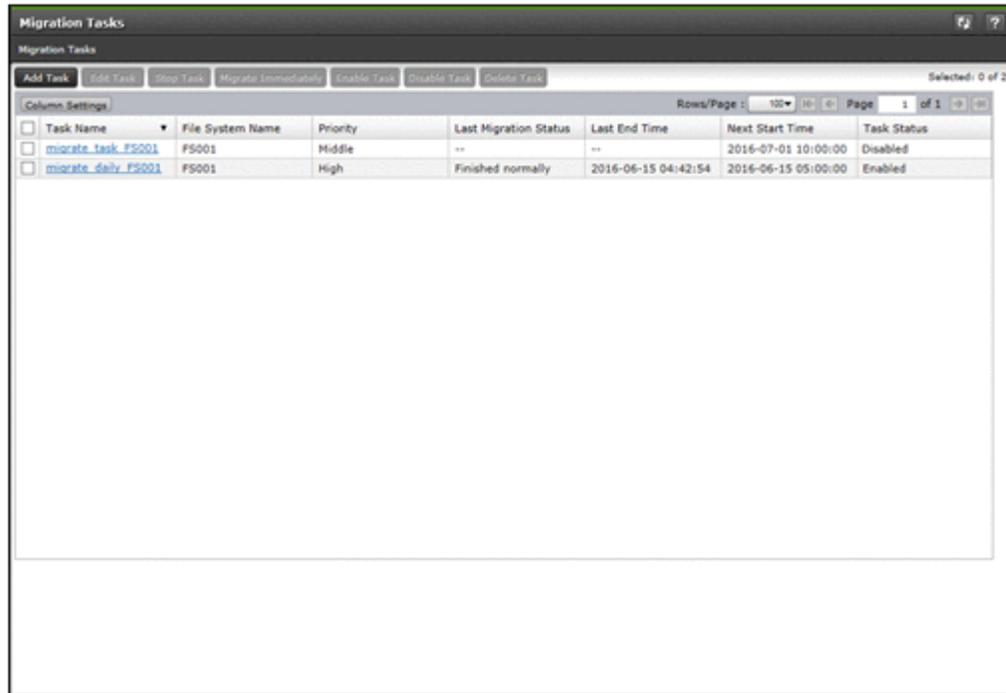


Table C-294 Operations that can be performed from the Migration Tasks dialog box

Button	Function	See
Add Task	Adds a migration task.	Migration Task Wizard on page C-348
Edit Task	Allows the user to edit the settings of the selected migration task.	Migration Task Wizard on page C-348
Stop Task	Stops the selected migration task.	Stop Task dialog box on page C-353
Migrate Immediately	Immediately run the selected migration task.	Migrate Immediately dialog box on page C-354
Enable Task	Enables the selected migration task.	Enable Task dialog box on page C-354
Disable Task	Disables the selected migration task.	Disable Task dialog box on page C-355
Delete Task	Deletes the selected migration task.	Delete Task dialog box on page C-355
Column Settings	Sets the columns to be displayed.	N/A

Button	Function	See
	In the dialog box that appears when you click Column Settings , select the columns you want to display, and then click OK . Note that, if you click Restore Default Settings , all columns will be selected.	
Rows/Page	Select, from the drop-down list box, the maximum number of rows to be displayed on a page.	N/A
Page	When information is displayed on multiple pages, specify, in the text box, the page number of the page you want to view. Alternatively, click  or  to move to the previous or following page, respectively. Similarly, click  or  to move to the first or last page, respectively.	N/A
Note: N/A = Not applicable.		

Table C-295 Information shown in the Migration Tasks dialog box

Item	Description
Task Name	The name of the migration task.
File System Name	The name of the file system corresponding to the migration task.
Priority	The priority level of the migration task to be executed according to a schedule. High The priority is High (1 to 3). Middle The priority is Middle (4 to 6). Low The priority is Low (7 to 10).
Last Migration Status	The status of the migration task that was last executed. Executing The task is executing. Finished normally The task that was last executed ended successfully. Partially failed Processing for the task that was last executed finished, but the migration of some files or directories failed. Use the Download Report dialog box or the <code>arcresultctl</code> command to check the message that was output when the migration failed, resolve the problem, and then execute the task again. Note that, when you execute the task again, files and directories that are not subject to the applicable policy will not be migrated. Failed to start (Message ID)

Item	Description
	<p>An attempt to execute the task failed.</p> <p><i>Interrupted</i></p> <p>Task processing was interrupted because of one of the following reasons: a maximum duration, interruption, or failover occurred; or the file system was unmounted. If the task is interrupted repeatedly, change the maximum duration value.</p> <p>If no migration task was executed, -- is displayed.</p>
Last End Time	<p>The date and time when the migration task that was last executed finished.</p> <p>If no migration task was executed, -- is displayed.</p>
Next Start Time	<p>The date and time when the next migration task is to be executed next time.</p>
Task Status	<p>Indicates whether a migration task is enabled.</p> <p><i>Enabled</i></p> <p>The migration task is enabled.</p> <p><i>Disabled</i></p> <p>The migration task is disabled.</p>

migration-task page

You can use this page to view detailed information about a specific migration task.

To open the *migration-task* page, click the desired *migration-task* link in the **Migration Tasks** dialog box.



Tip: To go back to the **Migration Tasks** dialog box, click the part **Migration Tasks** of **Migration Tasks** > *migration-task* at the top left of the window.

Table C-296 Operations that can be performed from the migration-task page

Button	Function	See
Enable Task	Enables the migration task.	N/A
Disable Task	Disables the migration task.	N/A
Download Report	Downloads a list of files and directories whose migration succeeded or failed (text file in UTF-8 format).	Download Report dialog box on page C-345
Note: N/A = Not applicable.		

Table C-297 Information shown in the migration-task page

Item	Description	See	
Task Name	The name of the migration task.	N/A	
File System Name	The name of the file system.	N/A	
Task Information	Information about the migration task.	Task Information tab on page C-341	
	Task Details		Detailed information about the migration task.
	Policy Details		Detailed information about the migration policy.
History	The migration history.	History tab on page C-344	
Note: N/A = Not applicable.			

Task Information tab

You can use the **Task Information** tab to view the information about the migration task.

Task Details subtab

You can use the **Task Details** subtab to view the detailed information about the migration task.

Table C-298 Information shown on the Task Details subtab of the Task Information tab in the migration-task page

Item	Description
Execution ID	<p>The execution ID of the migration task. The format of the execution ID is as follows:</p> <p><i>date-in-YYYYMMDD-format-execution-serial-number-of-the-migration-task-in-NNN-format</i></p> <p>Note that, if the migration task is currently executing, the execution ID will not be displayed. Instead, -- will be displayed.</p>
Priority	<p>The priority level of the migration task to be executed according to a schedule.</p> <p>High</p> <p>The priority is High (1 to 3).</p> <p>Middle</p> <p>The priority is Middle (4 to 6).</p> <p>Low</p> <p>The priority is Low (7 to 10).</p>
Last Migration Status	<p>The status of the migration task that was last executed.</p> <p>Executing</p>

Item	Description
	<p>The task is executing.</p> <p>Finished normally</p> <p>The task that was last executed ended successfully.</p> <p>Partially failed</p> <p>Processing for the task that was last executed finished, but the migration of some files or directories failed. Use the Download Report dialog box or the <code>arcresultctl</code> command to check the message that was output when the migration failed, resolve the problem, and then execute the task again. Note that, when you execute the task again, files and directories that are not subject to the applicable policy will not be migrated.</p> <p>Failed to start (Message ID)</p> <p>An attempt to execute the task failed.</p> <p>Interrupted</p> <p>Task processing was interrupted because of one of the following reasons: a maximum duration, interruption, or failover occurred; or the file system was unmounted. If the task is interrupted repeatedly, change the maximum duration value.</p>
Progress	<p>The progress of the migration task when Last Migration Status is <code>Executing</code>. Migration tasks are processed in the following order:</p> <p>Waiting</p> <p>The task is waiting until another migration task is completed.</p> <p>Initializing</p> <p>Migration has started.</p> <p>Pre-processing (nn/mm)</p> <p>The progress of the pre-processing is displayed.</p> <p>Processing filters (nn/mm)</p> <p>The progress of the filter processing is displayed.</p> <p>Transferring data (nn/mm)</p> <p>The progress of the data transfer is displayed.</p> <p>Post-processing (nn/mm)</p> <p>The progress of the post-processing is displayed.</p> <p>Note that, if Last Migration Status is not <code>Executing</code>, <code>--</code> is displayed.</p>
Next Start Time	<p>The date and time when the next migration task is to be executed next time.</p>
Last End Time	<p>The date and time when the migration task that was last executed finished.</p> <p>If no migration task was executed, <code>--</code> is displayed.</p>
Number of Targets	<p>The total number of files and directories to be migrated by the migration task.</p>

Item	Description
	Note that, if Progress is <code>Waiting</code> , <code>Initializing</code> , <code>Pre-processing</code> , or <code>Processing filters</code> , <code>0</code> is displayed.
Number of Successful Migrations	The total number of files and directories that were successfully migrated.
Number of Failed Migrations	The total number of files and directories that could not be migrated.
Total Size of Files Migrated Successfully	The total size of files that were successfully migrated (in MB).
Total Size of Files That Failed to Be Migrated	The total size of files that were could not be migrated (in MB).
Work Space Used	<p>The amount of used work space when the migration task was run (in GB).</p> <p>Note that, if the migration task is running or the Active File Migration function is not being used, <code>--</code> is displayed. In addition, when the capacity of the work space is insufficient, <code>Overflowed</code> is displayed. When an error occurs in the work space, <code>Failed to obtain the amount of used space</code> is displayed.</p>
Task Comment	The comment.
Interval	The interval at which the migration task is executed.
Maximum Duration	The maximum duration for the migration task.
Task Status	<p>Indicates whether a migration task is enabled.</p> <p><code>Enabled</code></p> <p>The migration task is enabled.</p> <p><code>Disabled</code></p> <p>The migration task is disabled.</p>
Migration Results	Information about the migration task.
	<p>Successful</p> <p>Detailed information about the files and directories that were successfully migrated.</p> <p>New File</p> <p>The number of files that were created.</p> <p>Data Changes</p> <p>The number of files whose data was changed.</p> <p>Attribute Changes</p> <p>The number of files for which only the attribute was changed.</p> <p>Directories</p> <p>The number of directories.</p>
	<p>Failed</p> <p>If you click the <code>Details information</code> link, information about the failed migration task is displayed.</p> <p>For details about the Failed dialog box that appears when you click the <code>Details information</code> link, see Failed dialog box on page C-345.</p>

Policy Details subtab

You can use the **Policy Details** subtab to view the detailed information about the migration policy.

Table C-299 Information shown on the Policy Details subtab of the Task Information tab in the migration-task page

Item	Description
Policy ID	The policy ID.
Filter condition	If you click the Condition link, a list of selection conditions for the files set for the policy is displayed. For details about the Policy Information dialog box that appears when you click the Condition link, see Policy Information dialog box on page C-346 .

History tab

You can use the **History** tab to view the migration history.

Table C-300 Operations that can be performed from the History tab in the migration-task page

Item	Description
History Data	From the history data, select, from the drop-down list box, the data to be displayed in the graph. All Select to display all data. File Count Select to display the number of files that were migrated. File Size Select to display the size of the files that were migrated.
Time Range	Select, from the drop-down list box, the period for which history data is to be displayed in the graph. Past 1 day Select to display data for the past one day. Past 1 week Select to display data for the past one week. Past 1 month Select to display data for the past one month. Past 3 months Select to display data for the past three months. Past 6 months Select to display data for the past six months. Past 1 year

Item	Description
	Select to display data for the past one year.
Download all data as csv file	Click this to download a CSV file containing history data of the past one year.

Download Report dialog box

You can use the **Download Report** dialog box to download a list of the files and directories whose migration succeeded or failed (text file in UTF-8 format).

To open the **Download Report** dialog box, click **Download Report** on the **Task Details** subtab of the *migration-task* page in the **Migration Tasks** dialog box.



Note:

- If you stop a task that is currently executing, only the files and directories that have been migrated at the time that the task is stopped will be recorded.
- Files whose paths contain multi-byte characters other than Unicode (UTF-8) characters will not be correctly recorded.

Table C-301 Operations that can be performed from the Download Report dialog box

Item	Description
Migration results list	Select the radio button corresponding to the report to be downloaded. List of successful migrations Select to download a list of files and directories that were successfully migrated. List of failed migrations Select to download a list of files and directories whose migration failed.
Download	Download the report that was selected for Migration results list .

Failed dialog box

You can use the **Failed** dialog box to check a failed migration task.

To open the **Failed** dialog box, on the *migration-task* page in the **Migration Tasks** dialog box, click the *Details information* link of **Failed** on the **Task Details** subtab of the **Task Information** tab.

Table C-302 Operations that can be performed from the Failed dialog box

Button	Description
Rows/Page	Select, from the drop-down list box, the maximum number of rows to be displayed on a page.
Page	When information is displayed on multiple pages, specify, in the text box, the page number of the page you want to view. Alternatively, click  or  to move to the previous or following page, respectively. Similarly, click  or  to move to the first or last page, respectively.

Table C-303 Information shown in the Failed dialog box

Item	Description
Message ID	The message ID of the message that includes the cause of the failure when the migration of files and directories fails.
Count	The total number of files and directories whose migration failed due to the cause included in the message indicated by Message ID .

Policy Information dialog box

You can use the **Policy Information** dialog box to view, add, or edit the selection conditions for files that are set for the policy. A maximum of 20 selection conditions can be set for a policy.

The following shows how to open the **Policy Information** dialog box:

- On the *migration-task* page in the **Migration Tasks** dialog box, click the `Condition` link of **Filter condition** on the **Policy Details** subtab of the **Task Information** tab.
- Click **Add** or **Edit** on the **4. Policy Settings** page of the Migration Task Wizard.
- Click **Condition** on the **5. Confirmation** page of the Migration Task Wizard.

Table C-304 Information shown in the Policy Information dialog box

Item	Description
Attribute	Displays the type of selection condition for files.
Conditions	Displays the comparison operator used for a selection condition for files.
Value	Displays the value of a selection condition for files.

Table C-305 Operations that can be performed from the Policy Information dialog box

Button	Description
Add	<p>You can add a selection condition by specifying the selection condition by using the drop-down list boxes and text boxes under this button, and then clicking Add.</p> <p>Each selection condition consists of the following items in the given order: Attribute, Condition, and Value. For details about the values that can be specified for each item, see Table C-306 Selection conditions that can be specified on page C-347.</p>
Edit	<p>You can edit a selection condition by selecting the condition to be edited from the list, using the drop-down list boxes and text boxes under this button to specify the selection condition, and then clicking Edit.</p> <p>Each selection condition consists of the following items in the given order: Attribute, Condition, and Value. For details about the values that can be specified for each item, see Table C-306 Selection conditions that can be specified on page C-347.</p>
Delete	You can delete the selected selection condition.

Table C-306 Selection conditions that can be specified

Attribute	Conditions	Value
File Extension	is is not	Specify the file extensions by using no more than 4,095 bytes. Do not include a period (.). Upper-case and lower-case letters are distinguished.
File Name	is is not	Specify a file to be moved or not moved using no more than 4,095 bytes. Upper-case and lower-case letters are distinguished. Only Unicode (UTF-8) characters are searched for as multibyte characters.
Directory Path	starts with does not start with	Specify an absolute path of the directory, using no more than 4,073 bytes. Upper-case and lower-case letters are distinguished. All files under the specified directory are targeted for migration. For example, specify <code>example/tmp</code> when targeting files under <code>/mnt/fs01/example/tmp/</code> . Only Unicode (UTF-8) characters are searched for as multibyte characters.
Last Accessed Time (atime)#	is (in local time of the node) is not (in local time of the node)	One of the following options is selected to determine. Specify a specific date and time.

Attribute	Conditions	Value
Last Change Time (attributes change time (ctime)), Last Modified Time (data modification time (mtime))	before (in local time of the node) after (in local time of the node)	Select a date using the  icon to the right. Specify relative date and time based on the current date and time. See the followed example and the files that are targeted in the case of the migration start date and time is at 12:30:00 on March 6. is Now-5 day(s) : The files of 12:30:00 on March 1 after Now-3 hour(s) : The files of 9:30:01 on March 6 or later before Now-0 day(s) : The files of 12:29:59 on March 6 or earlier
File Size	is is not greater than less than	Specify the file size by using an integer consisting, and then select a unit (BYTE , KB , MB , or GB) from the drop-down list box. For the file size, specify an integer in one of the following ranges depending on the unit: - BYTE : 1 to 1,125,899,906,842,624 - KB : 1 to 1,099,511,627,776 - MB : 1 to 1,073,741,824 - GB : 1 to 1,048,576
Type of Change	is is not	Select a data modification type (Created , Data was changed , or Attribute was changed) from the drop-down list box.
#: WORM files cannot be searched by access time because retention periods are set for the <code>atime</code> of WORM files. For details about WORM files, see the <i>File System Protocols (CIFS/NFS) Administrator's Guide</i> .		

Migration Task Wizard

You can use the Migration Task Wizard to create or edit a migration task. A maximum of 10 tasks can be set for a file system.

To open the Migration Task Wizard, click **Add Task** in the **Migration Tasks** dialog box. Alternatively, select the name of the task to be edited, and then click **Edit Task**. When the Migration Task Wizard appears, the **1. Introduction** page is displayed first.

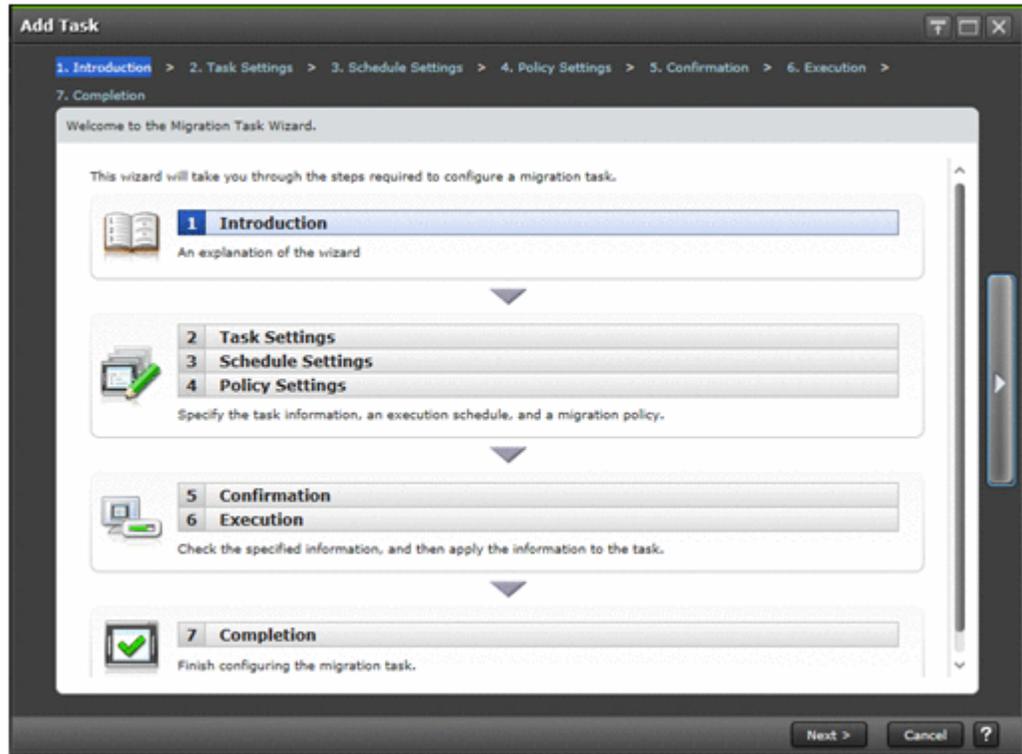


Table C-307 Pages shown for the Migration Task Wizard

Page	Description	See
1. Introduction	Check the information shown, and then click Next > .	N/A
2. Task Settings	Specify the necessary information, and then click Next > .	2. Task Settings page on page C-350
3. Schedule Settings	Specify the necessary information, and then click Next > .	3. Schedule Settings page on page C-350
4. Policy Settings	Specify the necessary information, and then click Next > .	4. Policy Settings page on page C-351
5. Confirmation	Check the displayed information, select the Yes, I have confirmed the above settings. check box, and then click Apply .	N/A
6. Execution	After settings have been configured, the 7. Completion page is automatically displayed.	N/A
7. Completion	Check the displayed information, and then click Finish .	N/A

Note: N/A = Not applicable.

2. Task Settings page

You can use this page to specify the name of the migration task and other information.

Table C-308 Information specified on the 2. Task Settings page in the Migration Task Wizard

Item	Description
File system name	Specify the name of the file system. You can also select a file system from the File Systems dialog box (File Systems dialog box on page C-352) that appears when you click Select File System . Note that you cannot change this setting if you are editing an existing migration task.
Task name	Specify the name of the migration task by using no more than 32 characters. You can use alphanumeric characters and underscores (_). Specify a name that is unique in the file system. Note that you cannot change this setting if you are editing an existing migration task.
Task comment	Specify a comment by using no more than 256 bytes. You can use any alphanumeric character, exclamation mark (!), hash mark (#), dollar sign (\$), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), colon (:), semicolon (;), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left square bracket ([), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (), right curly bracket (}), tilde (~), space, and multi-byte characters that are encoded in UTF-8.
Priority	Select, from the drop-down list box, the priority level of the migration task to be executed according to a schedule. High Select to specify High. The number 3 will be set as the numerical priority level. Middle Select to specify Middle. The number 5 will be set as the numerical priority level. Low Select to specify Low. The number 7 will be set as the numerical priority level.

3. Schedule Settings page

You can use this page to specify the schedule of the migration task.

Table C-309 Information specified on the 3. Schedule Settings page in the Migration Task Wizard

Item	Description
Start date	Select the date on which the migration task will be run for the first time, by using the icon  on the right.
Start time	To run on a specific date and time, specify the time in <i>HH:MM</i> format. Be sure to specify a time in the future.
Interval	Specify the interval at which the migration task is to be run, by specifying a value in the range from 10 minutes to 1 month. Note that, if the target file system is a home-directory-roaming file system (for which the default setting is 1 hour) or read-write-content-sharing file system (for which the default setting is 10 minutes), you cannot change the default value to a value exceeding 1 hour.
Maximum Duration	Specify the time at which the migration task will be interrupted, by specifying a value in the range from 0 to 60 hours. If you do not want to specify a time, specify 0. Note that, if the target file system is a home-directory-roaming file system or read-write-content-sharing file system, you cannot change the value from the default setting (0).

4. Policy Settings page

You can use this page to specify migration policies. The maximum number of migration policies is 10. If you do not specify a policy, all files will be migrated. Note that, if the target file system is a home-directory-roaming file system or read-write-content-sharing file system, you cannot set any migration policies.

Table C-310 Information shown on the 4. Policy Settings page in the Migration Task Wizard

Item	Description
Policies	The policy ID of the specified policy. If no policy is specified, No Data is displayed.

Table C-311 Operations that can be performed from the 4. Policy Settings page in the Migration Task Wizard

Button	Description	See
Add	Adds a policy.	Policy Information dialog box on page C-346

Button	Description	See
Edit	Edits the settings of the selected policy.	Policy Information dialog box on page C-346
Delete	Deletes the selected policy.	N/A
Note: N/A = Not applicable.		

File Systems dialog box

You can use the **File Systems** dialog box to select a file system.

To open the **File Systems** dialog box, click **Select File System** on the **2. Task Settings** page of the Migration Task Wizard.

Table C-312 Operations that can be performed from the File Systems dialog box

Button	Description
Column Settings	Sets the columns to be displayed. In the dialog box that appears when you click Column Settings , select the columns you want to display, and then click OK . Note that, if you click Restore Default Settings , all columns will be selected.
Rows/Page	Select, from the drop-down list box, the maximum number of rows to be displayed on a page.
Page	When information is displayed on multiple pages, specify, in the text box, the page number of the page you want to view. Alternatively, click  or  to move to the previous or following page, respectively. Similarly, click  or  to move to the first or last page, respectively.

Table C-313 Information shown in the File Systems dialog box

Item	Description
Name	The name of the file system.
Mount Status	The status of the file system. Online (RW) The file system is mounted with both read and write operations permitted. Online (RO) The file system is mounted as read-only. Unmounted The file system is unmounted.

Item	Description
	<p>Expanding</p> <p>The file system is being expanded or an error occurred during expansion processing. Wait a while, and then refresh the processing node information. If the status does not change, an error might have occurred during processing. Obtain all the log data, and then inform maintenance personnel.</p> <p>Reclaiming</p> <p>The unused area of the virtual LUs that are used for the file system is being released.</p> <p>Data corrupted</p> <p>The file system is blocked because of an error in the OS or a pool capacity shortage.</p> <p>Take corrective action by referring to the <i>Cluster Troubleshooting Guide</i>.</p> <p>Device error</p> <p>The file system is blocked because of an error in the LU (multiple drive failure).</p> <p>Take corrective action by referring to the <i>Cluster Troubleshooting Guide</i>.</p> <p>Unknown error</p> <p>Information about the file system could not be obtained.</p>
Namespace Type	<p>Displays how the file system is linked to the HCP system.</p> <p>File System</p> <p>The file system is linked to the HCP system at the file system level.</p> <p>Subtree</p> <p>The file system is linked to the HCP system at the share level.</p>
Target Namespace	<p>The namespace for the HCP system to which data will be migrated.</p>

Stop Task dialog box

You can use the **Stop Task** dialog box to stop a migration task.

To open the **Stop Task** dialog box, click **Stop Task** on the **Migration Tasks** dialog box.

Table C-314 Information displayed in the Stop Task dialog box and the operations that can be performed

Item	Description	See
Migration Task Information	Information about the migration task.	Table C-295 Information shown in the Migration Tasks

Item	Description	See
		dialog box on page C-339
Apply	After selecting the I have read the above warning. you can stop the migration task.	N/A
Note: N/A = Not applicable.		

Migrate Immediately dialog box

You can use the **Migrate Immediately** dialog box to immediately run a migration task.

To open the **Migrate Immediately** dialog box, click **Migrate Immediately** on the **Migration Tasks** dialog box.

Table C-315 Information displayed in the Migrate Immediately dialog box and the operations that can be performed

Item	Description	See
Migration Task Information	Information about the migration task.	Table C-295 Information shown in the Migration Tasks dialog box on page C-339
Apply	After selecting the I have confirmed the above settings. you can immediately run a migration task.	N/A
Note: N/A = Not applicable.		

Enable Task dialog box

You can use the **Enable Task** dialog box to enable a migration task.

To open the **Enable Task** dialog box, click **Enable Task** in the **Migration Tasks** dialog box or on the *migration-task* page in the **Migration Tasks** dialog box.

Table C-316 Information displayed in the Enable Task dialog box and the operations that can be performed

Item	Description	See
Migration Task Information	Information about the migration task.	Table C-295 Information shown in the Migration Tasks dialog box on page C-339

Item	Description	See
Apply	After selecting the I have read the above warning. you can enable a migration task.	N/A
Note: N/A = Not applicable.		

Disable Task dialog box

You can use the **Disable Task** dialog box to disable a migration task.

To open the **Disable Task** dialog box, click **Disable Task** in the **Migration Tasks** dialog box or on the *migration-task* page in the **Migration Tasks** dialog box.

Table C-317 Information displayed in the Disable Task dialog box and the operations that can be performed

Item	Description	See
Migration Task Information	Information about the migration task.	Table C-295 Information shown in the Migration Tasks dialog box on page C-339
Apply	After selecting the I have confirmed the above settings. you can disable a migration task.	N/A
Note: N/A = Not applicable.		

Delete Task dialog box

You can use the **Delete Task** dialog box to delete a migration task.

Note that, if the target file system is a home-directory-roaming file system or read-write-content-sharing file system, you cannot delete the migration task or its policies.

To open the **Delete Task** dialog box, click **Delete Task** on the **Migration Tasks** dialog box.

Table C-318 Information displayed in the Delete Task dialog box and the operations that can be performed

Item	Description	See
Migration Task Information	Information about the migration task.	Table C-295 Information shown in the Migration Tasks

Item	Description	See
		dialog box on page C-339
Apply	After selecting the I have read the above warning. you can delete a migration task.	N/A
Note: N/A = Not applicable.		



Operation performed by end users

End users registered on the HDI system, the NIS server, or the LDAP server (used for user authentication) can use the GUI to view information such as information about file shares and quota information as well as change their logon password. This appendix explains how to use the GUI as an end-user.

- [List of operations](#)
- [Logging on](#)
- [Basic GUI operations](#)
- [GUI reference](#)

List of operations

As an end user, you can perform the following tasks:

- View a list of NFS file shares (see [List of File Shares page \(for List of NFS File Shares\) on page D-3](#)).
- View a list of CIFS file shares (see [List of File Shares page \(for List of CIFS File Shares\) on page D-4](#)).
- View quota information set for a user (see [Display Quota page \(for User Quota Info.\) on page D-4](#)).
- View quota information set for a group (see [Display Quota page \(for Group Quota Info.\) on page D-6](#)).
- Change your log on password (see [Password Setup page on page D-8](#)).
- View and edit user comments (see [User Info. Setup page on page D-8](#)).

Logging on

You can open the log on window by specifying the following URL in a Web browser.

`https://virtual-IP-address-of-target-node/index.cgi`

Specify an ID and password, and then click **Login**. The **List of File Shares** page (for List of NFS File Shares) is shown.

To log off, click **Close**. Log off operations are not performed if you close your Web browser.

Basic GUI operations

This section describes the basic operations of the GUI used by end users.

GUI layout

The following figure shows the layout of the GUI used by end users.

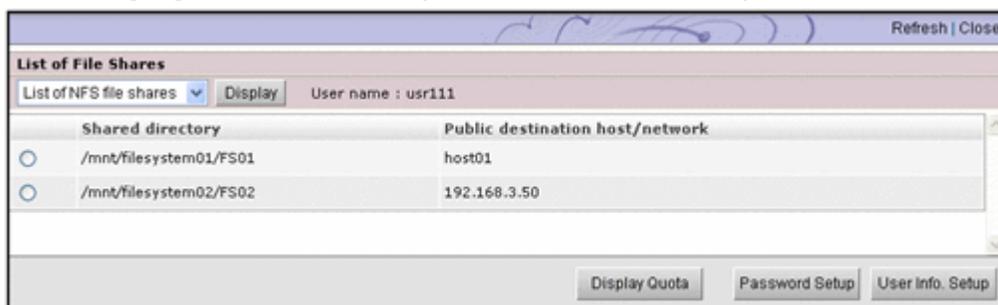


Figure D-1 GUI layout (for end users)

The following explains the components common to all pages.

Refresh

Click to refresh the information displayed in a page used to view a list or status. Although **Refresh** also appears in other pages, clicking **Refresh** in such pages does not refresh any information.

Close

Click to close the current window.

User name

Name of the logged-on user.

Notes about using the GUI

Note the following points when you use the GUI:

- You will be forced to log off if you do not access the program for 30 minutes or more during your log on session.
- If a failover occurs on the node that you are logged on to, you will be forced to log off.
- When using a wheel mouse, do not rotate the wheel while pressing the **Shift** key. This operation might cause the page 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 off by clicking **Close**, and then log on again.
If **Close** is not displayed, click the **X** on the title bar to close the window, and then log on again.
- Do not use the Web browser menu (or shortcuts) to perform any operations other than the following:
 - Change text size
 - Copy
 - Paste

GUI reference

This section describes the GUI windows used by end users.

List of File Shares page (for List of NFS File Shares)

In the **List of File Shares** page (for `List of NFS File Shares`), an end user can view a list of NFS shares.

You can view the **List of File Shares** page (for `List of NFS File Shares`) by selecting **List of NFS file shares** in the drop-down list and then clicking **Display** in the **List of File Shares** page.

The following table lists the information shown in the **List of File Shares** page (for `List of NFS File Shares`).

Table D-1 Information displayed in the List of File Shares page (for List of NFS File Shares)

Item	Description
Shared directory	Name of a shared directory
Public destination host/network	Public destination host or network

List of File Shares page (for List of CIFS File Shares)

In the **List of File Shares** page (for List of CIFS File Shares), an end user can view a list of CIFS shares.

You can view the **List of File Shares** page (for List of CIFS File Shares) by selecting **List of CIFS file shares** from the drop-down list and then clicking **Display** in the **List of File Shares** page.

The following table lists the information shown in the **List of File Shares** page (for List of CIFS File Shares).

Table D-2 Information displayed in the List of File Shares page (for List of CIFS File Shares)

Item	Description
Name of file share	Name of a CIFS share
Shared directory	Name of a shared directory
Comment for file share	Comment for the CIFS share

Display Quota page (for User Quota Info.)

In the **Display Quota** page (for User Quota Info.), end users can view their own quota information set for each file system.

You can view the **Display Quota** page (for User Quota Info.) by selecting a shared directory or share name and then clicking **Display Quota** in the **List of File Shares** page.

The following table lists the user quota information shown in the **Display Quota** page (for User Quota Info.).

Table D-3 User quota information displayed in the Display Quota page (for User Quota Info.)

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.

Item	Description
	For an NFS share, Shared directory displays the name of the shared directory whose quota information is being viewed.
Current used block capacity	Amount of block space being used by each user (units: MB) Shown in red if the amount exceeds the value set as the soft limit or reaches the hard limit. The displayed value is rounded up to the nearest ones place. If there is less than 1 MB left before the amount reaches the Hard limit of block , it might not be possible to create a new file.
Soft limit of block	Soft limit (warning value) for block usage
Hard limit of block	Hard limit (upper bound) for block usage
Block grace period	Remaining grace time until new blocks can no longer be assigned after the block usage exceeds the soft limit. Displayed in one of the following formats: <i>n days</i> The remaining grace time is 24 hours or longer. For example, <i>1 days</i> appears if there are 24 hours or more, but less than 48 hours remaining. <i>n hours</i> The remaining grace time is less than 24 hours. The value is shown in orange. For example, <i>0 hours</i> appears if less than 1 hour remains. Over The grace time has elapsed. Shown in red. - The block usage is less than the soft limit.
Current used i-node count	Usage of inode for each user 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 inode usage
Hard limit of i-node	Hard limit (upper bound) for inode usage
i-node grace period	Remaining grace time until files can no longer be created after the inode usage exceeds the soft limit. Displayed in one of the following formats: <i>n days</i> The remaining grace time is 24 hours or longer. For example, <i>1 days</i> appears if there are 24 hours or more, but less than 48 hours remaining. <i>n hours</i> The remaining grace time is less than 24 hours. The value is shown in orange. For example, <i>0 hours</i> appears if less than 1 hour remains. Over

Item	Description
	The grace time has elapsed. Shown in red.
	-
	The user's inode usage is less than the soft limit.

Display Quota page (for Group Quota Info.)

In the **Display Quota** page (for *Group Quota Info.*), end users can view the quota information set for each file system for the group to which they belong.

You can view the **Display Quota** page (for *Group Quota Info.*) by selecting **Group quota info.** from the drop-down list and then clicking **Display** in the **Display Quota** page (for *User Quota Info.*).

The following table lists the group quota information displayed in the **Display Quota** page (for *Group Quota Info.*).

Table D-4 Group quota information displayed in the Display Quota page (for Group Quota Info.)

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. 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-on user belongs
Block	Availability of the block for each group Used capacity Amount of block space being used Shown in red if the amount exceeds the value set as the soft limit or reaches the hard limit. The displayed value is rounded up to the nearest ones place. If there is less than 1 MB left before the amount reaches the Hard limit , it might not be possible to create a new file. Soft limit Soft limit (warning value) for block usage Hard limit Hard limit (upper bound) for block usage Grace period Remaining grace time until new blocks can no longer be assigned after the block usage exceeds the soft limit. Displayed in one of the following forms:

Item	Description
	<p><i>n</i> days The remaining grace time is 24 hours or longer. For example, <i>1 days</i> appears if there are 24 hours or more, but less than 48 hours remaining.</p> <p><i>n</i> hours The remaining grace time is less than 24 hours. The value is shown in orange. For example, <i>0 hours</i> appears if less than 1 hour remains.</p> <p>Over The grace time has elapsed. Shown in red.</p> <p>- The block usage is less than the soft limit.</p>
i-node	<p>Availability of inodes for each group</p> <p>Used count Usage of inode Shown in red if it exceeds the value set as the soft limit or reaches the hard limit.</p> <p>Soft limit Soft limit (warning value) for inode usage by the group</p> <p>Hard limit Hard limit (upper bound) for inode usage by the group</p> <p>Grace period Remaining grace time until files can no longer be created after the inode usage exceeds the soft limit. Displayed in one of the following forms:</p> <p><i>n</i> days The remaining grace time is 24 hours or longer. For example, <i>1 days</i> appears if there are 24 hours or more, but less than 48 hours remaining.</p> <p><i>n</i> hours The remaining grace time is less than 24 hours. The value is shown in orange. For example, <i>0 hours</i> appears if less than 1 hour remains.</p> <p>Over The grace time has elapsed. Shown in red.</p> <p>- The block usage is less than the soft limit.</p>
Block grace period	Block grace period set for the file system to which the shared directory belongs
i-node grace period	inode grace period set for the file system to which the shared directory belongs

Password Setup page

In the **Password Setup** page, an end user who is registered by the HDI system can change his or her log on password. For increased security, end users should change their passwords regularly.

If user information has been registered in the CIFS environment, the change is also applied to the password for CIFS user authentication.

You can view the **Password Setup** page by clicking **Password Setup** in the **List of File Shares** page.

The following table lists the information to be specified in the **Password Setup** page.

Table D-5 Information specified in the Password Setup page

Item	Description
Current password	Enter your current password.
New password	Enter your new password, using from 6 to 20 characters. You can use any alphanumeric character, exclamation mark (!), quote ("), hash mark (#), dollar sign (\$), percent sign (%), ampersand (&), single quotation mark ('), 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 square bracket ([), backslash (\), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (), right curly bracket (}), and tilde (~).
Re-enter new password	Re-enter the new password that you specified in New password .

User Info. Setup page

In the **User Info. Setup** page, a logged-on end user who is registered by the HDI system can edit the comment in his or her user information.

You can view the **User Info. Setup** page by clicking **User Info. Setup** in the **List of File Shares** page.

The following table lists the information displayed in the **User Info. Setup** page.

Table D-6 Information displayed in the User Info. Setup page

Item	Description
User name	User name

Item	Description
UID	User ID
Comment	<p>Comment for the user</p> <p>If you want to change the comment, enter a maximum of 32 characters. You can use any alphanumeric character, hash mark (#), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), hyphen (-), period (.), forward slash (/), semicolon (;), left angle bracket (<), right angle bracket (>), question mark (?), at mark (@), left square bracket ([), right square bracket (]), caret (^), underscore (_), left curly bracket ({), vertical bar (), right curly bracket (}), and tilde (~). You can also specify spaces, but spaces cannot be specified at the beginning nor at the end of the character string. If you leave this item blank, no comment is entered.</p>



Backing up and restoring quota information

This appendix explains how to back up and restore quota information to and from tape devices.

- [Backing up quota information](#)
- [Restoring quota information](#)

Backing up quota information

When you back up quota information, quota information currently set for the target file systems or directories is backed up. If multiple unique directories are specified as backup target base points in the backup target list, quota information is backed up for each directory specified as the base point of a backup target.

The backed up quota information is output as a file to the media used as the backup destination. For a file system, quota information is always output to a file regardless of the setting. For a directory, quota information (subtree quota) is output to a file only when the information is set for the directory.

The following table shows the relationship between the quota information that is backed up and the name of the files where quota information is stored.

Table E-1 Relationship between quota information that is backed up and the files where quota information is stored

Quota information that is backed up		File where quota information is stored
Quotas set for a file system	Default quotas, user quotas, and grace periods	<code>.quota.user</code>
	Group quotas and grace periods	<code>.quota.group</code>
Quotas set for a directory (subtree quota)	Quotas and grace periods for the directory	<code>.quota.subtree</code>
	Default quotas, user quotas, and grace periods	<code>.quota.user</code>
	Group quotas and grace periods	<code>.quota.group</code>

The output location of files that will store quota information differs depending on the directory that is specified as the base point of a backup target.

Reference note:

The directory used as the base point of a backup target differs depending on the backup management software you are using. For details, see the supplementary Backup Restore documentation that is provided with HDI.

Output location when a mount point is specified

If the mount point for the file system is specified as the backup target, the output location for the files storing quota information is as follows:

Output location for quota information for the file system

The files storing the quota information for a file system are created immediately under the following directory on the backup media:

/mnt/path-of-the-backup-target-directory

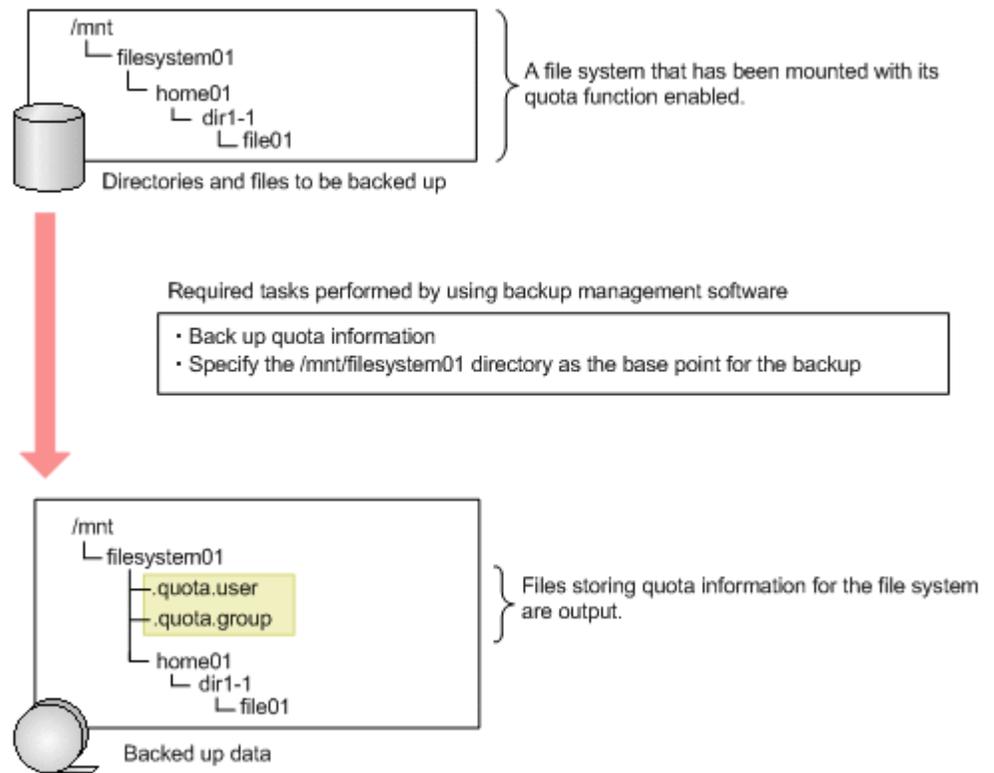


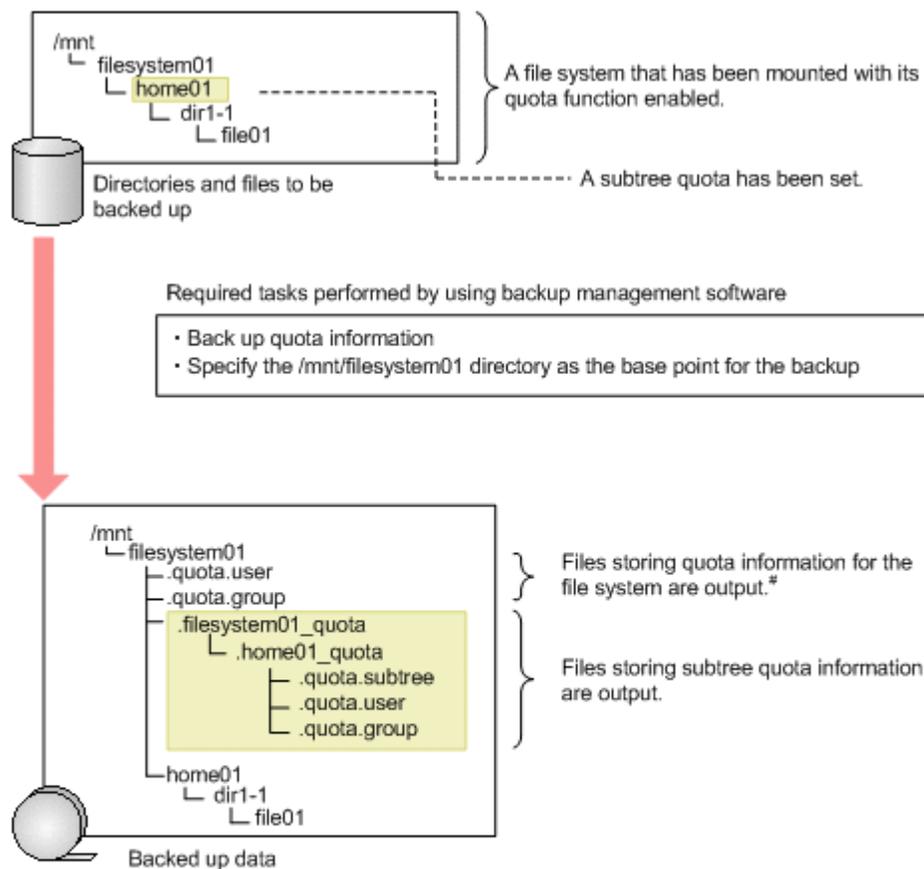
Figure E-1 How the quota information for a file system is output (when the mount point for the file system is specified as the backup target)

For example, if `/mnt/filesystem01` is the backup target, after the backup, the files `.quota.user` and `.quota.group`, which store quota information for the file system, are output directly below the mount point for the media at the backup location.

Output location for subtree quota information

Subtree quota information is output to the following location on the media.

/mnt/path-of-the-backup-target-directory/.file-system-name_quota/.directory-name-where-subtree-quotas-are-set_quota



#: If you back up quota information for a file system that is mounted with its quota function enabled, the files `.quota.user` and `.quota.group` of the file system will be output regardless of whether quota information is set for the file system. If no quota information is set, all values in those files will be 0.

Figure E-2 How the subtree quota information is output (when the mount point for the file system is specified as the backup target)

For example, if `/mnt/filesystem01` has been set for the directory that is the base point of the backup target, and a subtree quota has been set for the `/mnt/filesystem01/home01` directory, after the backup, the `.filesystem01_quota/.home01_quota` directory is created directly below the mount point on the backup destination media. The files `.quota.subtree`, `.quota.user`, and `.quota.group`, which store the subtree quota information, will be output into that directory.

Output location when a directory under the mount point is specified

If a directory under the mount point is specified as the backup target directory, the output location for the files storing quota information is as follows:

Output location for quota information for the file system

The files storing the quota information for a file system are created immediately under the following directory:

`/mnt/path-of-the-backup-target-directory`

If multiple directories under the same file system are specified as backup targets, after the backup, quota information for the file system is also output to the multiple locations.

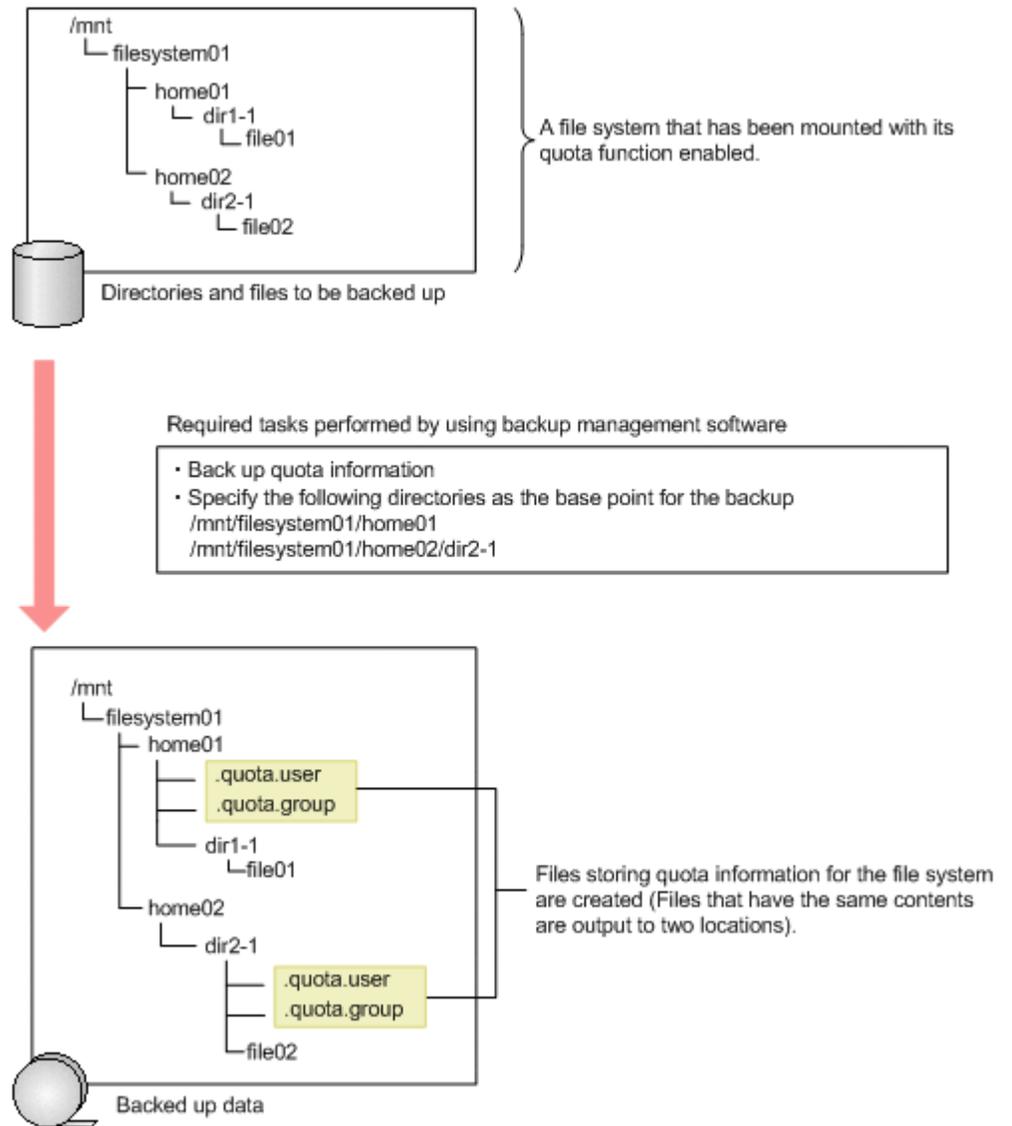


Figure E-3 How the quota information for a file system is output (When directories under the mount point for the file system are specified for the backup target)

For example, if `/mnt/filesystem01/home01` and `/mnt/filesystem01/home02/dir2-1` have been set as the backup targets, after the backup, the `/mnt/filesystem01/home01` and `/mnt/filesystem01/home02/dir2-1` directories are created on the backup destination media. The files `.quota.user` and `.quota.group` that store quota information are output into those directories respectively.

Output location for subtree quota information

Subtree quota information is output to the following location on the media.

/mnt/path-directly-above-the-base-point-of-the-backup-target/.name-of-the-directory-for-which-the-subtree-quota-is-set_quota

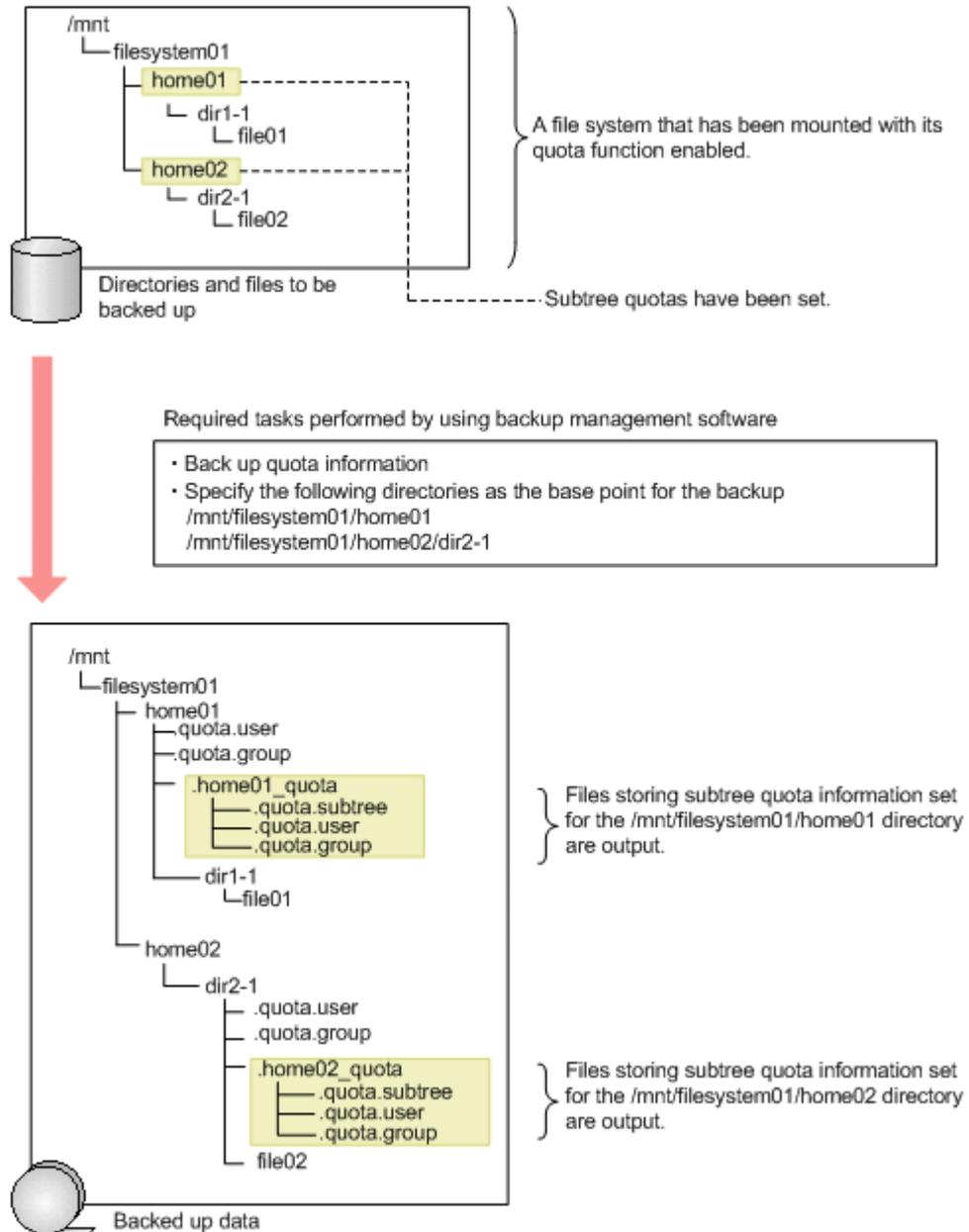


Figure E-4 How the subtree quota information is output (when directories under the mount point for the file system are specified as the backup target)

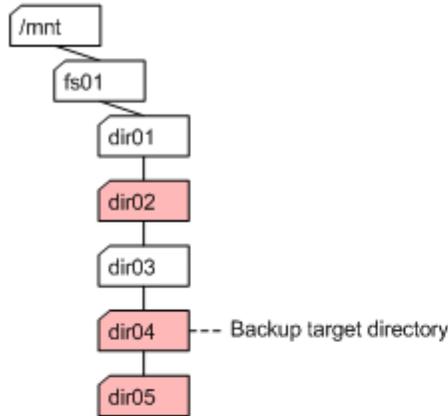
For example, subtree quota information is set in the `/mnt/filesystem01/home01` and `/mnt/filesystem01/home02` directories. In this case, if `/mnt/filesystem01/home01` and `/mnt/filesystem01/home02/dir2-1` have been set as the backup targets, after the backup, the `/mnt/`

filesystem01/.home01_quota and /mnt/filesystem01/home02/.home02_quota directories are created on the backup destination media. The files .quota.subtree, .quota.user, and .quota.group that store subtree quota information are output into those directories respectively.

Cautions when backing up quota information

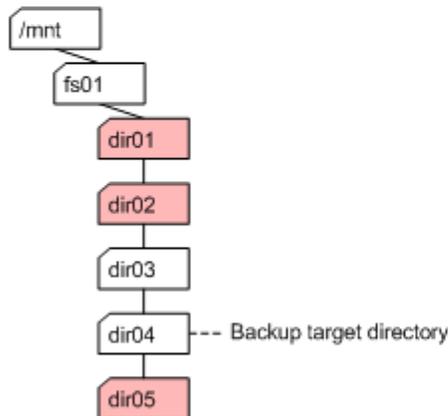
- During a backup operation, do not update quota information that is set on the backup source volume because the integrity of data cannot be guaranteed between quota information set on the backup source volume and quota information backed up to a media.
- When a symbolic link is included in the backup target, do not back up the quota information. If the quota information is backed up when a symbolic link is included in the backup target, quota information for the link destination might be backed up, rather than the quota information for the symbolic link location.
- If a subdirectory of the mount-point directory is specified as the backup target directory, the backup target directory and all the subdirectories are unconditionally assumed to be backup targets for subtree quota information. Additionally, one of the higher-level directories of the backup target directory might become a backup target. This depends on whether a subtree quota is set for the backup target directory. See the examples in the following figure.

If a subtree quota is set for the backup target directory:



Directory name	Whether subtree quota information is backed up
dir02	N
dir04	Y
dir05	Y

If a subtree quota is not set for the backup target directory:



Directory name	Whether subtree quota information is backed up
dir01	N
dir02	Y
dir05	Y

Legend:

- : Directory
- : Directory for which a subtree quota is set
- Y: Backed up
- N: Not backed up

In both examples in the above figure, the backup target directory is `dir04`. In the first example, a subtree quota is set for `dir04`. In this case, the subtree quota information of `dir04` and `dir05` is backed up. The subtree quota information of `dir02` is not backed up.

In the second example, no subtree quota is set for `dir04`. In this case, the subtree quota information of `dir05` and `dir02` is backed up. The subtree quota information of `dir02` is backed up because this directory is closest to `dir04` among the higher-level directories for which a subtree quota is set. The subtree quota information of `dir01` is not backed up.

Restoring quota information

When restoring quota information, specify the files storing the quota information you want to restore. You can specify one or more of the following files: `.quota.user`, `.quota.group`, and `.quota.subtree`.

By restoring the files storing quota information, the quota information is set for the file system or directory for the restore destination. However, depending upon the quota information settings for the file system or directory at the restore destination, system behavior might be as follows:

- If quota information is set in the file system or directory at the restore destination, it is updated with the quota information set when the backup is acquired.
- Directories and files created after a backup is acquired, and quota settings for users and groups added after a backup is acquired, keep the same settings as before the restore operation was performed.
- If a directory has not been prepared in the file system at the restore destination, you cannot restore only subtree quotas, without restoring the directory at the same time. If you attempt to do so, the subtree quotas will not be restored and a warning message will be output.

The following explains the files you specify when restoring quota information at the file system level or directory level, and explains settings of quota information after the restore operation is performed.

Restoring quota information at the file system level

When you restore quota information at the file system level, select all data (directories and files in the file system) and all the files storing the quota information to be restored.

An example is shown below for restoring the quotas set for a file system.

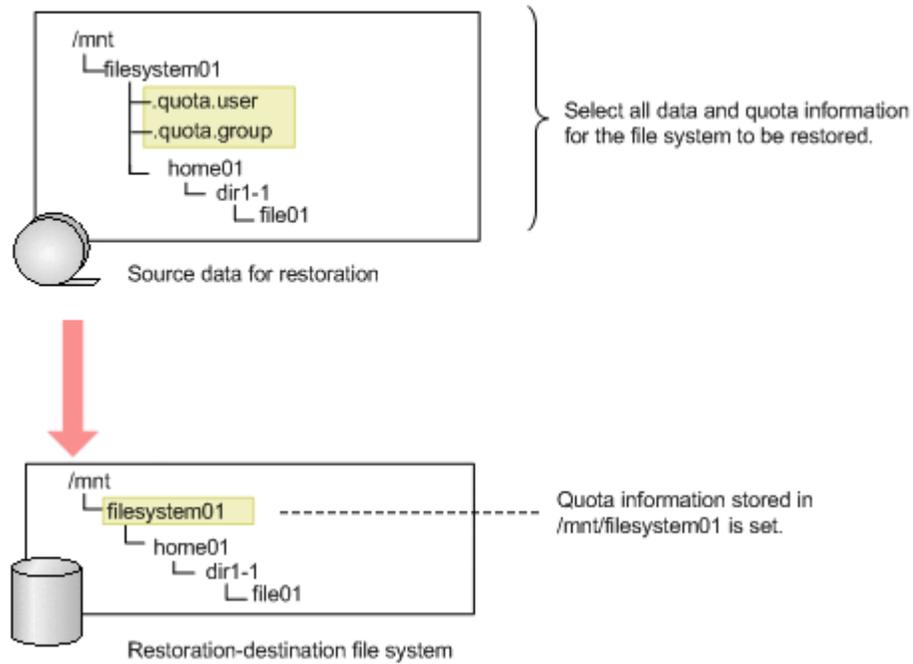


Figure E-5 Restoring data at the file system level (when restoring quotas set for a file system)

The following example shows restoring subtree quotas.

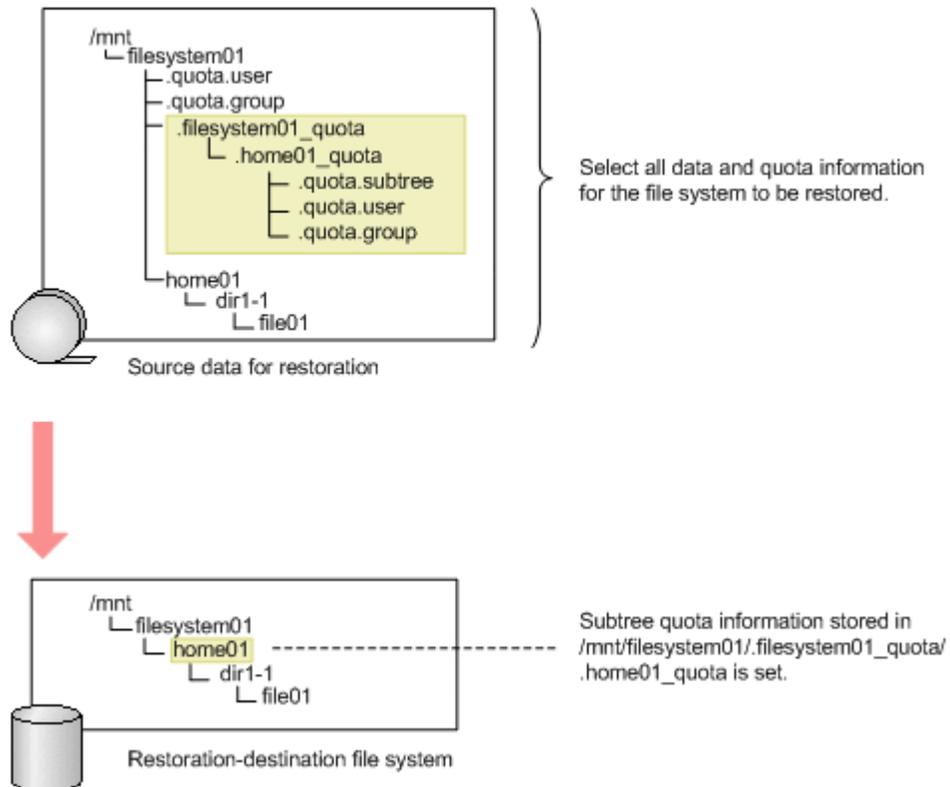


Figure E-6 Restoring data at the file system level (when restoring subtree quotas)

Restoring quota information at the directory level

When you restore quota information at the directory level, select all data (subdirectories and files in the directory) and all the files storing the quota information to be restored.

The following example shows restoring the quotas set for a file system.

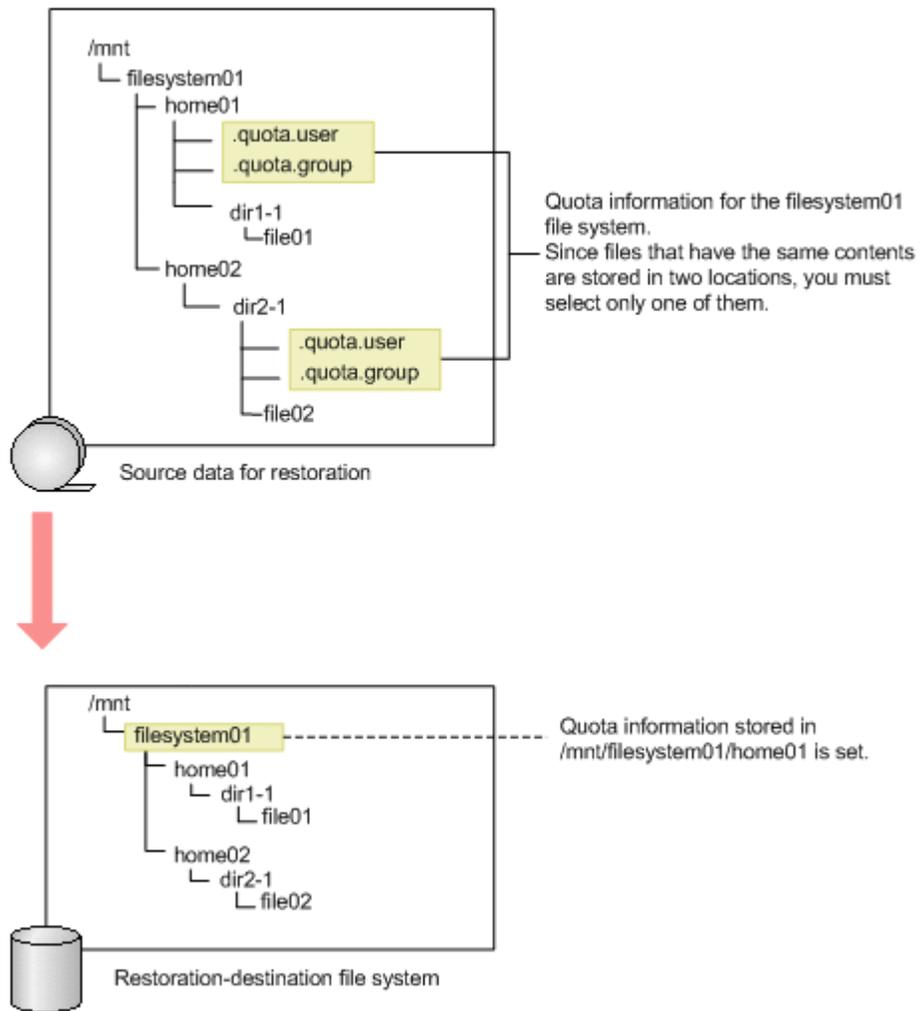


Figure E-7 Restoring data at the directory level (when restoring quotas for a file system)

If there are multiple files storing quota information below the file system that is to be restored, select only one copy each of the `.quota.user` file and the `.quota.group` file.

The following example shows restoring subtree quotas.

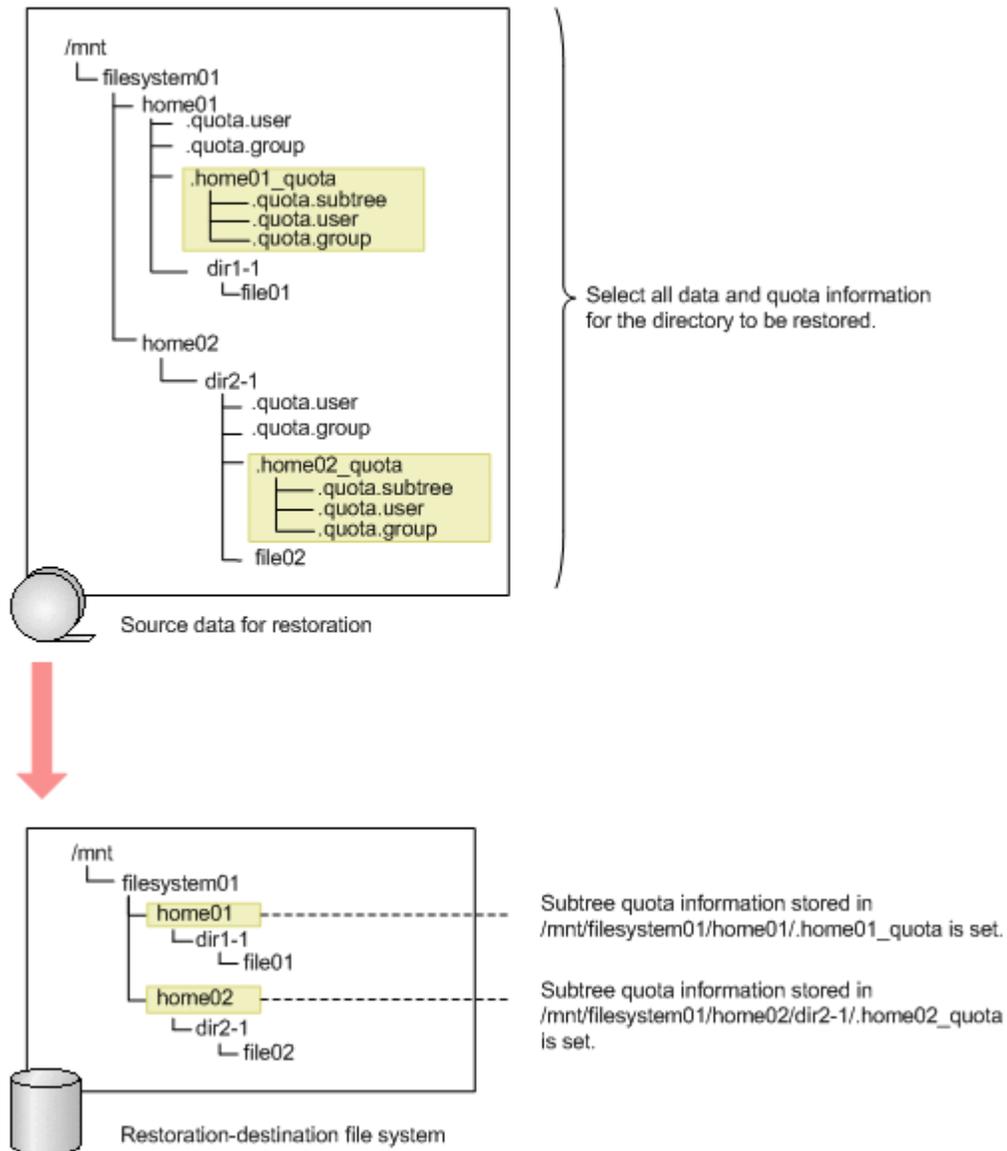


Figure E-8 Restoring data at the directory level (when restoring subtree quotas)

When subtree quotas are restored, subtree quota information is set for the directory that is at a higher level than the restore destination.

Cautions for restoring quota information

Note the following when you restore quota information:

- During a restoration, any quotas that are set for the file systems and directories at the restore destination will be updated to the quota information set in the files `.quota.user`, `.quota.group`, and `.quota.subtree`. When restoring quota information, check if quotas have been set at the restore destination, and if it is OK to update the

quotas at the restore destination to the quotas as they were when the backup was made.

- If multiple `.quota.user` files, `.quota.group` files, or `.quota.subtree` files are restored to the same restore-destination, you might end up restoring the quota information to an unintended state. Therefore, when restoring quota information, Hitachi Data Systems recommends that you do so by selecting one `.quota.user` file, one `.quota.group` file, and one `.quota.subtree` file.
- If you restore a subtree quota to a directory other than the one that you backed up the information from, the subtree quotas might not be restored correctly. In this case, Hitachi Data Systems recommends that you manually set subtree quota instead of restoring the settings from a backup.
- Do not change the quota information set for the restore-destination file system during restoration processing, because the quota information backed up to the media might not be set properly on the restore-destination file system.
- Subtree quotas can also be restored to a directory that has already been used by users, and for which subtree quotas have not been set. In this case, you must use the `stquotaset` command to count the inode usage and block usage of the directories and files under the target directory, and include them in the total for the quota usage.
- When restoring subtree quota information by using the DAR function, select the files `.quota.user`, `.quota.group`, or `.quota.subtree`, not the directory that stores these files.



Reserved words

This appendix lists the words reserved by the system.

- [List of reserved words](#)

List of reserved words

The following table shows the reserved words for cluster, node, and node host names.

Table F-1 List of reserved words for cluster, node, and node host names

Category	Reserved words
A	add, admin
C	CLU_partition, cluster
D	Data_management, debian#, define, delete
F	Failover_policy, Filesystem, for, force
H	ha_parameter, ha_services, hostname
I	in, IP_address
L	localhost#, 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, RUS_management
S	set, show, start, status, stop, SyncImage
T	to
V	VNDB_Fileystem, VNDB_LVM, VNDB_NFS, Vserver
Symbol	One period (.), two periods (..)
<p>Note: The above reserved words cannot be specified for a node host name regardless of whether upper case or lower case is used.</p> <p>#: Only for node host names can these names not be specified.</p>	

The following table shows the reserved words for user names.

Table F-2 List of reserved words for user names

Category	Reserved words
A	avahi, avahi-autoipd
B	backup, bin, bind
D	daemon, Debian-exim
E	enasroot
F	ftp
G	games, gdm, gnats
H	haldaemon, hddsroot, hplip, hsguiroot

Category	Reserved words
I	identd, irc
L	libuuid, libvirt-qemu, list, lp
M	mail, man, messagebus
N	nasroot, news, nobody, ntp
O	offline, online
P	postgres, proftpd, proxy
R	root
S	service, snmp, sshd, statd, sync, sys
T	telnetd
U	uucp
V	vde2-net
W	www-data
Symbol	__groupowner

The following table shows the reserved words for group names.

Table F-3 List of reserved words for group names

Category	Reserved words
A	adm, audio, avahi, avahi-autoipd
B	backup, bin, bind
C	cdrom, crontab
D	daemon, Debian-exim, dialout, dip, disk
E	enasroot
F	fax, floppy, ftp
G	games, gdm, gnats
H	haldaemon, hddsroot, hsguiroot
I	irc
K	kmem, kvm
L	libuuid, libvirt, list, lp, lpadmin
M	mail, man, messagebus, mlocate
N	nasroot, netdev, news, nogroup, ntp
O	operator
P	plugdev, postgres, powerdev, proxy
R	root

Category	Reserved words
S	sasl, scanner, service, shadow, src, ssh, ssl-cert, staff, stb-admin, sudo, sys
T	tape, telnetd, tty
U	users, utmp, uucp
V	vde2-net, video, voice
W	winbindd_priv, www-data

MIB objects

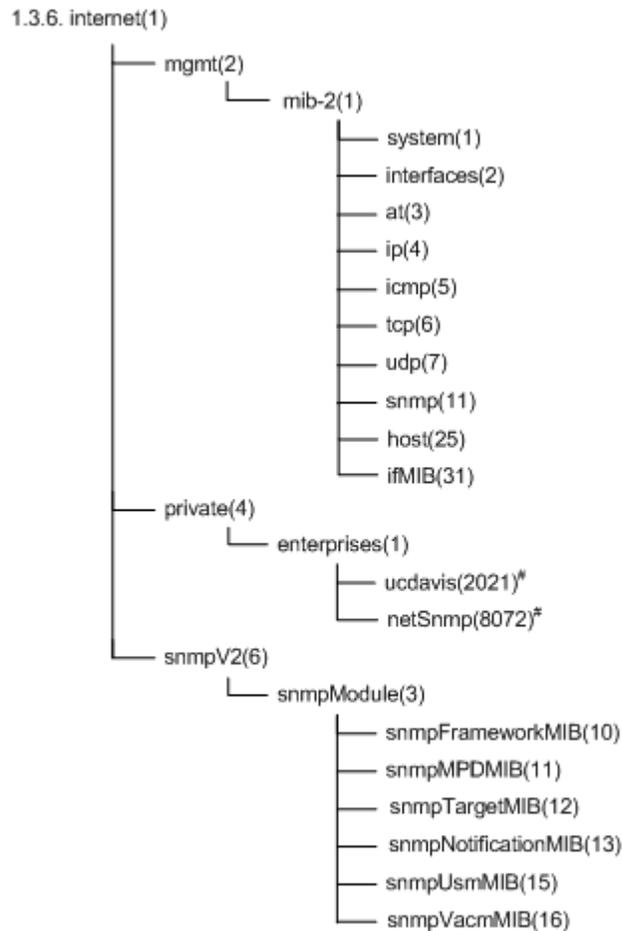
This appendix explains SNMP MIB objects used in the HDI system.

- [List of MIB objects](#)
- [MIB objects for responding to SNMP get requests](#)
- [MIB objects used for SNMP traps](#)

List of MIB objects

This appendix explains MIB objects that are used to respond to SNMP `get` requests in the HDI system, and MIB objects that are used for SNMP traps in the HDI system.

The following figures describe the structures for standard MIB objects and Hitachi's unique Management Information Base (MIB) objects used in the HDI system:



#:
Since the MIB objects in `ucdavis(2021)` and `netSnmp(8072)` for `private(4)` group are functionality provided by the SNMP agent package, they are treated as standard MIB objects.

Figure G-1 Structure for standard MIB objects

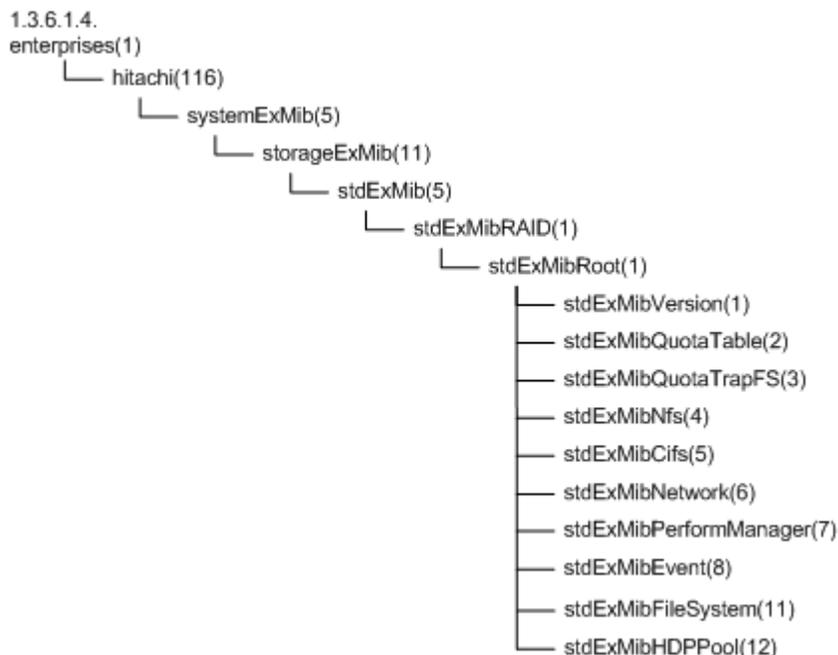


Figure G-2 Groups of MIB objects for responding to SNMP get requests and tables to be referenced (standard MIB objects)

MIB objects for responding to SNMP get requests

The following table lists the environments in which the MIB objects in an HDI system that are used to respond to SNMP `get` requests can be obtained and the tables to be referenced.

Table G-1 Environments in which the MIB objects used to respond to SNMP get requests can be obtained and the tables to be referenced (standard MIB objects)

Group name	Definition RFC number	Description	Tables
1.3.6.1.2.mib-2 (1)	system (1)	This group is for <code>system</code> information.	Table G-3 system (1) group on page G-6
	interfaces (2)	This group is for <code>interfaces</code> information.	Table G-4 interfaces (2) group on page G-6
	at (3)	This group is for <code>at</code> information.	Table G-5 at (3) group on page G-8
	ip (4)	This group is for <code>ip</code> information.	Table G-6 ip (4) group on page G-9

Group name		Definition RFC number	Description	Tables
	icmp (5)	1213	This group is for <code>icmp</code> information.	Table G-7 icmp (5) group on page G-17
	tcp (6)	1213	This group is for <code>tcp</code> information.	Table G-8 tcp (6) group on page G-18
	udp (7)	1213	This group is for <code>udp</code> information.	Table G-9 udp (7) group on page G-20
	snmp (11)	1907	This group is for <code>snmp</code> information.	Table G-10 snmp (11) group on page G-20
	host (25)	2790	This group is for <code>host</code> information.	Table G-11 host (25) group on page G-22
	ifMIB (31)	2233	This group is for <code>ifMIB</code> information.	Table G-12 ifMIB (31) group on page G-28
	ipv6MIB (55)	2465	This group is for <code>ipv6MIB</code> information.	Table G-13 ipv6MIB (55) group on page G-30
1.3.6.1.4.enterprises (1)	ucdavis (2021)	N/A	This group is for <code>ucdavis</code> information.	Table G-14 ucdavis (2021) group on page G-31
	netSnmp (8072)	N/A	This group is for <code>netSnmp</code> information.	Table G-15 netSnmp (8072) group on page G-39
1.3.6.1.6.snmpModules (3)	snmpFrameworkMIB (10)	2271	This group is for <code>snmp</code> management structures.	Table G-16 snmpFrameworkMIB (10) group on page G-41
	snmpMPDMIB (11)	2272	This group is for message processing.	Table G-17 snmpMPDMIB (11) group on page G-41
	snmpTargetMIB (12)	2273	This group is for parameter formation, for message creation.	Table G-18 snmpTargetMIB (12) group on page G-42
	snmpNotificationMIB (13)	2273	This group is for parameter formation, for notification.	Table G-19 snmpNotificationMIB (13) group on page G-44

Group name		Definition RFC number	Description	Tables
	snmpUsmMIB (15)	2274	This group is for security information definition.	Table G-20 snmpUsmMIB (15) group on page G-44
	snmpVacmMIB (16)	2275	This group is for access/control information definition.	Table G-21 snmpVacmMIB (16) group on page G-45

Note: N/A = Not applicable.

Table G-2 Environments in which the MIB objects used to respond to SNMP get requests can be obtained and the tables to be referenced (Hitachi MIB objects)

Group name	Description	Tables
stdExMibVersion (1)	This group is for version information.	Not applicable
stdExMibQuotaTable (2)	This group is for quota management.	Table G-22 stdExMibQuotaTable (2) group on page G-48
stdExMibNfs (4)	This group is for NFS.	Table G-23 stdExMibNfs (4) group on page G-55
stdExMibCifs (5)	This group is for CIFS.	Table G-24 stdExMibCifs (5) group on page G-63
stdExMibNetwork (6)	This group is for the network.	Table G-25 stdExMibNetwork (6) group on page G-63
stdExMibPerformManager (7)	This group is for performance management.	Table G-26 stdExMibPerformManager (7) group on page G-64
stdExMibFileSystem (11)	This group is for file systems.	Table G-27 stdExMibFileSystem (11) group on page G-66
stdExMibHDPPool (12)	This group is for pools.	Table G-28 stdExMibHDPPool (12) group on page G-69

Tables [Table G-3 system \(1\) group on page G-6](#) to [Table G-28 stdExMibHDPPool \(12\) group on page G-69](#) summarize the groups of MIB objects used in responding to SNMP `get` requests. In the tables, the type is described as – for the MIB objects that have no data types and have `Entry` types (which are in table structure and therefore, cannot be accessed).

Table G-3 system (1) group

ID	Object name	Type	Meaning
1	sysDescr (1)	DisplayString	Names or version numbers for the hardware, OS, and network OS.
2	sysObjectID (2)	OBJECT IDENTIFIER	Vendor authentication ID for the network management subsystem.
3	sysUpTime (3)	TimeTicks	Time elapsed since system startup.
4	sysContact (4)	DisplayString	Contact information for the management node.
5	sysName (5)	DisplayString	The name and domain name of the management node.
6	sysLocation (6)	DisplayString	Location in which the management node is set up.
7	sysServices (7)	INTEGER	A value indicating services.
8	sysORLastChange (8)	TimeTicks	The latest value for <code>sysUpTime</code> .
9	sysORTable (9)	-	For each MIB module, lists the functions of the local SNMPv2 entity acting as an agent.
9.1	sysOREntry (1)	-	Contains <code>sysORTable</code> entries.
9.1.1	sysORIndex (1)	INTEGER	A support variable used to identify instances of <code>sysORTable</code> columns and objects. This cannot be obtained.
9.1.2	sysORID (2)	OBJECT IDENTIFIER	Indicates proper identifiers for each MIB module. MIB modules are supported based on the local SNMPv2 entity acting as an agent.
9.1.3	sysORDescr (3)	DisplayString	Defines a text description of the function identified by the corresponding <code>sysORID</code> .
9.1.4	sysORUpTime (4)	TimeStamp	Indicates the value of <code>sysUpTime</code> at the time this overview row was last instantiated.

Table G-4 interfaces (2) group

ID	Object name	Type	Meaning
1	ifNumber (1)	Integer32	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

ID	Object name	Type	Meaning
2.1.1	ifIndex (1)	InterfaceIndex	A number identifying this interface (values are sequential, from 1 to <code>ifNumber</code>)
2.1.2	ifDescr (2)	DisplayString	Information about the interface
2.1.3	ifType (3)	IANAifType	The interface type
2.1.4	ifMtu (4)	Integer32	The maximum size of datagrams that can be transmitted with this interface
2.1.5	ifSpeed (5)	Gauge32	An estimate of the current line speed for this interface ^{#1}
2.1.6	ifPhysAddress (6)	PhysAddress	The physical address immediately below the network layer of this interface
2.1.7	ifAdminStatus (7)	INTEGER	The desired status for this interface Each value represents the following: 1: up, 2: down, 3: testing
2.1.8	ifOperStatus (8)	INTEGER	The current status of this interface Each value represents the following: 1: up, 2: down, 3: testing, 4: unknown, 5: dormant, 6: notPresent, 7: lowerLayerDown
2.1.9	ifLastChange (9)	TimeTicks	The value of <code>sysUpTime</code> at the time at which <code>ifOperStatus</code> was last changed for this interface
2.1.10	ifInOctets (10)	Counter32	The number of octets received with this interface ^{#2}
2.1.11	ifInUcastPkts (11)	Counter32	The number of unicast packets for which the upper protocol has been notified ^{#3}
2.1.12	ifInNUcastPkts (12)	Counter32	The number of non-unicast packets (broadcast or multicast packets) for which the upper protocol has been notified
2.1.13	ifInDiscards (13)	Counter32	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)	Counter32	The number of packets that could not be received because an error occurred within the packet
2.1.15	ifInUnknownProtos (15)	Counter32	The number of packets discarded, because of receiving unsupported protocol
2.1.16	ifOutOctets (16)	Counter32	The number of octets from packets transmitted with this interface ^{#2}

ID	Object name	Type	Meaning
2.1.17	ifOutUcastPkts (17)	Counter32	The number of unicast packets sent by the upper layer ^{#3}
2.1.18	ifOutNUcastPkts (18)	Counter32	The number of non-unicast packets sent by the upper layer
2.1.19	ifOutDiscards (19)	Counter32	The number of packets with no errors, but that were discarded during transmission processing (for which the transmission buffer was insufficient, and so on.)
2.1.20	ifOutErrors (20)	Counter32	The number of packets that could not be sent because of an error
2.1.21	ifOutQLen (21)	Gauge32	The size of the queue for transmission packets
2.1.22	ifSpecific (22)	OBJECT IDENTIFIER	A reference to a MIB defining properties of the interface media The object ID of a MIB is dependent on <i>ifType</i>

#1: The estimated line speed for a GbE interface is 100,000,000 bps. This is the value output by standard MIBs for GbE interfaces. The estimated line speed for 10GbE port or trunking port interfaces is not close to the actual value. The estimate for a 10GbE port is 10,000,000,000, but the output value is 4,294,967,295. The output value for a trunking port is always 100,000,000.

#2: ifInOctets and ifOutOctets are 32-bit counters, and are reset if there is 100 Mbps of traffic within 5 minutes.

#3: ifInUcastPkts and ifOutUcastPkts are 32-bit counters, and might be reset if the system is continuously run for a long time.

Table G-5 at (3) group

ID	Object name	Type	Meaning
1	atTable (1)	-	The table for <i>NetworkAddress</i> for the corresponding value of the physical address
1.1	atEntry (1)	-	A list related to one <i>NetworkAddress</i> for the corresponding value of the physical address for each entry
1.1.1	atIfIndex (1)	INTEGER	The value of <i>ifIndex</i> for the corresponding interface
1.1.2	atPhysAddress (2)	PhysAddress	The physical address
1.1.3	atNetAddress (3)	NetworkAddresses	The IP address corresponding to <i>atPhysAddress</i> , depending on the media

Table G-6 ip (4) group

ID	Object name	Type	Meaning
1	ipForwarding (1)	INTEGER	Availability of IP relay functionality (whether or not operation is performed by gateway) Each value represents the following: 1: forwarding, 2: notForwarding
2	ipDefaultTTL (2)	Integer32	The default TTL setting in IP headers
3	ipInReceives (3)	Counter32	The total number of IP datagrams received from all interfaces
4	ipInHdrErrors (4)	Counter32	The number of datagrams received and then discarded because of IP header errors
5	ipInAddrErrors (5)	Counter32	The number of packets discarded because of an invalid destination address in the IP header
6	ipForwDatagrams (6)	Counter32	The number of packets for which relay was deemed necessary
7	ipInUnknownProtos (7)	Counter32	The number of IP data programs discarded because of the following: <ul style="list-style-type: none"> • The protocol cannot be confirmed for incoming IP packets. • The protocol is unsupported.
8	ipInDiscards (8)	Counter32	The total number of IP datagrams discarded during transmission for reasons other than errors
9	ipInDelivers (9)	Counter32	The number of IP datagrams reported to the upper layer
10	ipOutRequests (10)	Counter32	The total number of IP datagrams requested by the upper layer, for IP packet transmission
11	ipOutDiscards (11)	Counter32	The number of IP datagrams discarded for reasons other than errors
12	ipOutNoRoutes (12)	Counter32	The number of IP datagrams discarded because no transmission route was specified
13	ipReasmTimeout (13)	Integer32	The maximum number of seconds to hold fragment packets waiting for reassembly
14	ipReasmReqds (14)	Counter32	The number of incoming IP datagrams for which reassembly is necessary

ID	Object name	Type	Meaning
15	ipReasmOKs (15)	Counter32	The number of incoming IP datagrams for which reassembly was successful
16	ipReasmFails (16)	Counter32	The number of incoming IP datagrams for which reassembly failed
17	ipFragOKs (17)	Counter32	The number of IP datagrams for which fragmentation was successful
18	ipFragFails (18)	Counter32	The number of IP datagrams for which fragmentation failed
19	ipFragCreates (19)	Counter32	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)	IpAddress	IP address
20.1.2	ipAdEntIfIndex (2)	INTEGER	The index value for the interface used by this entry
20.1.3	ipAdEntNetMask (3)	IpAddress	The subnet mask for the IP address of this entry
20.1.4	ipAdEntBcastAddr (4)	INTEGER	The value of the lowest bit of the address during IP broadcast transmission
20.1.5	ipAdEntReasmMaxSize (5)	INTEGER	The maximum IP packet size that can be reassembled 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)	IpAddress	The destination IP address of this route
21.1.2	ipRouteIfIndex (2)	INTEGER	The index value of the interface existing on the first hop of this route
21.1.3	ipRouteMetric1 (3)	INTEGER	The primary routing metric of this route
21.1.4	ipRouteMetric2 (4)	INTEGER	The alternate routing metric of this route [#]

ID	Object name	Type	Meaning
21.1.5	ipRouteMetric3 (5)	INTEGER	The alternate routing metric of this route [#]
21.1.6	ipRouteMetric4 (6)	INTEGER	The alternate routing metric of this route [#]
21.1.7	ipRouteNextHop (7)	IpAddress	The IP address of the next hop of this route
21.1.8	ipRouteType (8)	INTEGER	The route type Each value represents the following: 1: other, 2: invalid, 3: direct, 4: indirect
21.1.9	ipRouteProto (9)	INTEGER	The routing structure that learned the route 1: other, 2: local, 3: netmgmt, 4: icmp, 5: egg, 6: ggp, 7: hello, 8: rip, 9: is-is, 10: es-is, 11: ciscoIgrp, 12: bbnSpfIgp, 13: ospf, 14: gbp
21.1.10	ipRouteAge (10)	INTEGER	The amount of time elapsed since the route was updated [#]
21.1.11	ipRouteMask (11)	IpAddress	The subnet mask value for ipRouteDest
21.1.12	ipRouteMetric5 (12)	INTEGER	The alternate routing metric of this route [#]
21.1.13	ipRouteInfo (13)	OBJECT IDENTIFIER	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)	INTEGER	The ID number of the active interface
22.1.2	ipNetToMediaPhysAddress (2)	PhysAddress	The media-dependent physical address
22.1.3	ipNetToMediaNetAddress (3)	IpAddress	The IP address corresponding to the media-dependent physical address
22.1.4	ipNetToMediaType (4)	INTEGER	The mapping type Each value represents the following: 1: other, 2: invalid, 3: dynamic, 4: static
23	ipRoutingDiscards (23)	Counter	The number of routing entries selected for rejection despite being active, such as those rejected

ID	Object name	Type	Meaning
			because of an insufficient buffer for the routing table
24	ipForward (24)	-	The MIB module for the management of CIDR multipath IP Routes
24.4	ipCidrRouteTable (4)	-	The IP CIDR entity's IP Routing table
24.4.1	ipCidrRouteEntry (1)	-	An ipCidrRoute entry
24.4.1.1	ipCidrRouteDest (1)	IpAddress	The destination IP address
24.4.1.2	ipCidrRouteMask (2)	IpAddress	The IP address and the mask value
24.4.1.3	ipCidrRouteTos (3)	Integer32	The IP TOS Field
24.4.1.4	ipCidrRouteNextHop (4)	IpAddress	On remote routes, the address of the next system en route
24.4.1.5	ipCidrRouteIfIndex (5)	Integer32	The index value of the local interface
24.4.1.6	ipCidrRouteType (6)	INTEGER	The type of route Each value represents the following: 1: other, 2: reject, 3: local, 4: remote
24.4.1.7	ipCidrRouteProto (7)	INTEGER	The routing mechanism via which this route was learned Each value represents the following: 1: other, 2: local, 3: netmgmt, 4: icmp, 5: egp, 6: ggp, 7: hello, 8: rip, 9: isIs, 10: esIs, 11: ciscoIgrp, 12: bbnSpfIgp, 13: ospf, 14: bgp, 15: idpr, 16: ciscoEigrp
24.4.1.9	ipCidrRouteInfo (9)	OBJECT IDENTIFIER	A reference to MIB definitions specific to the particular routing protocol that is responsible for this route
24.4.1.10	ipCidrRouteNextHopAS (10)	Integer32	The Autonomous System Number of the Next Hop
24.4.1.11	ipCidrRouteMetric1 (11)	Integer32	The primary routing metric
24.4.1.12	ipCidrRouteMetric2 (12)	Integer32	An alternate routing metric
24.4.1.13	ipCidrRouteMetric3 (13)	Integer32	An alternate routing metric
24.4.1.14	ipCidrRouteMetric4 (14)	Integer32	An alternate routing metric
24.4.1.15	ipCidrRouteMetric5 (15)	Integer32	An alternate routing metric

ID	Object name	Type	Meaning
24.4.1.16	ipCidrRouteStatus (16)	RowStatus	The row status variable Each value represents the following: 1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
24.6	inetCidrRouteNumber (6)	Gauge32	The number of inetCidrRouteTable entries
24.7	inetCidrRouteTable (7)	-	The inet CIDR table
24.7.1	inetCidrRouteEntry (1)	-	An inetCidrRoute entry
24.7.1.7	inetCidrRouteIfIndex (7)	InterfaceIndex OrZero	The index value that identifies the local interface
24.7.1.8	inetCidrRouteType (8)	INTEGER	The type of route Each value represents the following: 1: other, 2: reject, 3: local, 4: remote, 5: blackhole
24.7.1.9	inetCidrRouteProto (9)	IANAipRouteProtocol	The routing mechanism via which this route was learned Each value represents the following: 1: other, 2: local, 3: netmgmt, 4: icmp, 5: egg, 6: ggp, 7: hello, 8: rip, 9: isIs, 10: esIs, 11: ciscoIgrp, 12: bbnSpfIgp, 13: ospf, 14: bgp, 15: idpr, 16: ciscoEigrp, 17: dvmrp
24.7.1.10	inetCidrRouteAge (10)	Gauge32	The number of seconds since this route was last updated
24.7.1.11	inetCidrRouteNextHopAS (11)	InetAutonomousSystemNumber	The Autonomous System Number of the Next Hop
24.7.1.12	inetCidrRouteMetric1 (12)	Integer32	The primary routing metric
24.7.1.13	inetCidrRouteMetric2 (13)	Integer32	An alternate routing metric
24.7.1.14	inetCidrRouteMetric3 (14)	Integer32	An alternate routing metric
24.7.1.15	inetCidrRouteMetric4 (15)	Integer32	An alternate routing metric
24.7.1.16	inetCidrRouteMetric5 (16)	Integer32	An alternate routing metric
24.7.1.17	inetCidrRouteStatus (17)	RowStatus	The row status variable Each value represents the following:

ID	Object name	Type	Meaning
			1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
25	ipv6IpForwarding (25)	INTEGER	The indication of whether this entity is acting as an IPv6 router on any interface in respect to the forwarding of datagrams received by, but not addressed to, this entity Each value represents the following: 1: forwarding, 2: notForwarding
26	ipv6IpDefaultHopLimit (26)	Unsigned32	The default value inserted into the Hop Limit field of the IPv6 header
31	ipTrafficStats (31)	-	The received traffic statistics
31.1	ipSystemStatsTable (1)	-	The ipSystemStats table
31.1.1	ipSystemStatsEntry (1)	-	An ipSystemStats entry
31.1.1.3	ipSystemStatsInReceives (3)	Counter32	The total number of datagrams received
31.1.1.4	ipSystemStatsHCInReceives (4)	Counter64	The total number of datagrams received
31.1.1.5	ipSystemStatsInOctets (5)	Counter32	The total number of octets received
31.1.1.6	ipSystemStatsHCInOctets (6)	Counter64	The total number of octets received
31.1.1.7	ipSystemStatsInHdrErrors (7)	Counter32	The number of datagrams discarded because of errors in their IP headers
31.1.1.9	ipSystemStatsInAddrErrors (9)	Counter32	The number of datagrams discarded because the IP address in their IP header's destination field was not a valid address
31.1.1.10	ipSystemStatsInUnknownProtos (10)	Counter32	The number of datagrams received successfully but discarded because of an unknown or unsupported protocol
31.1.1.12	ipSystemStatsInForwardDatagrams (12)	Counter32	The number of IP datagrams for which this entity was not their final IP destination and for which this entity attempted to find a route to forward them to that final destination
31.1.1.13	ipSystemStatsHCInForwardDatagrams (13)	Counter64	The number of IP datagrams for which this entity was not their final IP destination and for which this entity attempted to find a route to forward them to that final destination

ID	Object name	Type	Meaning
31.1.1.14	ipSystemStatsReasmReqds (14)	Counter32	The number of IP fragments received that needed to be reassembled
31.1.1.15	ipSystemStatsReasmOKs (15)	Counter32	The number of IP datagrams successfully reassembled
31.1.1.16	ipSystemStatsReasmFails (16)	Counter32	The number of failures detected by the IP re-assembly algorithm
31.1.1.17	ipSystemStatsInDiscards (17)	Counter32	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but were discarded
31.1.1.18	ipSystemStatsInDelivers (18)	Counter32	The total number of IP datagrams successfully delivered
31.1.1.20	ipSystemStatsOutRequests (20)	Counter32	The total number of IP datagrams transmitted
31.1.1.21	ipSystemStatsHCOutRequests (21)	Counter64	The total number of IP datagrams transmitted
31.1.1.22	ipSystemStatsOutNoRoutes (22)	Counter32	The number of IP datagrams discarded
31.1.1.24	ipSystemStatsHCOutForwDatagrams (24)	Counter64	The number of datagrams for which this entity was not their final IP destination and for which it was successful in finding a path to their final destination
31.1.1.25	ipSystemStatsOutDiscards (25)	Counter32	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but were discarded
31.1.1.28	ipSystemStatsOutFragFails (28)	Counter32	The number of IP datagrams that have been discarded because they needed to be fragmented but could not be
31.1.1.29	ipSystemStatsOutFragCreates (29)	Counter32	The number of output datagram fragments that have been generated
31.1.1.46	ipSystemStatsDiscontinuityTime (46)	TimeStamp	The time on the most recent occasion at which any one or more of this entry's counters suffered a discontinuity
31.1.1.47	ipSystemStatsRefreshRate (47)	Unsigned32	The minimum reasonable polling interval
34	ipAddressTable (34)	-	The ipAddress table
34.1	ipAddressEntry (1)	-	An ipAddress entry
34.1.1	ipAddressIfIndex (1)	InterfaceIndex	The index

ID	Object name	Type	Meaning
34.1.4	ipAddressType (4)	INTEGER	The type of address Each value represents the following: 1: unicast, 2: anycast, 3: broadcast
34.1.5	ipAddressPrefix (5)	RowPointer	A pointer to the row in the prefix table
34.1.6	ipAddressOrigin (6)	IpAddressOriginTC	The origin of the address Each value represents the following: 1: other, 2: manual, 4: dhcp, 5: linklayer, 6: random
34.1.7	ipAddressStatus (7)	IpAddressStatusTC	The status of the address Each value represents the following: 1: preferred, 2: deprecated, 3: invalid, 4: inaccessible, 5: unknown, 6: tentative, 7: duplicate, 8: optimistic
34.1.8	ipAddressCreated (8)	TimeStamp	The value of sysUpTime at the time this entry was created
34.1.9	ipAddressLastChanged (9)	TimeStamp	The value of sysUpTime at the time this entry was last updated
34.1.10	ipAddressRowStatus (10)	RowStatus	The status of ipAddress Each value represents the following: 1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
34.1.11	ipAddressStorageType (11)	StorageType	The storage type for ipAddress Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
35	ipNetToPhysicalTable (35)	-	The ipNetToPhysical table
35.1	ipNetToPhysicalEntry (1)	-	An ipNetToPhysical entry
35.1.4	ipNetToPhysicalPhysAddress (4)	PhysAddress	The MAC address
35.1.6	ipNetToPhysicalType (6)	INTEGER	The type of IP address Each value represents the following: 1: other, 2: invalid, 3: dynamic, 4: static, 5: local
35.1.7	ipNetToPhysicalState (7)	INTEGER	The status of the IP address Each value represents the following: 1: reachable, 2: stale, 3: delay, 4: probe, 5: invalid, 6: unknown, 7: incomplete

ID	Object name	Type	Meaning
35.1.8	ipNetToPhysicalRowStatus (8)	RowStatus	The status of the ipNetToPhysical row Each value represents the following: 1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
#: These cannot be obtained.			

Table G-7 icmp (5) group

ID	Object name	Type	Meaning
1	icmpInMsgs (1)	Counter32	The total number of ICMP messages received by this entity
2	icmpInErrors (2)	Counter32	The number of ICMP error messages received (such as those for checksum errors and frame length errors)
3	icmpInDestUnreachs (3)	Counter32	The number of ICMP Destination Unreachable messages received
4	icmpInTimeExcds (4)	Counter32	The number of ICMP Time Exceed messages received
5	icmpInParmProbs (5)	Counter32	The number of ICMP Parameter Problem messages received
6	icmpInSrcQuenchs (6)	Counter32	The number of ICMP Source Quench messages received
7	icmpInRedirects (7)	Counter32	The number of ICMP Network Redirect messages received
8	icmpInEchos (8)	Counter32	The number of ICMP Echo request messages received
9	icmpInEchoReps (9)	Counter32	The number of ICMP Echo response messages received
10	icmpInTimestamps (10)	Counter32	The number of ICMP TimeStamp request messages received
11	icmpInTimestampReps (11)	Counter32	The number of ICMP TimeStamp response messages received
12	icmpInAddrMasks (12)	Counter32	The number of ICMP Address Mask request messages received
13	icmpInAddrMaskReps (13)	Counter32	The number of incoming ICMP Address Mask response messages
14	icmpOutMsgs (14)	Counter32	The total number of ICMP send attempts (including those for which errors occurred)
15	icmpOutErrors (15)	Counter32	The number of ICMP messages that were not sent because of an error

ID	Object name	Type	Meaning
16	icmpOutDestUnreachs (16)	Counter32	The number of ICMP Destination Unreachable messages sent
17	icmpOutTimeExcds (17)	Counter32	The number of ICMP Time Exceeded messages sent
18	icmpOutParmProbs (18)	Counter32	The number of ICMP Parameter Problem messages sent
19	icmpOutSrcQuenchs (19)	Counter32	The number of ICMP Source Quench messages sent
20	icmpOutRedirects (20)	Counter32	The number of ICMP Redirect messages sent
21	icmpOutEchos (21)	Counter32	The number of ICMP Echo request messages sent
22	icmpOutEchoReps (22)	Counter32	The number of ICMP Echo response messages sent
23	icmpOutTimestamps (23)	Counter32	The number of ICMP Timestamp request messages sent
24	icmpOutTimestampReps (24)	Counter32	The number of ICMP Timestamp response messages sent
25	icmpOutAddrMasks (25)	Counter32	The number of ICMP Address Mask request messages sent
26	icmpOutAddrMaskReps (26)	Counter32	The number of ICMP Address Mask response messages sent

Table G-8 tcp (6) group

ID	Object name	Type	Meaning
1	tcpRtoAlgorithm (1)	INTEGER	The algorithm to decide the timeout time used for retransmission Each value represents the following: 1: other, 2: constant, 3: rsre, 4: vanj, 5: rfc2988
2	tcpRtoMin (2)	Integer32	The minimum value for the retransmission timeout time
3	tcpRtoMax (3)	Integer32	The maximum value for the retransmission timeout time
4	tcpMaxConn (4)	Integer32	The total number of supportable TCP connections. -1 is returned when this number is dynamic
5	tcpActiveOpens (5)	Counter32	The number of times that TCP connections were moved from the CLOSE status to the SYN-SENT status

ID	Object name	Type	Meaning
6	tcpPassiveOpens (6)	Counter32	The number of times that TCP connections were moved from the LISTEN status to the SYN-RCVD status
7	tcpAttemptFails (7)	Counter32	The number of times TCP connections were moved from the SYN-SENT or SYN-RCVD statuses to the CLOSE status, and added to the number of times TCP connections were moved from the SYN-RCVD status to the LISTEN status
8	tcpEstabResets (8)	Counter32	The number of times TCP connections were moved from the ESTABLISHED or CLOSE-WAIT statuses to the CLOSE status
9	tcpCurrEstab (9)	Gauge32	The total number of TCP connections in the ESTABLISHED or CLOSE-WAIT status
10	tcpInSegs (10)	Counter32	The total number of incoming segments, including error segments [#]
11	tcpOutSegs (11)	Counter32	The total number of segments sent [#]
12	tcpRetransSegs (12)	Counter32	The total number of resent 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)	INTEGER	The TCP connection status Each value represents the following: 1: closed, 2: listen, 3: synSent, 4: synReceived, 5: established, 6: finWait1, 7: finWait2, 8: closeWait, 9: lastAck, 10: closing, 11: timeWait, 12: deleteTCB
13.1.2	tcpConnLocalAddress (2)	IpAddress	The local IP address of this TCP connection
13.1.3	tcpConnLocalPort (3)	Integer32	The local port number of this TCP connection
13.1.4	tcpConnRemAddress (4)	IpAddress	The remote IP address of this TCP connection
13.1.5	tcpConnRemPort (5)	Integer32	The remote port number of this TCP connection
14	tcpInErrs (14)	Counter32	The total number of error segments received
15	tcpOutRsts (15)	Counter32	The number of segments sent that have the RST flag
19	tcpConnectionTable (19)	-	The TCP connection table
19.1	tcpConnectionEntry (1)	-	A TCP connection entry

ID	Object name	Type	Meaning
19.1.7	tcpConnectionState (7)	INTEGER	The state of the TCP connection for the IP address Each value represents the following: 1: closed, 2: listen, 3: synSent, 4: synReceived, 5: established, 6: finWait1, 7: finWait2, 8: closeWait, 9: lastAck, 10: closing, 11: timeWait, 12: deleteTCB
19.1.8	tcpConnectionProcess (8)	Unsigned32	The process ID for the process connected to the network
#: ifInUcastPkts and ifOutUcastPkts are 32-bit counters, and might be reset if the system is continuously run for a long time.			

Table G-9 udp (7) group

ID	Object name	Type	Meaning
1	udpInDatagrams (1)	Counter32	The number of UDP datagrams reported to the upper layer
2	udpNoPorts (2)	Counter32	The total number of incoming UDP packets for which no parent application exists in the address port
3	udpInErrors (3)	Counter32	The number of UDP datagrams unable to be reported to the application because of reasons other than <code>udpNoPorts</code>
4	udpOutDatagrams (4)	Counter32	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)	IpAddress	The local IP address of this UDP listener
5.1.2	udpLocalPort (2)	Integer32	The local port number of this UDP listener
5.7	udpEndPointTable (7)	-	The UDP EndPoint information table
5.7.1	udpEndPointEntry (1)	-	A UDP EndPoint entry
5.7.1.8	udpEndPointProcess (8)	Unsigned32	The process ID for the process associated with the network endpoint

Table G-10 snmp (11) group

ID	Object name	Type	Meaning
1	snmpInPkts (1)	Counter32	The total number of incoming SNMP messages

ID	Object name	Type	Meaning
2	snmpOutPkts (2)	Counter32	The total number of outgoing SNMP messages
3	snmpInBadVersions (3)	Counter32	The total number of incoming messages of unsupported versions
4	snmpInBadCommunityNames (4)	Counter32	The total number of incoming SNMP messages for unused communities
5	snmpInBadCommunityUses (5)	Counter32	The total number of incoming messages indicating operations not allowed by the community
6	snmpInASNParseErrors (6)	Counter32	The total number of incoming ASN.1 error messages
8	snmpInTooBigs (8)	Counter32	The total number of incoming PDUs for which the error status is <code>tooBig</code>
9	snmpInNoSuchNames (9)	Counter32	The total number of incoming PDUs for which the error status is <code>noSuchName</code>
10	snmpInBadValues (10)	Counter32	The total number of incoming PDUs for which the error status is <code>badValue</code>
11	snmpInReadOnly (11)	Counter32	The total number of incoming PDUs for which the error status is <code>readOnly</code>
12	snmpInGenErrs (12)	Counter32	The total number of incoming PDUs for which the error status is <code>genErr</code>
13	snmpInTotalReqVars (13)	Counter32	The total number of MIB objects for which MIB collection was successful
14	snmpInTotalSetVars (14)	Counter32	The total number of MIB objects for which MIB setup was successful
15	snmpInGetRequests (15)	Counter32	The total number of <code>GetRequestPDUS</code> received
16	snmpInGetNexts (16)	Counter32	The total number of <code>GetNextRequestPDUS</code> received
17	snmpInSetRequests (17)	Counter32	The total number of <code>SetRequestPDUS</code> received
18	snmpInGetResponses (18)	Counter32	The total number of <code>GetResponsePDUS</code> received
19	snmpInTraps (19)	Counter32	The total number of <code>TrapPDUS</code> received
20	snmpOutTooBigs (20)	Counter32	The total number of outgoing PDUs for which the error status is <code>tooBig</code>
21	snmpOutNoSuchNames (21)	Counter32	The total number of outgoing PDUs for which the error status is <code>noSuchName</code>
22	snmpOutBadValues (22)	Counter32	The total number of outgoing PDUs for which the error status is <code>badValue</code>
24	snmpOutGenErrs (24)	Counter32	The total number of outgoing PDUs for which the error status is <code>genErr</code>

ID	Object name	Type	Meaning
25	snmpOutGetRequests (25)	Counter32	The total number of <i>GetRequest</i> PDUS sent
26	snmpOutGetNexts (26)	Counter32	The total number of <i>GetNextRequest</i> PDUS sent
27	snmpOutSetRequests (27)	Counter32	The total number of <i>SetRequest</i> PDUS sent
28	snmpOutGetResponses (28)	Counter32	The total number of <i>GetResponse</i> PDUS sent
29	snmpOutTraps (29)	Counter32	The total number of <i>Trap</i> PDUS sent
30	snmpEnableAuthenTraps (30)	INTEGER	Indicates whether an authentication-failure Trap was issued Each value represents the following: 1: enabled, 2: disabled
31	snmpSilentDrops (31)	Counter32	Indicates the total number, sent to the SNMP entity, of <i>GetRequest</i> -PDUS, <i>GetNextRequest</i> -PDUS, <i>GetBulkRequest</i> -PDUS, <i>SetRequest</i> -PDUS, and <i>InformRequest</i> -PDUS. (If the size of a response containing an alternate <i>Response</i> -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 <i>snmpSilentDrops</i> object will be discarded without being reported.)
32	snmpProxyDrops (32)	Counter32	Indicates the total number, sent to the SNMP entity, of <i>GetRequest</i> -PDUS, <i>GetNextRequest</i> -PDUS, <i>GetBulkRequest</i> -PDUS, <i>SetRequest</i> -PDUS, and <i>InformRequest</i> -PDUS. (If the transmission of messages (which are probably converted) to the proxy target fails without a <i>Response</i> -PDU being returned (aside from timeouts), the <i>snmpProxyDrops</i> object will be discarded without being reported.)

Note: These MIB information items are reset when SNMP agents are restarted. Because SNMP agents are restarted in an HDI system once a day, information for only one day is stored at most.

Table G-11 host (25) group

ID	Object name	Type	Meaning
1	hrSystem (1)	-	Host resource system
1.1	hrSystemUptime (1)	TimeTicks	Time elapsed since system initialization

ID	Object name	Type	Meaning
1.2	hrSystemDate (2)	DateAndTime	Current date and time
1.3	hrSystemInitialLoad Device (3)	Integer32	The index of the hrDeviceEntry for the device from which this host is configured to load its initial operating system configuration
1.4	hrSystemInitialLoadParameters (4)	International DisplayString	Parameter passed to the kernel after Linux startup
1.5	hrSystemNumUsers (5)	Gauge32	Number of user sessions for which this host is storing state information
1.6	hrSystemProcesses (6)	Gauge32	Number of processes currently loaded
1.7	hrSystemMaxProcesses (7)	Gauge32	Returns the fixed value 0
2	hrStorage (2)	-	System storage area for the host resource
2.1	hrStorageTypes (1)	-	Storage area type for the host resource Note: An OID definition is used as the response for hrStorageType, and this object has no real state. The same is true of objects from OID 2.1.1 to 2.1.10.
2.1.1	hrStorageOther (1)	-	The storage area type for the corresponding index during hrStorageType collection is not OID2.1.2 to 2.1.10
2.1.2	hrStorageRam (2)	-	The storage area type for the corresponding index during hrStorageType collection corresponds to RAM
2.1.3	hrStorageVirtualMemory (3)	-	The storage area type for the corresponding index during hrStorageType collection corresponds to virtual memory
2.1.4	hrStorageFixedDisk (4)	-	The storage area type for the corresponding index during hrStorageType collection corresponds to the hard disk
2.1.5	hrStorageRemovableDisk (5)	-	The storage area type for the corresponding index during hrStorageType collection corresponds to the removable disk
2.1.6	hrStorageFloppyDisk (6)	-	The storage area type for the corresponding index during hrStorageType collection corresponds to the floppy disk

ID	Object name	Type	Meaning
2.1.7	hrStorageCompactDisc (7)	-	The storage area type for the corresponding index during <code>hrStorageType</code> collection corresponds to the compact disc
2.1.8	hrStorageRamDisk (8)	-	The storage area type for the corresponding index during <code>hrStorageType</code> collection corresponds to the RAM disk
2.1.9	hrStorageFlashMemory (9)	-	The storage area type for the corresponding index during <code>hrStorageType</code> collection corresponds to the flash memory
2.1.10	hrStorageNetworkDisk (10)	-	The storage area type for the corresponding index during <code>hrStorageType</code> collection corresponds to a file system in the network
2.2	hrMemorySize (2)	KBytes	Amount of main physical memory
2.3	hrStorageTable (3)	-	The (conceptual) table of logical storage area on the host
2.3.1	hrStorageEntry (1)	-	The (conceptual) entry in the logical storage area on the host
2.3.1.1	hrStorageIndex (1)	Integer32	Unique value for each logical storage area for the host
2.3.1.2	hrStorageType (2)	AutonomousType	Storage device type (OID allocated to <code>hrStorageTypes</code> by the index) indicated by this entry
2.3.1.3	hrStorageDescr (3)	DisplayString	Name of the logical storage area
2.3.1.4	hrStorageAllocationUnits (4)	Integer32	Block size allocated from the logical storage area
2.3.1.5	hrStorageSize (5)	Integer32	Block amount
2.3.1.6	hrStorageUsed (6)	Integer32	Block usage
3	hrDevice (3)	-	Device
3.1	hrDeviceTypes (1)	-	Device type Note: An OID definition is used as the response for <code>hrDeviceType</code> , and this object has no real state. The same is true of objects from OID3.1.1 to 3.1.6, or 3.1.10 to 3.1.21.
3.1.1	hrDeviceOther (1)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection is not OID 3.1.2 to 3.1.6, or 3.1.10 to 3.1.21
3.1.2	hrDeviceUnknown (2)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection cannot be recognized

ID	Object name	Type	Meaning
3.1.3	hrDeviceProcessor (3)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the processor (CPU)
3.1.4	hrDeviceNetwork (4)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the network interface
3.1.5	hrDevicePrinter (5)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the printer
3.1.6	hrDeviceDiskStorage (6)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the disk
3.1.10	hrDeviceVideo (10)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the video device
3.1.11	hrDeviceAudio (11)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the audio device
3.1.12	hrDeviceCoprocesor (12)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the coprocessor
3.1.13	hrDeviceKeyboard (13)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the keyboard
3.1.14	hrDeviceModem (14)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the modem
3.1.15	hrDeviceParallelPort (15)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the parallel port
3.1.16	hrDevicePointing (16)	-	The device type for the corresponding index during hrDeviceType collection corresponds to a pointing device such as a mouse
3.1.17	hrDeviceSerialPort (17)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the serial port
3.1.18	hrDeviceTape (18)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the tape device
3.1.19	hrDeviceClock (19)	-	The device type for the corresponding index during hrDeviceType collection corresponds to the clock
3.1.20	hrDeviceVolatileMemory (20)	-	The device type for the corresponding index during hrDeviceType collection corresponds to volatile memory

ID	Object name	Type	Meaning
3.1.21	hrDeviceNonVolatileMemory (21)	-	The device type for the corresponding index during hrDeviceType collection corresponds to non-volatile memory
3.2	hrDeviceTable (2)	-	The (conceptual) table for the devices on the host
3.2.1	hrDeviceEntry (1)	-	The (conceptual) entry for a device on the host
3.2.1.1	hrDeviceIndex (1)	Integer32	Unique value for each device on the host
3.2.1.2	hrDeviceType (2)	AutonomousType	The device type indicated by this entry (OID allocated to hrDeviceTypes by the index)
3.2.1.3	hrDeviceDescr (3)	DisplayString	Device name
3.2.1.4	hrDeviceID (4)	ProductID	Device ID
3.3	hrProcessorTable (3)	-	The (conceptual) table for the processors on the host
3.3.1	hrProcessorEntry (1)	-	The (conceptual) entry for a processor on the host
3.3.1.1	hrProcessorFrwID (1)	ProductID	Processor firmware ID
3.4	hrNetworkTable (4)	-	The (conceptual) table for the network devices on the host
3.4.1	hrNetworkEntry (1)	-	The (conceptual) entry for a network device on the host
3.4.1.1	hrNetworkIfIndex (1)	InterfaceIndexOrZero	Value of ifIndex corresponding to this network device
3.6	hrDiskStorageTable (6)	-	The (conceptual) table for long-term storage devices on the host
3.6.1	hrDiskStorageEntry (1)	-	The (conceptual) entry for a long-term storage device on the host
3.6.1.1	hrDiskStorageAccess (1)	INTEGER	Access attribute Each value represents the following: 1: readWrite, 2: readOnly
3.6.1.2	hrDiskStorageMedia (2)	INTEGER	Media type Each value represents the following: 1: other, 2: unknown, 3: hardDisk, 4: floppyDisk, 5: opticalDiskROM, 6: opticalDiskWORM, 7: opticalDiskRM, 8: ramDisk
3.6.1.3	hrDiskStorageRemovable (3)	TruthValue	Removability Each value represents the following: 1: true, 2: false

ID	Object name	Type	Meaning
3.6.1.4	hrDiskStorageCapacity (4)	KBytes	Total capacity
3.7	hrPartitionTable (7)	-	The (conceptual) table for long-term storage device partitions on the host
3.7.1	hrPartitionEntry (1)	-	The (conceptual) entry for a long-term storage device partition on the host
3.7.1.1	hrPartitionIndex (1)	Integer32	Unique value for each long-term storage device partition on the host ^{#1}
3.7.1.2	hrPartitionLabel (2)	International DisplayString	Device partition name ^{#1}
3.7.1.3	hrPartitionID (3)	OCTET STRING	Device partition number ^{#1}
3.7.1.4	hrPartitionSize (4)	KBytes	Device partition size ^{#1}
3.7.1.5	hrPartitionFSIndex (5)	Integer32	Index for the device partition file system ^{#1}
3.8	hrFSTabl (8)	-	The (conceptual) table for the file system
3.8.1	hrFSEntry (1)	-	The (conceptual) entry in the file system
3.8.1.1	hrFSIndex (1)	Integer32	Unique value for each file system
3.8.1.2	hrFSMountPoint (2)	International DisplayString	Root path name for this file system
3.8.1.3	hrFSRemoteMountPoint (3)	International DisplayString	Name and address of the server on which this file system is mounted ^{#2}
3.8.1.4	hrFSType (4)	AutonomousType	OID allocated to hrFSTypes by the mount type
3.8.1.5	hrFSAccess (5)	INTEGER	Access attribute Each value represents the following: 1: readWrite, 2: readOnly
3.8.1.6	hrFSBootable (6)	TruthValue	Flag indicating whether the file system can be booted Each value represents the following: 1: true, 2: false
3.8.1.7	hrFSStorageIndex (7)	Integer32	Index to hrStorageEntry indicating information about this file system
3.8.1.8	hrFSLastFullBackupDate (8)	DateAndTime	Last date on which this file system was copied to another storage device for backup ^{#3}
3.8.1.9	hrFSLastPartialBackupDate (9)	DateAndTime	Last date on which part of this file system was copied to another storage device for backup ^{#3}
3.9	hrFSTypes (9)	-	Device type

ID	Object name	Type	Meaning
			Note: An OID definition is used as the response for <code>hrFSType</code> , and this object has no real state. The same is true of object <code>OID3.9.1</code> .
3.9.1	<code>hrFSOther (1)</code>	-	Only XFS can be used as the file system for this system. Because there are no objects corresponding to XFS in <code>hrFSTypes (8)</code> , this object is allocated.
5	<code>hrSWRunPerf (5)</code>	-	Performance table for running software
5.1	<code>hrSWRunPerfTable (1)</code>	-	The (conceptual) table for performance metrics of running software
5.1.1	<code>hrSWRunPerfEntry (1)</code>	-	The (conceptual) entry for performance metrics of running software
5.1.1.1	<code>hrSWRunPerfCPU (1)</code>	Integer32	CPU time spent running a process (units: 10ms)
5.1.1.2	<code>hrSWRunPerfMem (2)</code>	KBytes	Total actual system memory allocated to running processes
<p>#1: These cannot be obtained. #2: Null ("") is always obtained. #3: The value of 0-1-1,0:0:0.0 is always obtained.</p>			

Table G-12 ifMIB (31) group

ID	Object name	Type	Meaning
1	<code>ifMIBObjects (1)</code>	-	The additional object for interface entries
1.1	<code>ifXTable (1)</code>	-	A list of interface entries. The number of entries is given by the value of <code>ifNumber</code> . This table contains additional objects for the interface table
1.1.1	<code>ifXEntry (1)</code>	-	An entry containing additional management information applicable to a particular interface
1.1.1.1	<code>ifName (1)</code>	DisplayString	The textual name of the interface
1.1.1.2	<code>ifInMulticastPkts (2)</code>	Counter32	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer
1.1.1.3	<code>ifInBroadcastPkts (3)</code>	Counter32	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer
1.1.1.4	<code>ifOutMulticastPkts (4)</code>	Counter32	The total number of packets that higher-level protocols requested be transmitted, and which were

ID	Object name	Type	Meaning
			addressed to a multicast address at this sub-layer
1.1.1.5	ifOutBroadcastPkts (5)	Counter32	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer
1.1.1.6	ifHCInOctets (6)	Counter64	The total number of octets received on the interface. This object is a 64-bit version of ifInOctets
1.1.1.7	ifHCInUcastPkts (7)	Counter64	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. This object is a 64-bit version of ifInUcastPkts.
1.1.1.8	ifHCInMulticastPkts (8)	Counter64	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. This object is a 64-bit version of ifInMulticastPkts.
1.1.1.9	ifHCInBroadcastPkts (9)	Counter64	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. This object is a 64-bit version of ifInBroadcastPkts.
1.1.1.10	ifHCOctets (10)	Counter64	The total number of octets transmitted out of the interface. This object is a 64-bit version of ifOutOctets.
1.1.1.11	ifHCOUcastPkts (11)	Counter64	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer. This object is a 64-bit version of ifOutUcastPkts.
1.1.1.12	ifHCOMulticastPkts (12)	Counter64	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer. This object is a 64-bit version of ifOutMulticastPkts.
1.1.1.13	ifHCOBroadcastPkts (13)	Counter64	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer. This object is a 64-bit version of ifOutBroadcastPkts.
1.1.1.14	ifLinkUpDownTrapEnable (14)	INTEGER	Indicates whether linkUp/linkDown traps should be generated for this interface.

ID	Object name	Type	Meaning
			Each value represents the following: 1: enabled, 2: disabled
1.1.1.15	ifHighSpeed (15)	Gauge32	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If this object reports a value of 'n' then the speed of the interface is somewhere in the range of 'n-500,000' to 'n+499,999'.
1.1.1.16	ifPromiscuousMode (16)	TruthValue	This object has a value of false(2) if this interface only accepts packets/frames that are addressed to this station. This object has a value of true(1) when the station accepts all packets/frames transmitted on the media. Each value represents the following: 1: true, 2: false
1.1.1.17	ifConnectorPresent (17)	TruthValue	This object has the value 'true(1)' if the interface sublayer has a physical connector and the value 'false(2)' otherwise. Each value represents the following: 1: true, 2: false
1.1.1.18	ifAlias (18)	DisplayString	This object is an 'alias' name for the interface as specified by a network manager.
1.1.1.19	ifCounterDiscontinuity Time (19)	TimeStamp	The value of sysUpTime on the most recent occasion at which any one or more of this interface's counters suffered a discontinuity

Table G-13 ipv6MIB (55) group

ID	Object name	Type	Meaning
1	ipv6MIBObjects (1)	-	IPv6 MIB objects
1.1	ipv6Forwarding (1)	INTEGER	The indication of whether this entity is acting as an IPv6 router in respect to the forwarding of datagrams received by, but not addressed to, this entity Each value represents the following: 1: forwarding, 2: notForwarding
1.2	ipv6DefaultHopLimit (2)	INTEGER	The default value inserted into the Hop Limit field of the IPv6 header
1.3	ipv6Interfaces (3)	Unsigned32	The number of IPv6 interfaces

ID	Object name	Type	Meaning
1.5	ipv6IfTable (5)	-	The IPv6 Interfaces table contains information on the entity's internetwork-layer interfaces
1.5.1	ipv6IfEntry (1)	-	An interface entry containing objects about a particular IPv6 interface
1.5.1.2	ipv6IfDescr (2)	DisplayString	A textual string containing information about the interface
1.5.1.3	ipv6IfLowerLayer (3)	VariablePointer	The object ID ($\{0, 0\}$) that identifies the protocol layer over which this network interface operates
1.5.1.4	ipv6IfEffectiveMtu (4)	Unsigned32	The size of the largest IPv6 packet which can be sent/received on the interface
1.5.1.8	ipv6IfPhysicalAddresses (8)	PhysAddress	The interface's physical address
1.5.1.9	ipv6IfAdminStatus (9)	INTEGER	The desired state of the interface Each value represents the following: 1: up, 2: down
1.5.1.10	ipv6IfOperStatus (10)	INTEGER	The current operational state of the interface Each value represents the following: 1: up, 2: down, 3: noIfIdentifier, 4: unknown, 5: notPresent

Table G-14 ucdavis (2021) group

ID	Object name	Type	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)	Integer32	An index number allocated to this process information.
2.1.2	prNames (2)	DisplayString	The process names specified in that of the <code>proc</code> line.
2.1.3	prMin (3)	Integer32	The minimum value set for the <code>proc</code> line.
2.1.4	prMax (4)	Integer32	The maximum value set for the <code>proc</code> line.
2.1.5	prCount (5)	Integer32	The number of processes specified in <code>prNames</code> that are currently running.
2.1.100	prErrorFlag (100)	UCDErrorFlag	In the case of an error, this is 1. Otherwise, it is 0.

ID	Object name	Type	Meaning
			Each value represents the following: 0: no error, 1: error
2.1.101	prErrMsg (101)	DisplayString	This contains an error message, when prErrorFlag is 1.
2.1.102	prErrFix (102)	UCDErrorFix	When the administrator sets this object to 1, the command already specified on the procfix line of the snmpd.conf file is run. Each value represents the following: 0: noError, 1: runFix
2.1.103	prErrFixCmd (103)	DisplayString	The name of the command run when prErrFix is set to 1.
4	memory (4)	-	Contains the memory status.
4.1	memIndex (1)	Integer32	A dummy index number (always 0).
4.2	memErrorName (2)	DisplayString	A dummy name (always swap).
4.3	memTotalSwap (3)	Integer32	The amount of space reserved for the swap file.
4.4	memAvailSwap (4)	Integer32	The amount of unused swap file space.
4.5	memTotalReal (5)	Integer32	The amount of real memory installed.
4.6	memAvailReal (6)	Integer32	The amount of real memory available. Note: Nodes 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.#1
4.8	memAvailSwapTXT (8)	-	The amount of swap file space for text that is unused.#1
4.9	memTotalRealTXT (9)	-	The total real memory used for text.#1
4.10	memAvailRealTXT (10)	-	The amount of available memory used for text.#1
4.11	memTotalFree (11)	Integer32	The total available memory.
4.12	memMinimumSwap (12)	Integer32	The available size of the swap file during an error.
4.13	memShared (13)	Integer32	The total amount of shared memory.
4.14	memBuffer (14)	Integer32	The total amount of buffer memory.
4.15	memCached (15)	Integer32	The total amount of cache memory.

ID	Object name	Type	Meaning
4.100	memSwapError (100)	UCDErrorFlag	The swap error flag. Each value represents the following: 0: noError, 1: runFix
4.101	memSwapErrorMsg (101)	DisplayString	The error message when <code>memSwapError</code> is 1.
8	extTable (8)	-	Runs 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)	Integer32	An index number.
8.1.2	extNames (2)	DisplayString	The name specified for the set name in the <code>exec</code> line.
8.1.3	extCommand (3)	DisplayString	The full path name and arguments of the execution file specified in the <code>exec</code> line.
8.1.100	extResult (100)	Integer32	The error code returned when the execution file specified in <code>extCommand</code> is run.
8.1.101	extOutput (101)	DisplayString	The execution results of the execution file specified in <code>extCommand</code> .
8.1.102	extErrFix (102)	UCDErrorFix	When the administrator sets this object to 1, the command already specified in the <code>execfix</code> line of the <code>snmpd.conf</code> file is run. Each value represents the following: 0: noError, 1: runFix
8.1.103	extErrFixCmd (103)	DisplayString	The name of the command run when <code>extErrFix</code> is set to 1.
9	dskTable (9)	-	Contains the disk status. ^{#2}
9.1	dskEntry (1)	-	A hierarchical tree to hold disk information. ^{#2}
9.1.1	dskIndex (1)	Integer32	An index number. ^{#2}
9.1.2	dskPath (2)	DisplayString	The path name of the inspection target. ^{#2} The value specified for the path name to be inspected, in the <code>disk</code> line.
9.1.3	dskDevice (3)	DisplayString	The device name contained in <code>dskPath</code> . ^{#2}
9.1.4	dskMinimum (4)	Integer32	The minimum amount for error handling specified in the <code>disk</code> line (-1 when a percentage is specified).

ID	Object name	Type	Meaning
9.1.5	dskMinPercent (5)	Integer32	The minimum percentage amount for error handling specified in the <code>disk</code> line (-1 when units are specified in KB).
9.1.6	dskTotal (6)	Integer32	The maximum amount that can be stored on the device specified in <code>dskDevice.#2#3</code>
9.1.7	dskAvail (7)	Integer32	The amount of space currently available on the device specified in <code>dskDevice.#2#3</code>
9.1.8	dskUsed (8)	Integer32	The current usage rate of the device specified in <code>dskDevice.#2#3</code>
9.1.9	dskPercent (9)	Integer32	The current usage rate of the device specified in <code>dskDevice</code> , expressed as a percentage.#2#3
9.1.10	dskPercentNode (10)	Integer32	The current inode usage rate of the device specified in <code>dskDevice</code> , expressed as a percentage.#2#3
9.1.11	dskTotalLow (11)	Unsigned32	Total size of the disk/partition (KB). Together with <code>dskTotalHigh</code> composes 64-bit number.#4 (That is, the two <code>dskTotalHigh</code> and <code>dskTotalLow</code> values require a total of 64 bits.)
9.1.12	dskTotalHigh (12)	Unsigned32	Total size of the disk/partition (KB). Together with <code>dskTotalLow</code> composes 64-bit number.#4 (That is, the two <code>dskTotalHigh</code> and <code>dskTotalLow</code> values require a total of 64 bits.)
9.1.13	dskAvailLow (13)	Unsigned32	Unused capacity on the disk (KB). Together with <code>dskAvailHigh</code> composes 64-bit number.#4 (That is, the two <code>dskAvailHigh</code> and <code>dskAvailLow</code> values require a total of 64 bits.)
9.1.14	dskAvailHigh (14)	Unsigned32	Unused capacity on the disk (KB). Together with <code>dskAvailLow</code> composes 64-bit number.#4 (That is, the two <code>dskAvailHigh</code> and <code>dskAvailLow</code> values require a total of 64 bits.)
9.1.15	dskUsedLow (15)	Unsigned32	Used capacity on the disk (KB). Together with <code>dskUsedHigh</code> composes 64-bit number.#4 (That is, the two <code>dskUsedHigh</code> and <code>dskUsedLow</code> values require a total of 64 bits.)
9.1.16	dskUsedHigh (16)	Unsigned32	Used capacity on the disk (KB). Together with <code>dskUsedLow</code> composes 64-bit number.#4 (That is, the two

ID	Object name	Type	Meaning
			dskUsedHigh and dskUsedLow values require a total of 64 bits.)
9.1.100	dskErrorFlag (100)	UCDErrorFix	An error flag that indicates whether or not the available space is less than that specified on the <code>disk</code> line.#2#3 1: less than or equal to the specified space 0: greater than or equal to the specified space Each value represents the following: 0: noError, 1: runFix
9.1.101	dskErrorMsg (101)	DisplayString	The error message when <code>dskErrorFlag</code> is 1.#2#3
10	laTable (10)	-	Contains load average information for the system.
10.1	laEntry (1)	-	A hierarchical directory that contains load average information.
10.1.1	laIndex (1)	Integer32	An index number. This value is 1 for 1 minute average value information, 2 for 5 minute average value information, and 3 for 15 minute average value information.
10.1.2	laNames (2)	DisplayString	The monitoring name. This value is <code>Load-1</code> for 1 minute average value information, <code>Load-5</code> for 5 minute average value information, and <code>Load-15</code> for 15 minute average value information.
10.1.3	laLoad (3)	DisplayString	The load average value, expressed as a string. <code>laLoad-1</code> stores the accumulated value for the last minute. <code>laLoad-2</code> stores the accumulated value for the last 5 minutes. <code>laLoad-3</code> stores the accumulated value for the last 15 minutes.
10.1.4	laConfig (4)	DisplayString	The average value set in the <code>load</code> line for error handling.
10.1.5	laLoadInt (5)	Integer32	<code>laLoad</code> , expressed as a percentage.
10.1.6	laLoadFloat (6)	Float	<code>laLoad</code> , expressed as a floating-point decimal.
10.1.100	laErrorFlag (100)	UCDErrorFix	An error flag. This value is 1 when the set average value of the load average is exceeded, and 0 otherwise.

ID	Object name	Type	Meaning
			Each value represents the following: 0: noError, 1: runFix
10.1.101	laErrorMessage (101)	DisplayString	The error message when laLoadErrorFlag is 1.
11	systemStats (11)	-	Contains the system status.
11.1	ssIndex (1)	Integer32	A dummy index number (always 1).
11.2	ssErrorName (2)	DisplayString	The <code>systemStats</code> name (always <code>systemStats</code>).
11.3	ssSwapIn (3)	Integer32	The time required for swap-in.
11.4	ssSwapOut (4)	Integer32	The time required for swap-out.
11.5	ssIOSent (5)	Integer32	The time required for transmission to the block device.
11.6	ssIOReceive (6)	Integer32	The time required for reception from the block device.
11.7	ssSysInterrupts (7)	Integer32	The number of interruptions for 1 second, including clock interruptions.
11.8	ssSysContext (8)	Integer32	The number of context switches switched for 1 second.
11.9	ssCpuUser (9)	Integer32	The ratio of CPU capacity used by the user.
11.10	ssCpuSystem (10)	Integer32	The ratio of CPU capacity used by the system.
11.11	ssCpuIdle (11)	Integer32	The ratio of CPU capacity that is idle.
11.50	ssCpuRawUser (50)	Counter32	The time for which the user is using the CPU.
11.51	ssCpuRawNice (51)	Counter32	The value of the <code>nice</code> process.
11.52	ssCpuRawSystem (52)	Counter32	The time for which the system is using the CPU.
11.53	ssCpuRawIdle (53)	Counter32	The time for which the CPU is idle.
11.54	ssCpuRawWait (54)	Counter32	CPU time spent waiting for I/O
11.55	ssCpuRawKernel (55)	Counter32	Kernel CPU time
11.56	ssCpuRawInterrupt (56)	Counter32	Interrupt level CPU time
11.57	ssIORawSent (57)	Counter32	Number of requests sent to block devices
11.58	ssIORawReceived (58)	Counter32	Number of requests received from block devices
11.59	ssRawInterrupts (59)	Counter32	Number of interrupts

ID	Object name	Type	Meaning
11.60	ssRawContexts (60)	Counter32	Number of context switches
11.61	ssCpuRawSoftIRQ (61)	Counter32	Time for performing soft interrupt processing
11.62	ssRawSwapIn (62)	Counter32	Number of blocks swapped in
11.63	ssRawSwapOut (63)	Counter32	Number of blocks swapped out
13	ucdExperimental (13)	-	An experimental MIB
13.14	ucdDlmodMIB (14)	-	The dynamic load module MIB. The function for loading a predefined MIB definition file during snmpd operation.
13.14.1	dlmodNextIndex (1)	Integer32	The index of the next-loaded MIB.
13.15	ucdDiskIOMIB (15)	-	This MIB module defines objects for disk I/O statistics.
13.15.1	diskIOTable (1)	-	Table of IO devices and how much data they have read/written
13.15.1.1	diskIOEntry (1)	-	An entry containing a device and its statistics
13.15.1.1.1	diskIOIndex (1)	Integer32	Reference index for each observed device
13.15.1.1.2	diskIODevice (2)	DisplayString	The name of the device we are counting/checking (Example: ram0, sda)
13.15.1.1.3	diskIONRead (3)	Counter32	The number of bytes read from this device since boot (32-bit counter)
13.15.1.1.4	diskIONWritten (4)	Counter32	The number of bytes written to this device since boot (32-bit counter)
13.15.1.1.5	diskIOReads (5)	Counter32	The number of read accesses from this device since boot
13.15.1.1.6	diskIOWrites (6)	Counter32	The number of write accesses to this device since boot
13.15.1.1.12	diskIONReadX (12)	Counter64	The number of bytes read from this device since boot (64-bit version)
13.15.1.1.13	diskIONWrittenX (13)	Counter64	The number of bytes written to this device since boot (64-bit version)
16	logMatch (16)	-	Log search
16.1	logMatchMaxEntries (1)	Integer32	Maximum number of supportable logMatch entries
100	version (100)	-	Contains the snmpd version information.
100.1	versionIndex (1)	Integer32	The index to MIB.

ID	Object name	Type	Meaning
100.2	versionTag (2)	DisplayString	The CVS tag keyword.
100.3	versionDate (3)	DisplayString	The date from the RCS keyword.
100.4	versionCDate (4)	DisplayString	The date from <code>ctime()</code> .
100.5	versionIdent (5)	DisplayString	The ID from the RCS keyword.
100.6	versionConfigureOptions (6)	DisplayString	If this agent is configured, options are moved to the config script.
100.10	versionClearCache (10)	Integer32	When this is set to 1, the execution cache is cleared.
100.11	versionUpdateConfig (11)	Integer32	When this is set to 1, the config file is read.
100.12	versionRestartAgent (12)	Integer32	When this is set to 1, the agent is restarted.
100.13	versionSavePersistentData (13)	Integer32	When this is set to 1, persistent data for the agent is saved immediately.
100.20	versionDoDebugging (20)	Integer32	When this is set to 1, the device statement is released with a 0.
101	snmperrs (101)	-	Contains <code>snmpd</code> error information.
101.1	snmperrIndex (1)	Integer32	A fake index for <code>snmperrs</code> .
101.2	snmperrNames (2)	DisplayString	<code>Snmp</code>
101.100	snmperrErrorFlag (100)	UCDErrorFlag	An error flag indicating a problem with the agent. Each value represents the following: 0: noError, 1: error
101.101	snmperrErrorMessage (101)	DisplayString	A message explaining the problem.
<p>#1: These cannot be obtained.</p> <p>#2: On a node, the SNMP agent is restarted at 0:01 daily. If the agent is restarted during failover, the information about the resources that are failed over to the other node is not output. In this case, the information can be output by failing back and restarting the SNMP agent. The SNMP agent can be restarted by updating the <code>snmp.conf</code> file from the GUI. For details about how to edit the <code>snmp.conf</code> file, see Edit System File page on page C-209.</p> <p>#3: If the resources are failed over to the other node, root directory information of the OS disk is shown. Information about the specified file system is shown by failing back.</p> <p>#4: The following is an example of how to calculate the capacity when <code>dskTotalLow</code> is 3431333888 and <code>dskTotalHigh</code> is 4872:</p> <ol style="list-style-type: none"> Convert the obtained MIB values to hexadecimal numbers. 3431333888 = 0xCC860000 4872 = 0x1308 Concatenate the hexadecimal <code>dskTotalHigh</code> in front of <code>dskTotalLow</code>. 0x1308, 0xCC860000 = 0x1308CC860000 Convert the concatenated number to a decimal number. 			

ID	Object name	Type	Meaning
0x1308CC860000 = 20928512000000 (KB)			

Table G-15 netSnmp (8072) group

ID	Object name	Type	Meaning
1	netSnmpObjects (1)	-	Objects for <code>netSnmp</code>
1.2	nsMibRegistry (2)	-	Monitor for registered MIB modules
1.2.1	nsModuleTable (1)	-	Table showing all OIDs registered by the MIB module
1.2.1.1	nsModuleEntry (1)	-	MIB module entry
1.2.1.1.1	nsmContextName (1)	-	Context name for the registered MIB module [#]
1.2.1.1.2	nsmRegistrationPoint (2)	-	OID for the registered MIB module [#]
1.2.1.1.3	nsmRegistrationPriority (3)	-	Priority for the registered MIB module [#]
1.2.1.1.4	nsModuleName (4)	DisplayString	Name of the registered MIB module
1.2.1.1.5	nsModuleModes (5)	BITS	Access attribute for the registered MIB module Each value represents the following: 0: getAndGetNext, 1: set, 2: getBulk
1.2.1.1.6	nsModuleTimeout (6)	Integer32	Timeout value for the registered MIB module
1.5	nsCache (5)	-	Objects related to saving SNMP agent data
1.5.1	nsCacheDefaultTimeout (1)	INTEGER	Initial save timeout value
1.5.2	nsCacheEnabled (2)	TruthValue	Whether save is enabled Each value represents the following: 1: true, 2: false
1.5.3	nsCacheTable (3)	-	Table for each MIB module and saved data
1.5.3.1	nsCacheEntry (1)	-	Conceptual entry in the save table
1.5.3.1.1	nsCachedOID (1)	-	OID for saved data [#]
1.5.3.1.2	nsCacheTimeout (2)	INTEGER	Entry-specific save timeout value
1.5.3.1.3	nsCacheStatus (3)	NetsnmpCacheStatus	Current status of entry-specific save Each value represents the following: 1: enabled, 2: disabled, 3: empty, 4: active, 5: empty

ID	Object name	Type	Meaning
1.7	nsConfiguration (7)	-	Group for debugging and logging settings
1.7.1	nsConfigDebug (1)	-	Debugging settings (this is active if the debugging option is specified when <code>snmpd</code> is started)
1.7.1.1	nsDebugEnabled (1)	TruthValue	Setting used to output debugging information Each value represents the following: 1: true, 2: false
1.7.1.2	nsDebugOutputAll (2)	TruthValue	Setting used to output all debugging information Each value represents the following: 1: true, 2: false
1.7.1.3	nsDebugDumpPdu (3)	TruthValue	Setting used to output packet dump information Each value represents the following: 1: true, 2: false
1.7.2	nsConfigLogging (2)	-	Logging settings (this is active if the logging option is specified when <code>snmpd</code> is started)
1.7.2.1	nsLoggingTable (1)	-	Logging output table
1.7.2.1.1	nsLoggingEntry (1)	-	Logging output entry
1.7.2.1.1.1	nsLogLevel (1)	INTEGER	(Minimum) priority level that should be applied for this logging entry [#] Each value represents the following: 0: emergency, 1: alert, 2: critical, 3: error, 4: warning, 5: notice, 6: info, 7: debug
1.7.2.1.1.2	nsLogToken (2)	DisplayString	Entry for where this entry is logged [#]
1.7.2.1.1.3	nsLogType (3)	INTEGER	Logging type for this entry Each value represents the following: 1: stdout, 2: stderr, 3: file, 4: syslog, 5: callback
1.7.2.1.1.4	nsLogMaxLevel (4)	INTEGER	Maximum priority level that should be applied for this logging entry Each value represents the following: 0: emergency, 1: alert, 2: critical, 3: error, 4: warning, 5: notice, 6: info, 7: debug
1.7.2.1.1.5	nsLogStatus (5)	RowStatus	Logging status Each value represents the following:

ID	Object name	Type	Meaning
			1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
#: These cannot be obtained.			

Table G-16 snmpFrameworkMIB (10) group

ID	Object name	Type	Meaning
2	snmpFrameworkMIBObjects (2)	-	N/A
2.1	snmpEngine (1)	-	N/A
2.1.1	snmpEngineID (1)	SnmpEngineID	A unique identifier for SNMP engine operation.
2.1.2	snmpEngineBoots (2)	INTEGER	The number of times the SNMP engine was (re)initialized since snmpEngineID was last set.
2.1.3	snmpEngineTime (3)	INTEGER	The number of seconds that have elapsed since the value of snmpEngineBoots was last set.
2.1.4	snmpEngineMaxMessageSize (4)	INTEGER	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).
Note: N/A = Not applicable.			

Table G-17 snmpMPDMIB (11) group

ID	Object name	Type	Meaning
2	snmpMPDMIBObjects (2)	-	N/A
2.1	snmpMPDStats (1)	-	N/A
2.1.1	snmpUnknownSecurityModels (1)	Counter32	The total number of packets received by the SNMP engine, not including those not supported by the SNMP engine.
2.1.2	snmpInvalidMsgs (2)	Counter32	The total number of packets received by the SNMP engine, not including invalid or inconsistent components in SNMP messages.
2.1.3	snmpUnknownPDUHandlers (3)	Counter32	The total number of packets received by the SNMP engine, not including those for which PDUs

ID	Object name	Type	Meaning
			containing pduType packets could not be passed.
<p>Note: N/A = Not applicable.</p> <p>These MIB information items are reset when SNMP agents are restarted. Because SNMP agents are restarted in an HDI system once a day, information for only one day is stored at most.</p>			

Table G-18 snmpTargetMIB (12) group

ID	Object name	Type	Meaning
1	snmpTargetObjects (1)	-	N/A
1.2	snmpTargetAddrTable (2)	-	The transport table is used to create SNMP messages.
1.2.1	snmpTargetAddrEntry (1)	-	The transport address is used to create SNMP operations.
1.2.1.1	snmpTargetAddrName (1)	SnmpAdminString	A unique identifier that is locally optional but related to this snmpTargetAddrEntry.#
1.2.1.2	snmpTargetAddrTDomain (2)	TDomain	Indicates the address of the transport type included in the snmpTargetAddrTAddress object.
1.2.1.3	snmpTargetAddrTAddress (3)	TAddress	This address format, which contains the transport address, is dependent on the value of the snmpTargetAddrTDomain object.
1.2.1.4	snmpTargetAddrTimeout (4)	TimeInterval	This reflects the expected maximum round-trip time for contacting the transport address defined in this row.
1.2.1.5	snmpTargetAddrRetryCount (5)	Integer32	Specifies the default number of retries when a message, for which a response was created, cannot be received.
1.2.1.6	snmpTargetAddrTagList (6)	SnmpTagList	Contains the tag list used to choose the target address for a particular operation.
1.2.1.7	snmpTargetAddrParams (7)	SnmpAdminString	Identifies an entry from within the snmpTargetParamsTable.
1.2.1.8	snmpTargetAddrStorageType (8)	StorageType	The memory type. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.2.1.9	snmpTargetAddrRowStatus (9)	RowStatus	The status. Each value represents the following:

ID	Object name	Type	Meaning
			1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
1.3	snmpTargetParamsTable (3)	-	A table of SNMP target information used to create SNMP messages.
1.3.1	snmpTargetParamsEntry (1)	-	One piece of information for one SNMP set.
1.3.1.1	snmpTargetParamsName (1)	SnmpAdminString	A unique identifier that is locally optional but related to this <code>snmpTargetParamsEntry</code> .#
1.3.1.2	snmpTargetParamsMPModel (2)	SnmpMessageProcessingModel	When this entry is used to create an SNMP message, a certain message processing module has been used.
1.3.1.3	snmpTargetParamsSecurityModel (3)	SnmpSecurityModel	The security models for the SNMP messages. Each value represents the following: 0: SNMP_SEC_MODEL_ANY, 1: SNMP_SEC_MODEL_SNMPv1, 2: SNMP_SEC_MODEL_SNMPv2c, 3: SNMP_SEC_MODEL_USM, 256: SNMP_SEC_MODEL_SNMPv2p
1.3.1.4	snmpTargetParamsSecurityName (4)	SnmpAdminString	The <code>securityName</code> specifying the principal in an SNMP message occurs using this entry.
1.3.1.5	snmpTargetParamsSecurityLevel (5)	SnmpSecurityLevel	The security level used when this entry is used to create an SNMP message. Each value represents the following: 1: noAuthNoPriv, 2: authNoPriv, 3: authPriv
1.3.1.6	snmpTargetParamsStorageType (6)	StorageType	The <code>nonVolatile</code> , <code>permanent</code> , or <code>readOnly</code> memory type. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.3.1.7	snmpTargetParamsRowStatus (7)	RowStatus	When the value of this object is <code>active (1)</code> , the following objects are not corrected: <ul style="list-style-type: none"> • <code>snmpTargetParamsMPModel</code> • <code>snmpTargetParamsSecurityModel</code> • <code>snmpTargetParamsSecurityName</code> • <code>snmpTargetParamsSecurityLevel</code> Each value represents the following:

ID	Object name	Type	Meaning
			1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
Note: N/A = Not applicable. #: These cannot be obtained.			

Table G-19 snmpNotificationMIB (13) group

ID	Object name	Type	Meaning
1	snmpNotifyObjects (1)	-	N/A
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)	SnmpAdminString	Indicates the notification name.#
1.1.1.2	snmpNotifyTag (2)	SnmpTagValue	Used to select entries in the snmpTargetAddrTable.
1.1.1.3	snmpNotifyType (3)	INTEGER	This is 1 in case of a trap, or 2 in case of a notification. Each value represents the following: 1: trap, 2: inform
1.1.1.4	snmpNotifyStorageType (4)	StorageType	nonVolatile, permanent, or readOnly. Each value represents the following: 1: other, 2: volatile, 3: nonVolatile, 4: permanent, 5: readOnly
1.1.1.5	snmpNotifyRowStatus (5)	RowStatus	The status of the row of this overview. Each value represents the following: 1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
Note: N/A = Not applicable. #: These cannot be obtained.			

Table G-20 snmpUsmMIB (15) group

ID	Object name	Type	Meaning
1	usmMIBObjects (1)	-	N/A
1.1	usmStats (1)	-	N/A
1.1.1	usmStatsUnsupportedSecurityLevels (1)	Counter32	The total number of packets received by the SNMP engine, not including cases in which a securityLevel that is not used or

ID	Object name	Type	Meaning
			not in the SNMP engine was requested.
1.1.2	usmStatsNotInTimeWindows (2)	Counter32	The total number of packets received by the SNMP engine, not including those appearing outside of the SNMP engine.
1.1.3	usmStatsUnknownUserNames (3)	Counter32	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)	Counter32	The total number of packets received by the SNMP engine, not including <code>snmpEngineIDs</code> of which the SNMP engine was not notified.
1.1.5	usmStatsWrongDigests (5)	Counter32	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)	Counter32	The total number of packets received by the SNMP engine, not including those that could not be decrypted.
1.2	usmUser (2)	-	N/A
1.2.1	usmUserSpinLock (1)	TestAndIncr	Locks are used so that the various cooperating command generator applications can be reconciled.
<p>Note: N/A = Not applicable.</p> <p>These MIB information items are reset when SNMP agents are restarted. Because SNMP agents are restarted in an HDI system once a day, information for only 1 day is stored at most.</p>			

Table G-21 snmpVacmMIB (16) group

ID	Object name	Type	Meaning
1	vacmMIBObjects (1)	-	N/A
1.2	vacmSecurityToGroupTable (2)	-	A table used so that the access management policy for the combination of <code>securityModel</code> and <code>securityName</code> can be defined for the primary group. This is mapped to <code>groupName</code> .
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.#

ID	Object name	Type	Meaning
1.2.1.3	vacmGroupName (3)	SnmpAdminString	Group name.
1.2.1.4	vacmSecurityToGroupStorageType (4)	StorageType	The memory type. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.2.1.5	vacmSecurityToGroupStatus (5)	RowStatus	The status. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
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 <code>contextName</code> , so that access permissions can be obtained.#
1.4.1.2	vacmAccessSecurityModel (2)	-	This <code>securityModel</code> must be used to obtain access permissions.#
1.4.1.3	vacmAccessSecurityLevel (3)	-	The minimum security level.#
1.4.1.4	vacmAccessContextMatch (4)	INTEGER	The method by which the context for <code>exact</code> or <code>prefix</code> requests matches <code>vacmAccessContextPrefix</code> . Each value represents the following: 1: exact, 2: prefix
1.4.1.5	vacmAccessReadViewName (5)	SnmpAdminString	Used to define the view subtree for <code>GetRequests</code> .
1.4.1.6	vacmAccessWriteViewName (6)	SnmpAdminString	Used to define the view subtree for <code>SetRequests</code> .
1.4.1.7	vacmAccessNotifyViewName (7)	SnmpAdminString	Used to define the view subtree so that objects within trap messages and <code>InformRequests</code> can be loaded as <code>VarBinds</code> .
1.4.1.8	vacmAccessStorageType (8)	StorageType	The memory type. Each value represents the following:

ID	Object name	Type	Meaning
			1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.4.1.9	vacmAccessStatus (9)	RowStatus	The status. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.5	vacmMIBViews (5)	-	N/A
1.5.1	vacmViewSpinLock (1)	TestAndIncr	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)	SnmpAdminString	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)	OCTET STRING	The mask that defines the family of the view subtree for vacmViewTreeFamilySubtree.
1.5.2.1.4	vacmViewTreeFamilyType (4)	INTEGER	Indicates whether or not the subtree under the OID defined in vacmViewTreeFamilySubtree can be accessed. Each value represents the following: 1: include, 2: exclude
1.5.2.1.5	vacmViewTreeFamilyStorageType (5)	StorageType	The memory type. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.5.2.1.6	vacmViewTreeFamilyStatus (6)	RowStatus	The status. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
Note: N/A = Not applicable.			

ID	Object name	Type	Meaning
#: These cannot be obtained.			

Table G-22 stdExMibQuotaTable (2) group

ID	Object name	Type	Meaning
1	quotaEntry (1)	-	Quota management information for each file system
1.1	quotaFSIndex (1)	INTEGER	The index number that corresponds to the file system
1.2	quotaFSMntPoint (2)	DisplayString	The mount point for the file system
1.3	quotaFSBlockMaxGrace (3)	INTEGER	The grace period (number of days) when the number of blocks exceeds the soft limit
1.4	quotaFSFileMaxGrace (4)	INTEGER	The grace period (number of days) when the number of inodes exceeds the soft limit
1.5	quotaFSStatus (5)	INTEGER	Quota status (off/on) Each value represents the following: 0: off, 1: on, 2: group-on, 3: user-on
1.6	quotaFSUserTable (6)	-	Information about quota management for users
1.6.1	quotaUserEntry (1)	-	Information about quota management for each user
1.6.1.1	quotaUserIndex (1)	Integer32	Index number for a user
1.6.1.2	quotaUserUID (2)	Integer32	UID
1.6.1.3	quotaUserBlockCount (3)	INTEGER	The number (KB) of blocks being used
1.6.1.4	quotaUserFileCount (4)	INTEGER	The number of inodes being used
1.6.1.5	quotaUserBlockSoftLimit (5)	INTEGER	The soft limit for the number of blocks
1.6.1.6	quotaUserFileSoftLimit (6)	INTEGER	The soft limit for the number of inodes
1.6.1.7	quotaUserBlockHardLimit (7)	INTEGER	The hard limit for the number of blocks
1.6.1.8	quotaUserFileHardLimit (8)	INTEGER	The hard limit for the number of inodes
1.6.1.9	quotaUserBlockGracePeriod (9)	Counter32	Time (seconds) remaining for the grace period from when

ID	Object name	Type	Meaning
			the number of blocks exceeded the soft limit
1.6.1.10	quotaUserFileGracePeriod (10)	Counter32	Time (seconds) remaining for the grace period from when the number of inodes exceeded the soft limit
1.6.1.11	quotaUserBlockGracePeriodOver (11)	DisplayString	Outputs "over" when the grace period for the number of blocks exceeding the soft limit is expired.
1.6.1.12	quotaUserFileGracePeriodOver (12)	DisplayString	Outputs "over" when the grace period for the number of inodes exceeding the soft limit is expired.
1.6.1.13	quotaUser64UsedCount (13)	Counter64	The number of blocks used (64-bit compatible) (KB)
1.6.1.14	quotaUser64UsedMBCount (14)	Counter64	The number of blocks used (64-bit compatible) (MB)
1.6.1.15	quotaUser64UsedGBCount (15)	Counter64	The number of blocks used (64-bit compatible) (GB)
1.6.1.16	quotaUser64FileCount (16)	Counter64	The number of inodes used (64-bit compatible)
1.6.1.17	quotaUser64UsedSoftLimit (17)	Counter64	The soft limit for the number of blocks (64-bit compatible) (KB)
1.6.1.18	quotaUser64UsedMBSoftLimit (18)	Counter64	The soft limit for the number of blocks (64-bit compatible) (MB)
1.6.1.19	quotaUser64UsedGBSoftLimit (19)	Counter64	The soft limit for the number of blocks (64-bit compatible) (GB)
1.6.1.20	quotaUser64FileSoftLimit (20)	Counter64	The soft limit for the number of inodes (64-bit compatible)
1.6.1.21	quotaUser64UsedHardLimit (21)	Counter64	The hard limit for the number of blocks (64-bit compatible) (KB)
1.6.1.22	quotaUser64UsedMBHardLimit (22)	Counter64	The hard limit for the number of blocks (64-bit compatible) (MB)
1.6.1.23	quotaUser64UsedGBHardLimit (23)	Counter64	The hard limit for the number of blocks (64-bit compatible) (GB)
1.6.1.24	quotaUser64FileHardLimit (24)	Counter64	The hard limit for the number of inodes (64-bit compatible)
1.7	quotaFSGroupTable (7)	-	Information about quota management for groups

ID	Object name	Type	Meaning
1.7.1	quotaGroupEntry (1)	-	Information about quota management for each group
1.7.1.1	quotaGroupIndex (1)	Integer32	Index number for a group
1.7.1.2	quotaGroupGID (2)	Integer32	GID
1.7.1.3	quotaGroupBlockCount (3)	INTEGER	The number (KB) of blocks being used
1.7.1.4	quotaGroupFileCount (4)	INTEGER	The number of inodes being used
1.7.1.5	quotaGroupBlockSoftLimit (5)	INTEGER	The soft limit for the number of blocks
1.7.1.6	quotaGroupFileSoftLimit (6)	INTEGER	The soft limit for the number of inodes
1.7.1.7	quotaGroupBlockHardLimit (7)	INTEGER	The hard limit for the number of blocks
1.7.1.8	quotaGroupFileHardLimit (8)	INTEGER	The hard limit for the number of inodes
1.7.1.9	quotaGroupBlockGracePeriod (9)	Counter32	Time (seconds) remaining for the grace period from when the number of blocks exceeded the soft limit
1.7.1.10	quotaGroupFileGracePeriod (10)	Counter32	Time (seconds) remaining for the grace period from when the number of inodes exceeded the soft limit
1.7.1.11	quotaGroupBlockGracePeriodOver (11)	DisplayString	Shows "over" when the grace period is passed for the number of blocks exceeding the soft limit
1.7.1.12	quotaGroupFileGracePeriodOver (12)	DisplayString	Shows "over" when the grace period is passed for the number of inodes exceeding the soft limit
1.7.1.13	quotaGroup64UsedCount (13)	Counter64	The number of blocks used (64-bit compatible) (KB)
1.7.1.14	quotaGroup64UsedMBCount (14)	Counter64	The number of blocks used (64-bit compatible) (MB)
1.7.1.15	quotaGroup64UsedGBCount (15)	Counter64	The number of blocks used (64-bit compatible) (GB)
1.7.1.16	quotaGroup64FileCount (16)	Counter64	The number of inodes being used (for 64bit)
1.7.1.17	quotaGroup64UsedSoftLimit (17)	Counter64	The soft limit for the used capacity (for 64bit) (KB)
1.7.1.18	quotaGroup64UsedMBSoftLimit (18)	Counter64	The soft limit for the used capacity (for 64bit) (MB)

ID	Object name	Type	Meaning
1.7.1.19	quotaGroup64UsedGBSoftLimit (19)	Counter64	The soft limit for the used capacity (for 64bit) (GB)
1.7.1.20	quotaGroup64FileSoftLimit (20)	Counter64	The soft limit for the number of inodes (for 64bit)
1.7.1.21	quotaGroup64UsedHardLimit (21)	Counter64	The hard limit for the used capacity (for 64bit) (KB)
1.7.1.22	quotaGroup64UsedMBHardLimit (22)	Counter64	The hard limit for the used capacity (for 64bit) (MB)
1.7.1.23	quotaGroup64UsedGBHardLimit (23)	Counter64	The hard limit for the used capacity (for 64bit) (GB)
1.7.1.24	quotaGroup64FileHardLimit (24)	Counter64	The hard limit for the number of inodes (for 64bit)
2	quotaSubtreeEntry (2)	-	The subtree quota management information set for the directory
2.1	quotaSubtreeDirIndex (1)	INTEGER	The index number of the directory table
2.2	quotaSubtreeDirPath (2)	OCTET STRING	The directory path
2.3	quotaSubtreeDirUsed (3)	Counter64	The used capacity of the subtree quota (KB)
2.4	quotaSubtreeDirFileCount (4)	Counter64	The number of inodes being used
2.5	quotaSubtreeDirUsedSoftLimit (5)	Counter64	The soft limit for the used capacity (KB)
2.6	quotaSubtreeDirUsedMBSoftLimit (6)	Counter64	The soft limit for the used capacity (MB)
2.7	quotaSubtreeDirUsedGBSoftLimit (7)	Counter64	The soft limit for the used capacity (GB)
2.8	quotaSubtreeDirFileSoftLimit (8)	Counter64	The soft limit for the number of inodes
2.9	quotaSubtreeDirUsedHardLimit (9)	Counter64	The hard limit for the used capacity (KB)
2.10	quotaSubtreeDirUsedMBHardLimit (10)	Counter64	The hard limit for the used capacity (MB)
2.11	quotaSubtreeDirUsedGBHardLimit (11)	Counter64	The hard limit for the used capacity (GB)
2.12	quotaSubtreeDirFileHardLimit (12)	Counter64	The hard limit for the number of inodes
2.13	quotaSubtreeDirUsedSoftLimitPercent (13)	INTEGER	The used capacity as a percentage of the soft limit for the used capacity

ID	Object name	Type	Meaning
2.14	quotaSubtreeDirFileSoftLimitPercent (14)	INTEGER	The number of inodes as a percentage of the soft limit for the number of inodes
2.15	quotaSubtreeDirUsedHardLimitPercent (15)	INTEGER	The used capacity as a percentage of the hard limit for the used capacity
2.16	quotaSubtreeDirFileHardLimitPercent (16)	INTEGER	The number of inodes as a percentage of the hard limit for the number of inodes
2.17	quotaSubtreeDirUsedGracePeriod (17)	Counter32	The set grace period during which the soft limit for the used capacity can be exceeded (seconds)
2.18	quotaSubtreeDirFileGracePeriod (18)	Counter32	The set grace period during which the soft limit for the number of inodes can be exceeded (seconds)
2.19	quotaSubtreeUserTable (19)#	-	The user subtree quota management information
2.19.1	quotaSubtreeUserEntry (1)	-	The subtree quota management information for each user
2.19.1.1	quotaSubtreeUserIndex (1)	Integer32	The index number of the user ID
2.19.1.2	quotaSubtreeUserUID (2)	INTEGER	The user ID
2.19.1.3	quotaSubtreeUserUsed (3)	Counter64	The used capacity of the subtree quota (KB)
2.19.1.4	quotaSubtreeUserFileCount (4)	Counter64	The number of inodes being used
2.19.1.5	quotaSubtreeUserUsedSoftLimit (5)	Counter64	The soft limit for the used capacity (KB)
2.19.1.6	quotaSubtreeUserUsedMBSoftLimit (6)	Counter64	The soft limit for the used capacity (MB)
2.19.1.7	quotaSubtreeUserUsedGBSoftLimit (7)	Counter64	The soft limit for the used capacity (GB)
2.19.1.8	quotaSubtreeUserFileSoftLimit (8)	Counter64	The soft limit for the number of inodes
2.19.1.9	quotaSubtreeUserUsedHardLimit (9)	Counter64	The hard limit for the used capacity (KB)
2.19.1.10	quotaSubtreeUserUsedMBHardLimit (10)	Counter64	The hard limit for the used capacity (MB)
2.19.1.11	quotaSubtreeUserUsedGBHardLimit (11)	Counter64	The hard limit for the used capacity (GB)

ID	Object name	Type	Meaning
2.19.1.12	quotaSubtreeUserFileHardLimit (12)	Counter64	The hard limit for the number of inodes
2.19.1.13	quotaSubtreeUserUsedSoftLimitPercent (13)	INTEGER	The used capacity as a percentage of the soft limit for the used capacity
2.19.1.14	quotaSubtreeUserFileSoftLimitPercent (14)	INTEGER	The number of inodes as a percentage of the soft limit for the number of inodes
2.19.1.15	quotaSubtreeUserUsedHardLimitPercent (15)	INTEGER	The used capacity as a percentage of the hard limit for the used capacity
2.19.1.16	quotaSubtreeUserFileHardLimitPercent (16)	INTEGER	The number of inodes as a percentage of the hard limit for the number of inodes
2.19.1.17	quotaSubtreeUserUsedGracePeriod (17)	Counter32	The set grace period during which the soft limit for the used capacity can be exceeded (seconds)
2.19.1.18	quotaSubtreeUserFileGracePeriod (18)	Counter32	The set grace period during which the soft limit for the number of inodes can be exceeded (seconds)
2.19.1.19	quotaSubtreeUserUsedGracePeriodOver (19)	DisplayString	Shows "over" when the grace period is passed for the number of blocks exceeding the soft limit
2.19.1.20	quotaSubtreeUserFileGracePeriodOver (20)	DisplayString	Shows "over" when the grace period is passed for the number of inodes exceeding the soft limit
2.19.1.21	quotaSubtreeUserUsedMB (21)	Counter64	The used capacity of the subtree quota (MB)
2.19.1.22	quotaSubtreeUserUsedGB (22)	Counter64	The used capacity of the subtree quota (GB)
2.20	quotaSubtreeGroupTable (20)#	-	The group subtree quota management information
2.20.1	quotaSubtreeGroupEntry (1)	-	The subtree quota management information for each group
2.20.1.1	quotaSubtreeGroupIndex (1)	Integer32	The index number for the group
2.20.1.2	quotaSubtreeGroupGID (2)	INTEGER	The group ID
2.20.1.3	quotaSubtreeGroupUsed (3)	Counter64	The used capacity of the subtree quota (KB)

ID	Object name	Type	Meaning
2.20.1.4	quotaSubtreeGroupFileCount (4)	Counter64	The number of inodes being used
2.20.1.5	quotaSubtreeGroupUsedSoftLimit (5)	Counter64	The soft limit for the used capacity (KB)
2.20.1.6	quotaSubtreeGroupUsedMBSofLimit (6)	Counter64	The soft limit for the used capacity (MB)
2.20.1.7	quotaSubtreeGroupUsedGBSoftLimit (7)	Counter64	The soft limit for the used capacity (GB)
2.20.1.8	quotaSubtreeGroupFileSoftLimit (8)	Counter64	The soft limit for the number of inodes
2.20.1.9	quotaSubtreeGroupUsedHardLimit (9)	Counter64	The hard limit for the used capacity (KB)
2.20.1.10	quotaSubtreeGroupUsedMBHardLimit (10)	Counter64	The hard limit for the used capacity (MB)
2.20.1.11	quotaSubtreeGroupUsedGBHardLimit (11)	Counter64	The hard limit for the used capacity (GB)
2.20.1.12	quotaSubtreeGroupFileHardLimit (12)	Counter64	The hard limit for the number of inodes
2.20.1.13	quotaSubtreeGroupUsedSoftLimitPercent (13)	INTEGER	The used capacity as a percentage of the soft limit for the used capacity
2.20.1.14	quotaSubtreeGroupFileSoftLimitPercent (14)	INTEGER	The number of inodes as a percentage of the soft limit for the number of inodes
2.20.1.15	quotaSubtreeGroupUsedHardLimitPercent (15)	INTEGER	The used capacity as a percentage of the hard limit for the used capacity
2.20.1.16	quotaSubtreeGroupFileHardLimitPercent (16)	INTEGER	The number of inodes as a percentage of the hard limit for the number of inodes
2.20.1.17	quotaSubtreeGroupUsedGracePeriod (17)	Counter32	The set grace period during which the soft limit for the used capacity can be exceeded (seconds)
2.20.1.18	quotaSubtreeGroupFileGracePeriod (18)	Counter32	The set grace period during which the soft limit for the number of inodes can be exceeded (seconds)
2.20.1.19	quotaSubtreeGroupUsedGracePeriodOver (19)	DisplayString	Shows "over" when the grace period is passed for the number of blocks exceeding the soft limit
2.20.1.20	quotaSubtreeGroupFileGracePeriodOver (20)	DisplayString	Shows "over" when the grace period is passed for the number of inodes exceeding the soft limit

ID	Object name	Type	Meaning
2.20.1.21	quotaSubtreeGroupUsedMB (21)	Counter64	The used capacity of the subtree quota (MB)
2.20.1.22	quotaSubtreeGroupUsedGB (22)	Counter64	The used capacity of the subtree quota (GB)
2.21	quotaSubtreeDirUsedGracePeriodOver (21)	DisplayString	Shows "over" when the grace period is passed for the number of blocks exceeding the soft limit
2.22	quotaSubtreeDirFileGracePeriodOver (22)	DisplayString	Shows "over" when the grace period is passed for the number of inodes exceeding the soft limit
2.23	quotaSubtreeDirUsedMB (23)	Counter64	The used capacity of the subtree quota (MB)
2.24	quotaSubtreeDirUsedGB (24)	Counter64	The used capacity of the subtree quota (GB)
#: If multiple subtree quotas are set for the tree of directories that have parent-child relationships (from top to bottom), MIB objects are acquired only for the lowest subtree quota in that directory tree.			

Table G-23 stdExMibNfs (4) group

ID	Object name	Type	Meaning
1	stdExMibNfsRpcStats (1)	-	Number of RPC requests since system activation
1.1	nfsCALLS (1)	Counter32	The total number of RPC requests
1.2	nfsBADCALLS (2)	Counter32	The number of requests deleted in the RPC layer
1.3	nfsXDRCALL (3)	Counter32	The number of requests that have headers that XDR cannot decipher
2	stdExMibNfsV2ProcCall (2)	-	Number of received NFSv2 procedure calls
2.1	nfsV2ProcNULL (1)	Counter32	The number of received NULL procedure calls
2.2	nfsV2ProcGETATTR (2)	Counter32	The number of received GETATTR procedure calls
2.3	nfsV2ProcSETATTR (3)	Counter32	The number of received SETATTR procedure calls
2.4	nfsV2ProcROOT (4)	Counter32	The number of received ROOT procedure calls
2.5	nfsV2ProcLOOKUP (5)	Counter32	The number of received LOOKUP procedure calls
2.6	nfsV2ProcREADLINK (6)	Counter32	The number of received READLINK procedure calls

ID	Object name	Type	Meaning
2.7	nfsV2ProcREAD (7)	Counter32	The number of received READ procedure calls
2.8	nfsV2ProcWRITECACHE (8)	Counter32	The number of received WRITECACHE procedure calls
2.9	nfsV2ProcWRITE (9)	Counter32	The number of received WRITE procedure calls
2.10	nfsV2ProcCREATE (10)	Counter32	The number of received CREATE procedure calls
2.11	nfsV2ProcREMOVE (11)	Counter32	The number of received REMOVE procedure calls
2.12	nfsV2ProcRENAME (12)	Counter32	The number of received RENAME procedure calls
2.13	nfsV2ProcLINK (13)	Counter32	The number of received LINK procedure calls
2.14	nfsV2ProcSYMLINK (14)	Counter32	The number of received SYMLINK procedure calls
2.15	nfsV2ProcMKDIR (15)	Counter32	The number of received MKDIR procedure calls
2.16	nfsV2ProcRMDIR (16)	Counter32	The number of received RMDIR procedure calls
2.17	nfsV2ProcREaddir (17)	Counter32	The number of received REaddir procedure calls
2.18	nfsV2ProcFSSTAT (18)	Counter32	The number of received FSSTAT procedure calls
3	stdExMibNfsV2TotalProcCall (3)	-	Statistics of individual NFSv2 calls (in %)
3.1	nfsV2TotalProcNULL (1)	INTEGER	Statistics (%) for NULL procedure calls
3.2	nfsV2TotalProcGETATTR (2)	INTEGER	Statistics (%) for GETATTR procedure calls
3.3	nfsV2TotalProcSETATTR (3)	INTEGER	Statistics (%) for SETATTR procedure calls
3.4	nfsV2TotalProcROOT (4)	INTEGER	Statistics (%) for ROOT procedure calls
3.5	nfsV2TotalProcLOOKUP (5)	INTEGER	Statistics (%) for LOOKUP procedure calls
3.6	nfsV2TotalProcREADLINK (6)	INTEGER	Statistics (%) for READLINK procedure calls
3.7	nfsV2TotalProcREAD (7)	INTEGER	Statistics (%) for READ procedure calls
3.8	nfsV2TotalProcWRITECACHE (8)	INTEGER	Statistics (%) for WRITECACHE procedure calls

ID	Object name	Type	Meaning
3.9	nfsV2TotalProcWRITE (9)	INTEGER	Statistics (%) for WRITE procedure calls
3.10	nfsV2TotalProcCREATE (10)	INTEGER	Statistics (%) for CREATE procedure calls
3.11	nfsV2TotalProcREMOVE (11)	INTEGER	Statistics (%) for REMOVE procedure calls
3.12	nfsV2TotalProcRENAME (12)	INTEGER	Statistics (%) for RENAME procedure calls
3.13	nfsV2TotalProcLINK (13)	INTEGER	Statistics (%) for LINK procedure calls
3.14	nfsV2TotalProcSYMLINK (14)	INTEGER	Statistics (%) for SYMLINK procedure calls
3.15	nfsV2TotalProcMKDIR (15)	INTEGER	Statistics (%) for MKDIR procedure calls
3.16	nfsV2TotalProcRMDIR (16)	INTEGER	Statistics (%) for RMDIR procedure calls
3.17	nfsV2TotalProcREADDIR (17)	INTEGER	Statistics (%) for READDIR procedure calls
3.18	nfsV2TotalProcFSSTAT (18)	INTEGER	Statistics (%) for FSSTAT procedure calls
4	stdExMibNfsV3ProcCall (4)	-	Number of received NFSv3 procedure calls
4.1	nfsV3ProcNULL (1)	Counter32	The number of received NULL procedure calls
4.2	nfsV3ProcGETATTR (2)	Counter32	The number of received GETATTR procedure calls
4.3	nfsV3ProcSETATTR (3)	Counter32	The number of received SETATTR procedure calls
4.4	nfsV3ProcLOOKUP (4)	Counter32	The number of received LOOKUP procedure calls
4.5	nfsV3ProcACCESS (5)	Counter32	The number of received ACCESS procedure calls
4.6	nfsV3ProcREADLINK (6)	Counter32	The number of received READLINK procedure calls
4.7	nfsV3ProcREAD (7)	Counter32	The number of received READ procedure calls
4.8	nfsV3ProcWRITE (8)	Counter32	The number of received WRITE procedure calls
4.9	nfsV3ProcCREATE (9)	Counter32	The number of received CREATE procedure calls
4.10	nfsV3ProcMKDIR (10)	Counter32	The number of received WRITECACHE procedure calls

ID	Object name	Type	Meaning
4.11	nfsV3ProcSYMLINK (11)	Counter32	The number of received SYMLINK procedure calls
4.12	nfsV3ProcMKNOD (12)	Counter32	The number of received MKNOD procedure calls
4.13	nfsV3ProcREMOVE (13)	Counter32	The number of received REMOVE procedure calls
4.14	nfsV3ProcRMDIR (14)	Counter32	The number of received RMDIR procedure calls
4.15	nfsV3ProcRENAME (15)	Counter32	The number of received RENAME procedure calls
4.16	nfsV3ProcLINK (16)	Counter32	The number of received LINK procedure calls
4.17	nfsV3ProcREaddir (17)	Counter32	The number of received REaddir procedure calls
4.18	nfsV3ProcREaddirplus (18)	Counter32	The number of received REaddirplus procedure calls
4.19	nfsV3ProcFSSTAT (19)	Counter32	The number of received FSSTAT procedure calls
4.20	nfsV3ProcFSINFO (20)	Counter32	The number of received FSINFO procedure calls
4.21	nfsV3ProcPATHCONF (21)	Counter32	The number of received PATHCONF procedure calls
4.22	nfsV3ProcCOMMIT (22)	Counter32	The number of received COMMIT procedure calls
5	stdExMibNfsV3TotalProcCall (5)	-	Statistics of individual NFSv3 calls (in %)
5.1	nfsV3TotalProcNULL (1)	INTEGER	Statistics (%) for NULL procedure calls
5.2	nfsV3TotalProcGETATTR (2)	INTEGER	Statistics (%) for GETATTR procedure calls
5.3	nfsV3TotalProcSETATTR (3)	INTEGER	Statistics (%) for SETATTR procedure calls
5.4	nfsV3TotalProcLOOKUP (4)	INTEGER	Statistics (%) for LOOKUP procedure calls
5.5	nfsV3TotalProcACCESS (5)	INTEGER	Statistics (%) for ACCESS procedure calls
5.6	nfsV3TotalProcREADLINK (6)	INTEGER	Statistics (%) for READLINK procedure calls
5.7	nfsV3TotalProcREAD (7)	INTEGER	Statistics (%) for READ procedure calls
5.8	nfsV3TotalProcWRITE (8)	INTEGER	Statistics (%) for WRITE procedure calls

ID	Object name	Type	Meaning
5.9	nfsV3TotalProcCREATE (9)	INTEGER	Statistics (%) for CREATE procedure calls
5.10	nfsV3TotalProcMKDIR (10)	INTEGER	Statistics (%) for MKDIR procedure calls
5.11	nfsV3TotalProcSYMLINK (11)	INTEGER	Statistics (%) for SYMLINK procedure calls
5.12	nfsV3TotalProcMKNOD (12)	INTEGER	Statistics (%) for MKNOD procedure calls
5.13	nfsV3TotalProcREMOVE (13)	INTEGER	Statistics (%) for REMOVE procedure calls
5.14	nfsV3TotalProcRMDIR (14)	INTEGER	Statistics (%) for RMDIR procedure calls
5.15	nfsV3TotalProcRENAME (15)	INTEGER	Statistics (%) for RENAME procedure calls
5.16	nfsV3TotalProcLINK (16)	INTEGER	Statistics (%) for LINK procedure calls
5.17	nfsV3TotalProcREADDIR (17)	INTEGER	Statistics (%) for READDIR procedure calls
5.18	nfsV3TotalProcREADDIRPLUS (18)	INTEGER	Statistics (%) for READDIRPLUS procedure calls
5.19	nfsV3TotalProcFSSTAT (19)	INTEGER	Statistics (%) for FSSTAT procedure calls
5.20	nfsV3TotalProcFSINFO (20)	INTEGER	Statistics (%) for FSINFO procedure calls
5.21	nfsV3TotalProcPATHCONF (21)	INTEGER	Statistics (%) for PATHCONF procedure calls
5.22	nfsV3TotalProcCOMMIT (22)	INTEGER	Statistics (%) for COMMIT procedure calls
6	stdExMibNfsV4Call (6)	-	Number of received NFSv4 procedure calls or operations
6.1	nfsV4ProcNULL (1)	Counter32	Number of received NULL procedure calls
6.2	nfsV4ProcCOMPOUND (2)	Counter32	Number of received COMPOUND procedure calls
6.3	nfsV4OperACCESS (3)	Counter32	Number of received ACCESS operations
6.4	nfsV4OperCLOSE (4)	Counter32	Number of received CLOSE operations
6.5	nfsV4OperCOMMIT (5)	Counter32	Number of received COMMIT operations
6.6	nfsV4OperCREATE (6)	Counter32	Number of received CREATE operations

ID	Object name	Type	Meaning
6.7	nfsV4OperDELEGPURGE (7)	Counter32	Number of received DELEGPURGE operations
6.8	nfsV4OperDELEGRETURN (8)	Counter32	Number of received DELEGRETURN operations
6.9	nfsV4OperGETATTR (9)	Counter32	Number of received GETATTR operations
6.10	nfsV4OperGETFH (10)	Counter32	Number of received GETFH operations
6.11	nfsV4OperLINK (11)	Counter32	Number of received LINK operations
6.12	nfsV4OperLOCK (12)	Counter32	Number of received LOCK operations
6.13	nfsV4OperLOCKT (13)	Counter32	Number of received LOCKT operations
6.14	nfsV4OperLOCKU (14)	Counter32	Number of received LOCKU operations
6.15	nfsV4OperLOOKUP (15)	Counter32	Number of received LOOKUP operations
6.16	nfsV4OperLOOKUPROOT (16)	Counter32	Number of received LOOKUPROOT operations
6.17	nfsV4OperNVERIFY (17)	Counter32	Number of received NVERIFY operations
6.18	nfsV4OperOPEN (18)	Counter32	Number of received OPEN operations
6.19	nfsV4OperOPENATTR (19)	Counter32	Number of received OPENATTR operations
6.20	nfsV4OperOPENCONF (20)	Counter32	Number of received OPENCONF operations
6.21	nfsV4OperOPENDGRD (21)	Counter32	Number of received OPENDGRD operations
6.22	nfsV4OperPUTFH (22)	Counter32	Number of received PUTFH operations
6.23	nfsV4OperPUTPUBFH (23)	Counter32	Number of received PUTPUBFH operations
6.24	nfsV4OperPUTROOTFH (24)	Counter32	Number of received PUTROOTFH operations
6.25	nfsV4OperREAD (25)	Counter32	Number of received READ operations
6.26	nfsV4OperREaddir (26)	Counter32	Number of received REaddir operations
6.27	nfsV4OperREADLINK (27)	Counter32	Number of received READLINK operations

ID	Object name	Type	Meaning
6.28	nfsV4OperREMOVE (28)	Counter32	Number of received REMOVE operations
6.29	nfsV4OperRENAME (29)	Counter32	Number of received RENAME operations
6.30	nfsV4OperRENEW (30)	Counter32	Number of received RENEW operations
6.31	nfsV4OperRESTOREFH (31)	Counter32	Number of received RESTOREFH operations
6.32	nfsV4OperSAVEFH (32)	Counter32	Number of received SAVEFH operations
6.33	nfsV4OperSECINFO (33)	Counter32	Number of received SECINFO operations
6.34	nfsV4OperSETATTR (34)	Counter32	Number of received SETATTR operations
6.35	nfsV4OperSETCLTID (35)	Counter32	Number of received SETCLTID operations
6.36	nfsV4OperSETCLTIDCONF (36)	Counter32	Number of received SETCLTIDCONF operations
6.37	nfsV4OperVERIFY (37)	Counter32	Number of received VERIFY operations
6.38	nfsV4OperWRITE (38)	Counter32	Number of received WRITE operations
6.39	nfsV4OperRELOCKOWNER (39)	Counter32	Number of received RELOCKOWNER operations
7	stdExMibNfsV4TotalCall (7)	-	Statistics (%) based on the number of received NFSv4 total procedure calls or total operations as the parameter
7.1	nfsV4TotalProcNULL (1)	INTEGER	Statistics (%) for NULL procedure calls
7.2	nfsV4TotalProcCOMPOUND (2)	INTEGER	Statistics (%) for COMPOUND procedure calls
7.3	nfsV4TotalOperACCESS (3)	INTEGER	Statistics (%) for ACCESS operations
7.4	nfsV4TotalOperCLOSE (4)	INTEGER	Statistics (%) for CLOSE operations
7.5	nfsV4TotalOperCOMMIT (5)	INTEGER	Statistics (%) for COMMIT operations
7.6	nfsV4TotalOperCREATE (6)	INTEGER	Statistics (%) for CREATE operations
7.7	nfsV4TotalOperDELEGPURGE (7)	INTEGER	Statistics (%) for DELEGPURGE operations

ID	Object name	Type	Meaning
7.8	nfsV4TotalOperDELEGRETURN (8)	INTEGER	Statistics (%) for DELEGRETURN operations
7.9	nfsV4TotalOperGETATTR (9)	INTEGER	Statistics (%) for GETATTR operations
7.10	nfsV4TotalOperGETFH (10)	INTEGER	Statistics (%) for GETFH operations
7.11	nfsV4TotalOperLINK (11)	INTEGER	Statistics (%) for LINK operations
7.12	nfsV4TotalOperLOCK (12)	INTEGER	Statistics (%) for LOCK operations
7.13	nfsV4TotalOperLOCKT (13)	INTEGER	Statistics (%) for LOCKT operations
7.14	nfsV4TotalOperLOCKU (14)	INTEGER	Statistics (%) for LOCKU operations
7.15	nfsV4TotalOperLOOKUP (15)	INTEGER	Statistics (%) for LOOKUP operations
7.16	nfsV4TotalOperLOOKUPROOT (16)	INTEGER	Statistics (%) for LOOKUPROOT operations
7.17	nfsV4TotalOperNVERIFY (17)	INTEGER	Statistics (%) for NVERIFY operations
7.18	nfsV4TotalOperOPEN (18)	INTEGER	Statistics (%) for OPEN operations
7.19	nfsV4TotalOperOPENATTR (19)	INTEGER	Statistics (%) for OPENATTR operations
7.20	nfsV4TotalOperOPENCONF (20)	INTEGER	Statistics (%) for OPENCONF operations
7.21	nfsV4TotalOperOPENDGRD (21)	INTEGER	Statistics (%) for OPENDGRD operations
7.22	nfsV4TotalOperPUTFH (22)	INTEGER	Statistics (%) for PUTFH operations
7.23	nfsV4TotalOperPUTPUBFH (23)	INTEGER	Statistics (%) for PUTPUBFH operations
7.24	nfsV4TotalOperPUTROOTFH (24)	INTEGER	Statistics (%) for PUTROOTFH operations
7.25	nfsV4TotalOperREAD (25)	INTEGER	Statistics (%) for READ operations
7.26	nfsV4TotalOperREaddir (26)	INTEGER	Statistics (%) for REaddir operations
7.27	nfsV4TotalOperREADLINK (27)	INTEGER	Statistics (%) for READLINK operations
7.28	nfsV4TotalOperREMOVE (28)	INTEGER	Statistics (%) for REMOVE operations
7.29	nfsV4TotalOperRENAME (29)	INTEGER	Statistics (%) for RENAME operations
7.30	nfsV4TotalOperRENEW (30)	INTEGER	Statistics (%) for RENEW operations

ID	Object name	Type	Meaning
7.31	nfsV4TotalOperRESTOREFH (31)	INTEGER	Statistics (%) for RESTOREFH operations
7.32	nfsV4TotalOperSAVEFH (32)	INTEGER	Statistics (%) for SAVEFH operations
7.33	nfsV4TotalOperSECINFO (33)	INTEGER	Statistics (%) for SECINFO operations
7.34	nfsV4TotalOperSETATTR (34)	INTEGER	Statistics (%) for SETATTR operations
7.35	nfsV4TotalOperSETCLTID (35)	INTEGER	Statistics (%) for SETCLTID operations
7.36	nfsV4TotalOperSETCLTIDCONF (36)	INTEGER	Statistics (%) for SETCLTIDCONF operations
7.37	nfsV4TotalOperVERIFY (37)	INTEGER	Statistics (%) for VERIFY operations
7.38	nfsV4TotalOperWRITE (38)	INTEGER	Statistics (%) for WRITE operations
7.39	nfsV4TotalOperRELOCKOWNER (39)	INTEGER	Statistics (%) for RELOCKOWNER operations

Table G-24 stdExMibCifs (5) group

ID	Object name	Type	Meaning
1	stdExMibCifsItem (1)	-	CIFS item
1.1	cifsWorkGroup (1)	DisplayString	Workgroup name
1.2	cifsSeverComment (2)	DisplayString	Server comment ^{#1}
1.3	cifsSecurity (3)	DisplayString	Authentication mode
1.4	cifsPasswordServer (4)	DisplayString	Authentication server ^{#1}
1.5	cifsSharesCount (5)	INTEGER	The number of current CIFS shares
1.6	cifsSessionCount (6)	Counter32	The number of current sessions ^{#2}
<p>^{#1}: No more than 255 characters are shown, and the 256th and subsequent characters are truncated.</p> <p>^{#2}: The CIFS sessions established by specifying a NetBIOS name and those established by specifying a virtual IP address are counted separately even when the sessions are established concurrently from the same client.</p>			

Table G-25 stdExMibNetwork (6) group

ID	Object name	Type	Meaning
1	stdExMibIPAddressTable (1)	-	IP address management
1.1	ipAddressEntry (1) ^{#1}	-	Details about each IP address

ID	Object name	Type	Meaning
1.1.1	ipAddressIFIndex (1)	Integer32	Index number for each network interface
1.1.2	ipAddressAddr (2)# ²	IpAddress	IP address
1.1.3	ipAddressIFName (3)	DisplayString	Network interface name
1.1.4	ipv6IpAddressAddr (4)	DisplayString	IP address (IPv6)
2	stdExMibDefaultGateway (2)	IpAddress	Default gateway
3	stdExMibLinkAggregationGroup Table (3)	-	Trunking group information
3.1	lagEntry (1)	-	Trunking group entry
3.1.1	lagIndex (1)	Integer32	Trunking group index
3.1.2	lagMasterDeviceName (2)	DisplayString	Master device interface name for the trunking group
3.1.3	lagIpAddress (3)	IpAddress	Trunking group IP address
3.1.4	lagSubDeviceName (4)	DisplayString	Subdevice interface name for the trunking group
3.1.5	ipv6LagIpAddress (5)	DisplayString	Trunking group IP address (IPv6)
4	ipv6StdExMibDefaultGateway (4)	DisplayString	Default gateway (IPv6)
<p>#1: The IP address entries are output in the following order: management port, data ports, private maintenance port, and heartbeat port. The maximum number of entries is the number of installed data ports + 3.</p> <p>#2: Acquisition of this MIB might fail because there is a standard MIB with the same name. If acquisition fails, specify the following:</p> <pre>iso.org.dod.internet.private.enterprises.hitachi.systemExMib.storageExMib.stdExMib.stdExMibRAID.stdExMibRoot.stdExMibNetwork.stdExMibIPAddressTable.ipAddressEntry.ipAddressAddr</pre>			

Table G-26 stdExMibPerformManager (7) group

ID	Object name	Type	Meaning
1	stdExMibNWPerformManagerTable (1)	-	Network performance monitoring
1.1	netWorkPmEntry (1)	-	Network performance monitoring for each interface
1.1.1	nwpmIFIndex (1)	Integer32	Index number for each network interface
1.1.2	nwpmRcvPacket (2)	Counter32	(This object is no longer available.)
1.1.3	nwpmSendPacket (3)	Counter32	(This object is no longer available.)
1.1.4	nwpmCollision (4)	Counter32	The number of collisions

ID	Object name	Type	Meaning
1.1.5	nwpmBuffErrRcvPacket (5)	Counter32	The number of received packets that were discarded because of buffer insufficiency
1.1.6	nwpmBuffErrSendPacket (6)	Counter32	(This object is no longer available.)
1.1.7	nwpmPacketSendCareerErr (7)	Counter32	The number of career errors that occurred when sending packets
1.1.8	nwpmFrmAlignmentErr (8)	Counter32	The number of frame alignment errors
1.1.9	nwpmFIFOSendOverRunErr (9)	Counter32	(This object is no longer available.)
1.1.10	nwpmFIFORcvOverRunErr (10)	Counter32	The number of FIFO overrun errors (receiving)
2	stdExMibLagPerformManagerTable (2)	-	Performance monitoring information for the trunking group
2.1	lagPerformManagerEntry (1)	-	Performance monitoring entry for the trunking group
2.1.1	lagpmIFIndex (1)	Integer32	Trunking group interface index
2.1.2	lagpmRcvPacket (2)	Counter32	Number of received compressed packets for the trunking group
2.1.3	lagpmSendPacket (3)	Counter32	Number of sent compressed packets for the trunking group
2.1.4	lagpmCollision (4)	Counter32	Number of times a collision occurred for the trunking group
2.1.5	lagpmBuffErrRcvPacket (5)	Counter32	Number of received packets discarded because of an insufficiency for the trunking group buffer
2.1.6	lagpmBuffErrSendPacket (6)	Counter32	Number of sent packets discarded because of an insufficiency for the trunking group buffer
2.1.7	lagpmPacketSendCareerErr (7)	Counter32	Number of carrier errors that occurred during sending of trunking group packets
2.1.8	lagpmFrmAlignmentErr (8)	Counter32	Number of frame alignment errors for the trunking group
2.1.9	lagpmFIFOSendOverRunErr (9)	Counter32	Number of FIFO overrun errors for the trunking group (during sending)
2.1.10	lagpmFIFORcvOverRunErr (10)	Counter32	Number of FIFO overrun errors for the trunking group (during receiving)

Table G-27 stdExMibFileSystem (11) group

ID	Object name	Type	Meaning
1	fileSystemTable (1)	-	File systems management
1.1	fileSystemEntry (1)	-	Management information for each file system
1.1.1	fileSystemIndex (1)	Integer32	Index
1.1.2	fileSystemName (2)	DisplayString	File system path
1.1.3	fileSystemTotalCapacity (3)	Counter32	File system total capacity (MB)
1.1.4	fileSystemDeviceStatus (4)	INTEGER	Device file status Each value represents the following: 0: normal, 1: error
1.1.5	fileSystemKBCapacity (5)	Counter64	File system block capacity (KB)
1.1.6	fileSystemMBCapacity (6)	Counter64	File system block capacity (MB)
1.1.7	fileSystemGBCapacity (7)	Counter64	File system block capacity (GB)
1.1.8	fileSystemKBUsed (8)	Counter64	File system block usage (KB)
1.1.9	fileSystemMBUsed (9)	Counter64	File system block usage (MB)
1.1.10	fileSystemGBUsed (10)	Counter64	File system block usage (GB)
1.1.11	fileSystemUsedPercent (11)	INTEGER	File system usage rate (%)
1.1.12	fileSystemKBAvail (12)	Counter64	File system unused capacity (KB)
1.1.13	fileSystemMBAvail (13)	Counter64	File system unused capacity (MB)
1.1.14	fileSystemGBAvail (14)	Counter64	File system unused capacity (GB)
1.1.15	fileSystemInodeUsed (15)	Counter64	Number of used inodes
1.1.16	fileSystemInodeFree (16)	Counter64	Number of unused inodes
1.1.17	fileSystemMaxUsedInode (17)	INTEGER	Maximum percentage of the total capacity that can be used by inodes (%)
1.1.18	fileSystemVolumeManager (18)	INTEGER	Whether a volume manager can be used Each value represents the following: 0: --, 1: use
1.1.19	fileSystemMountStatus (19)	INTEGER	Mount status Each value represents the following: 0: ro, 1: rw, 2: --, 3: fatal error, 4: overflow, 5: not available, 6: blocked,

ID	Object name	Type	Meaning
			7: blocked and ready, 8: expanding, 9: reclaim
1.1.20	fileSystemTiering (20)	INTEGER	Whether tiers can be used Each value represents the following: 0: --, 1: use
1.1.70	fileSystemTier1Device Status (70)	INTEGER	Device file status of the file system (tier 1) Each value represents the following: 0: normal, 1: error
1.1.71	fileSystemTier1KBCapacity (71)	Counter64	Block capacity (KB) of the file system (tier 1)
1.1.72	fileSystemTier1MBCapacity (72)	Counter64	Block capacity (MB) of the file system (tier 1)
1.1.73	fileSystemTier1GBCapacity (73)	Counter64	Block capacity (GB) of the file system (tier 1)
1.1.74	fileSystemTier1KBUsed (74)	Counter64	Block usage (KB) of the file system (tier 1)
1.1.75	fileSystemTier1MBUsed (75)	Counter64	Block usage (MB) of the file system (tier 1)
1.1.76	fileSystemTier1GBUsed (76)	Counter64	Block usage (GB) of the file system (tier 1)
1.1.77	fileSystemTier1UsedPercent (77)	INTEGER	File system (tier 1) usage rate (%)
1.1.78	fileSystemTier1KBAvail (78)	Counter64	Unused capacity (KB) of the file system (tier 1)
1.1.79	fileSystemTier1MBAvail (79)	Counter64	Unused capacity (MB) of the file system (tier 1)
1.1.80	fileSystemTier1GBAvail (80)	Counter64	Unused capacity (GB) of the file system (tier 1)
1.1.81	fileSystemTier1InodeUsed (81)	Counter64	Number of inodes used by the file system (tier 1)
1.1.82	fileSystemTier1InodeFree (82)	Counter64	Number of inodes not used by the file system (tier 1)
1.1.83	fileSystemTier1MountStatus (83)	INTEGER	Mount status of the file system (tier 1) Each value represents the following: 0: ro, 1: rw, 2: --, 3: fatal error, 4: overflow, 5: not available, 6: blocked, 7: blocked and ready, 8: expanding, 9: reclaim
1.1.90	fileSystemTier2Device Status (90)	INTEGER	Device file status of the file system (tier 2) Each value represents the following:

ID	Object name	Type	Meaning
			0: normal, 1: error
1.1.91	fileSystemTier2KBCapacity (91)	Counter64	Block capacity (KB) of the file system (tier 2)
1.1.92	fileSystemTier2MBCapacity (92)	Counter64	Block capacity (MB) of the file system (tier 2)
1.1.93	fileSystemTier2GBCapacity (93)	Counter64	Block capacity (GB) of the file system (tier 2)
1.1.94	fileSystemTier2KBUsed (94)	Counter64	Block usage (KB) of the file system (tier 2)
1.1.95	fileSystemTier2MBUsed (95)	Counter64	Block usage (MB) of the file system (tier 2)
1.1.96	fileSystemTier2GBUsed (96)	Counter64	Block usage (GB) of the file system (tier 2)
1.1.97	fileSystemTier2UsedPercent (97)	INTEGER	File system (tier 2) usage rate (%)
1.1.98	fileSystemTier2KBAvail (98)	Counter64	Unused capacity (KB) of the file system (tier 2)
1.1.99	fileSystemTier2MBAvail (99)	Counter64	Unused capacity (MB) of the file system (tier 2)
1.1.100	fileSystemTier2GBAvail (100)	Counter64	Unused capacity (GB) of the file system (tier 2)
1.1.101	fileSystemTier2InodeUsed (101)	Counter64	Number of inodes used by the file system (tier 2)
1.1.102	fileSystemTier2InodeFree (102)	Counter64	Number of inodes not used by the file system (tier 2)
1.1.103	fileSystemTier2MountStatus (103)	INTEGER	Mount status of the file system (tier 2) Each value represents the following: 0: ro, 1: rw, 2: --, 3: fatal error, 4: overflow, 5: not available, 6: blocked, 7: blocked and ready, 8: expanding, 9: reclaim
2	fileSystemLUInfoTable (2)	-	Information about the LUs that make up file systems
2.1	fileSystemLUInfoEntry (1)	-	Information about an LU that makes up a file system
2.1.1	fileSystemLUInfoIndex (1)	Integer32	Index
2.1.2	fileSystemLUInfoDevice (2)	DisplayString	Logical unit number in the file system
2.1.3	fileSystemLUInfoFSName (3)	DisplayString	File system name

ID	Object name	Type	Meaning
2.1.4	fileSystemLUInfoDeviceInfo (4)	INTEGER	Storage device information Each value represents the following: 0: P-vol, 1: D-vol
2.1.5	fileSystemLUInfoSerial (5)	DisplayString	Serial number
2.1.6	fileSystemLUInfoDataPool (6)	DisplayString	DP number for a data pool that makes up the file system

Table G-28 stdExMibHDPPool (12) group

ID	Object name	Type	Meaning
1	hdpPoolTable (1)	-	Pool management information
1.1	hdpPoolEntry (1)	-	Management information for each pool
1.1.1	hdpPoolIndex (1)	Integer32	Index
1.1.2	hdpPoolNumber (2)	DisplayString	Pool number
1.1.3	hdpPoolSerialNumber (3)	DisplayString	Serial number
1.1.4	hdpPoolDrive (4)	INTEGER	Drive type Each value represents the following: 0: FC/SAS, 1: SATA, 2: SSD, 3: SAS7K, 99: -
1.1.5	hdpPoolTotal (5)	Counter32	Total pool capacity (GB)
1.1.6	hdpPoolUsed (6)	Counter32	Used pool capacity (GB)
1.1.7	hdpPoolFree (7)	Counter32	Unused pool capacity (GB)
1.1.8	hdpPoolUsedPercent (8)	INTEGER	Pool usage rate (%)
1.1.9	hdpPoolEarlyAlertPercent (9)	INTEGER	Warning threshold (%)
1.1.10	hdpPoolDepletionAlertPercent (10)	INTEGER	Critical threshold (%)
1.1.11	hdpPoolPvolFileSystemName (11)	OCTET STRING	File systems used by the pool

MIB objects used for SNMP traps

The following table lists the groups of MIB objects in the HDI system used for SNMP traps and the tables to be referenced for each group.

Table G-29 Groups of MIB objects used in SNMP traps and tables to be referenced

Group name	Description	Tables
stdExMibQuotaTrapFS (3)	A group related to quota monitoring.	Table G-30 stdExMibQuotaTrapFS (3) group on page G-70
stdExMibEvent (8)	A group related to event monitoring.	Table G-31 stdExMibEvent (8) group on page G-78

Tables [Table G-30 stdExMibQuotaTrapFS \(3\) group on page G-70](#) and [Table G-31 stdExMibEvent \(8\) group on page G-78](#) summarize the groups of MIB objects used in SNMP traps.

Table G-30 stdExMibQuotaTrapFS (3) group

ID	Object name	Type	Meaning
1	quotaTrapFSSoftLimitTable (1)	-	Information about traps that exceeded the soft limit
1.1	quotaSoftLimitEntry (1)	-	Details about traps that exceeded the soft limit
1.1.1	quotaSoftLimitTrapDate (1)	DisplayString	Time of trap occurrence
1.1.2	quotaSoftLimitCHAName (2)	DisplayString	Node host name
1.1.3	quotaSoftLimitCHANumber (3)	DisplayString	Node number
1.1.4	quotaSoftLimitRaidNumber (4)	DisplayString	Device ID
1.1.5	quotaSoftLimitFSMntPoint (5)	DisplayString	File system name
1.1.6	quotaSoftLimitType (6)	INTEGER	Difference between user quotas and group quotas Each value represents the following: 1: user, 2: group
1.1.7	quotaSoftLimitName (7)	DisplayString	User name or group name
1.1.8	quotaSoftLimitID (8)	Integer32	UID or GID
1.1.9	quotaSoftLimitClass (9)	INTEGER	Excess type (blocks or inodes) Each value represents the following: 1: block, 2: inode
1.1.10	quotaSoftLimitUsed (10)	Counter64	Current usage (if the excess type is blocks, the unit is KB)

ID	Object name	Type	Meaning
1.1.11	quotaSoftLimitSoftLimitValue (11)	Counter64	Soft limit (if the excess type is blocks, the unit is KB)
1.1.12	quotaSoftLimitHardLimitValue (12)	Counter64	Hard limit (if the excess type is blocks, the unit is KB)
1.1.13	quotaSoftLimitRemainGracePeriod (13)	Counter32	Time (seconds) remaining for the grace period
2	quotaTrapFSLimitExceeded (2)	-	Information about traps that exceeded the grace period
2.1	quotaLimitExceededEntry (1)	-	Details about traps that exceeded the grace period
2.1.1	quotaLimitExceededTrapDate (1)	DisplayString	Time of trap occurrence
2.1.2	quotaLimitExceededCHAName (2)	DisplayString	Node host name
2.1.3	quotaLimitExceededCHANumber (3)	DisplayString	Node number
2.1.4	quotaLimitExceededRaidNumber (4)	DisplayString	Device ID
2.1.5	quotaLimitExceededFSMountPoint (5)	DisplayString	File system name
2.1.6	quotaLimitExceededType (6)	INTEGER	Difference between user quotas and group quotas Each value represents the following: 1: user, 2: group
2.1.7	quotaLimitExceededName (7)	DisplayString	User name or group name
2.1.8	quotaLimitExceededID (8)	Integer32	UID or GID
2.1.9	quotaLimitExceededClass (9)	INTEGER	Excess type (blocks or inodes) Each value represents the following: 1: block, 2: inode
2.1.10	quotaLimitExceededUsed (10)	Counter64	Current usage (if the excess type is blocks, the unit is KB)
2.1.11	quotaLimitExceededSoftLimitValue (11)	Counter64	Soft limit (if the excess type is blocks, the unit is KB)
2.1.12	quotaLimitExceededHardLimitValue (12)	Counter64	Hard limit (if the excess type is blocks, the unit is KB)
2.1.13	quotaLimitExceededGracePeriodValue (13)	Counter32	Set value (days) for the grace period
3	quotaTrapFSSummary (3)	-	Information in the summary trap for quotas

ID	Object name	Type	Meaning
3.1	quotaSummaryEntry (1)	-	Details in the summary trap for quotas
3.1.1	quotaSummaryTrapDate (1)	DisplayString	Time when trap occurred
3.1.2	quotaSummaryCHAName (2)	DisplayString	Node host name
3.1.3	quotaSummaryCHANumber (3)	DisplayString	Node number
3.1.4	quotaSummaryRaidNumber (4)	DisplayString	Device ID
3.1.5	quotaSummaryFSMntPoint (5)	DisplayString	File system name
3.1.6	quotaSummaryBlockSoftLimitExceedingUsers (6)	Integer32	Number of users who exceed their block soft limit
3.1.7	quotaSummaryBlockSoftLimitExceedingGroups (7)	INTEGER	Number of groups that exceed their block soft limit
3.1.8	quotaSummaryBlockGracePeriodExpiredUsers (8)	INTEGER	Number of users whose block grace period has expired
3.1.9	quotaSummaryBlockGracePeriodExpiredGroups (9)	INTEGER	Number of groups whose block grace period has expired
3.1.10	quotaSummaryFileSoftLimitExceedingUsers (10)	INTEGER	Number of users who exceed their file soft limit
3.1.11	quotaSummaryFileSoftLimitExceedingGroups (11)	INTEGER	Number of groups that exceed their file soft limit
3.1.12	quotaSummaryFileGracePeriodExpiredUser (12)	INTEGER	Number of users whose file grace period has expired
3.1.13	quotaSummaryFileGracePeriodExpiredGroups (13)	INTEGER	Number of groups whose file grace period has expired
4	quotaTrapFSDetailSuppress (4)	-	Information in the trap for quotas when individual reports are suppressed
4.1	quotaDetailSuppressEntry (1)	-	Details in the trap for quotas when individual reports are suppressed
4.1.1	quotaDetailSuppressTrapDate (1)	DisplayString	Time when trap occurred
4.1.2	quotaDetailSuppressCHAName (2)	DisplayString	Node host name
4.1.3	quotaDetailSuppressCHANumber (3)	DisplayString	Node number
4.1.4	quotaDetailSuppressRaidNumber (4)	DisplayString	Device ID

ID	Object name	Type	Meaning
4.1.5	quotaDetailSuppressFSMnt Point (5)	DisplayString	File system name
4.1.6	quotaDetailSuppressType (6)	INTEGER	Difference between user quotas and group quotas Each value represents the following: 1: user, 2: group
4.1.7	quotaDetailSuppressBlock SoftLimitExceeding (7)	INTEGER	Number of users or groups that exceed their block soft limit
4.1.8	quotaDetailSuppressBlock GracePeriodExpired (8)	INTEGER	Number of users or groups whose block grace period has expired
4.1.9	quotaDetailSuppressFileSoftLimitExceeding (9)	INTEGER	Number of users or groups that exceed their file soft limit
4.1.10	quotaDetailSuppressFileGracePeriodExpired (10)	INTEGER	Number of users or groups whose file grace period has expired
5	quotaTrapFSSubtreeSoftLimitTable (5)	-	Information about traps that exceeded the soft limit for monitoring subtree quotas
5.1	quotaSubtreeSoftLimitEntry (1)	-	Details about traps that exceeded the soft limit for monitoring subtree quotas
5.1.1	quotaSubtreeSoftLimitTrapDate (1)	DisplayString	Time of trap occurrence
5.1.2	quotaSubtreeSoftLimitCHAName (2)	DisplayString	Node host name
5.1.3	quotaSubtreeSoftLimitCHANumber (3)	DisplayString	Node number
5.1.4	quotaSubtreeSoftLimitRaidNumber (4)	DisplayString	Device ID
5.1.5	quotaSubtreeSoftLimitFSDirectoryName (5)	DisplayString	File system name/directory name
5.1.6	quotaSubtreeSoftLimitType (6)	INTEGER	Quota type: Subtree quota Each value represents the following: 2: subtree
5.1.7	quotaSubtreeSoftLimitName (7)	DisplayString	NULL
5.1.8	quotaSubtreeSoftLimitID (8)	Integer32	-1
5.1.9	quotaSubtreeSoftLimitClasses (9)	INTEGER	Excess type (blocks or inodes) Each value represents the following: 1: block, 2: inode

ID	Object name	Type	Meaning
5.1.10	quotaSubtreeSoftLimitUsed (10)	Counter64	Current usage (if the excess type is blocks, the unit is KB)
5.1.11	quotaSubtreeSoftLimitSoftLimitValue (11)	Counter64	Soft limit (if the excess type is blocks, the unit is KB)
5.1.12	quotaSubtreeSoftLimitHardLimitValue (12)	Counter64	Hard limit (if the excess type is blocks, the unit is KB)
5.1.13	quotaSubtreeSoftLimitRemainGracePeriod (13)	Counter32	Time (seconds) remaining for the grace period
6	quotaTrapFSSubtreeLimitExceeded (6)	-	Information about traps that exceeded the grace period for monitoring subtree quotas
6.1	quotaSubtreeLimitExceededEntry (1)	-	Details about traps that exceeded the grace period for monitoring subtree quotas
6.1.1	quotaSubtreeLimitExceededTrapDate (1)	DisplayString	Time of trap occurrence
6.1.2	quotaSubtreeLimitExceededCHAName (2)	DisplayString	Node host name
6.1.3	quotaSubtreeLimitExceededCHANumber (3)	DisplayString	Node number
6.1.4	quotaSubtreeLimitExceededRaidNumber (4)	DisplayString	Device ID
6.1.5	quotaSubtreeLimitExceededFSDirName (5)	DisplayString	File system name/directory name
6.1.6	quotaSubtreeLimitExceededType (6)	INTEGER	Quota type: Subtree quota Each value represents the following: 2: subtree
6.1.7	quotaSubtreeLimitExceededName (7)	DisplayString	NULL
6.1.8	quotaSubtreeLimitExceededID (8)	Integer32	-1
6.1.9	quotaSubtreeLimitExceededClass (9)	INTEGER	Excess type (blocks or inodes) Each value represents the following: 1: block, 2: inode
6.1.10	quotaSubtreeLimitExceededUsed (10)	Counter64	Current usage (if the excess type is blocks, the unit is KB)
6.1.11	quotaSubtreeLimitExceededSoftLimitValue (11)	Counter64	Soft limit (if the excess type is blocks, the unit is KB)
6.1.12	quotaSubtreeLimitExceededHardLimitValue (12)	Counter64	Hard limit (if the excess type is blocks, the unit is KB)

ID	Object name	Type	Meaning
6.1.13	quotaSubtreeLimitExceededGracePeriodValue (13)	Counter32	Set value (days) for the grace period
7	quotaTrapFSSubtreeSummary (7)	-	Information in the summary trap for subtree quotas
7.1	quotaSubtreeSummaryEntry (1)	-	Details in the summary trap for subtree quotas
7.1.1	quotaSubtreeSummaryTrapDate (1)	DisplayString	Time when trap occurred
7.1.2	quotaSubtreeSummaryCHAName (2)	DisplayString	Node host name
7.1.3	quotaSubtreeSummaryCHANumber (3)	DisplayString	Node number
7.1.4	quotaSubtreeSummaryRaidNumber (4)	DisplayString	Device ID
7.1.5	quotaSubtreeSummaryFSDirName (5)	DisplayString	File system name or file system name/directory name
7.1.6	quotaSubtreeSummaryType (6)	INTEGER	Summary type: Subtree quota or subtree user group quota Each value represents the following: 2: subtree, 5: subtree-user-group
7.1.7	quotaSubtreeSummaryBlockSoftLimitExceedingUsers (7)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of users who exceed their soft limit for the number of blocks.
7.1.8	quotaSubtreeSummaryBlockSoftLimitExceedingGroups (8)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of groups that exceed their soft limit for the number of blocks.
7.1.9	quotaSubtreeSummaryBlockSoftLimitExceedingDirectories (9)	INTEGER	If the summary type is subtree quota, this value is the number of directories that exceed their soft limit for the number of blocks. If the summary type is subtree user group quota, this value is -1.
7.1.10	quotaSubtreeSummaryBlockGracePeriodExpiredUsers (10)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the

ID	Object name	Type	Meaning
			number of users whose grace period for the number of blocks has expired.
7.1.11	quotaSubtreeSummaryBlockGracePeriodExpiredGroups (11)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of groups whose grace period for the number of blocks has expired.
7.1.12	quotaSubtreeSummaryBlockGracePeriodExpiredDirectories (12)	INTEGER	If the summary type is subtree quota, this value is the number of directories whose grace period for the number of blocks has expired. If the summary type is subtree user group quota, this value is -1.
7.1.13	quotaSubtreeSummaryFileSoftLimitExceedingUsers (13)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of users who exceed their soft limit for the number of inodes.
7.1.14	quotaSubtreeSummaryFileSoftLimitExceedingGroups (14)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of groups that exceed their soft limit for the number of inodes.
7.1.15	quotaSubtreeSummaryFileSoftLimitExceedingDirectories (15)	INTEGER	If the summary type is subtree quota, this value is the number of directories that exceed their soft limit for the number of inodes. If the summary type is subtree user group quota, this value is -1.
7.1.16	quotaSubtreeSummaryFileGracePeriodExpiredUsers (16)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of users whose grace period for the number of inodes has expired.
7.1.17	quotaSubtreeSummaryFileGracePeriodExpiredGroups (17)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of groups whose grace

ID	Object name	Type	Meaning
			period for the number of inodes has expired.
7.1.18	quotaSubtreeSummaryFileGracePeriodExpiredDirectories (18)	INTEGER	If the summary type is subtree quota, this value is the number of directories whose grace period for the number of inodes has expired. If the summary type is subtree user group quota, this value is -1.
8	quotaTrapFSSubtreeDetailSuppress (8)	-	Information in the trap for subtree quotas when individual reports are suppressed
8.1	quotaSubtreeDetailSuppressEntry (1)	-	Details in the trap for subtree quotas when individual reports are suppressed
8.1.1	quotaSubtreeDetailSuppressTrapDate (1)	DisplayString	Time when trap occurred
8.1.2	quotaSubtreeDetailSuppressCHAName (2)	DisplayString	Node host name
8.1.3	quotaSubtreeDetailSuppressCHANumber (3)	DisplayString	Node number
8.1.4	quotaSubtreeDetailSuppressRaidNumber (4)	DisplayString	Device ID
8.1.5	quotaSubtreeDetailSuppressFSDirName (5)	DisplayString	File system name/directory name
8.1.6	quotaSubtreeDetailSuppressType (6)	INTEGER	Quota type: Subtree quota Each value represents the following: 2: subtree
8.1.7	quotaSubtreeDetailSuppressBlockSoftLimitExceeding (7)	INTEGER	Number of directories that exceed their soft limit for the number of blocks
8.1.8	quotaSubtreeDetailSuppressBlockGracePeriodExpired (8)	INTEGER	Number of directories whose grace period for the number of blocks has expired
8.1.9	quotaSubtreeDetailSuppressFileSoftLimitExceeding (9)	INTEGER	Number of directories that exceed their soft limit for the number of inodes
8.1.10	quotaSubtreeDetailSuppressFileGracePeriodExpired (10)	INTEGER	Number of directories whose grace period for the number of inodes has expired
For details about how to use subtree quotas, see the <i>CLI Administrator's Guide</i> .			

Table G-31 stdExMibEvent (8) group

ID	Object name	Type	Meaning
1	stdExMibEventTrap (1)	-	Information about event notification traps
1.1	eventTrapEntry (1)	-	Details about event notification traps
1.1.1	eventTrapDate (1)	DisplayString	Time of trap occurrence
1.1.2	eventTrapGenDate (2)	DisplayString	Time of event occurrence
1.1.3	eventTrapCHAName (3)	DisplayString	Node host name
1.1.4	eventTrapCHANumber (4)	DisplayString	Node number
1.1.5	eventRaidNumber (5)	DisplayString	Device ID
1.1.6	eventTrapProcessID (6)	Integer32	Process ID
1.1.7	eventTrapProcessName (7)	DisplayString	Process name
1.1.8	eventTrapMsgID (8)	DisplayString	Message ID
1.1.9	eventTrapMsg (9)	OCTET STRING	Event message
1.1.10	eventTrapImportanceDeg (10)	Counter32	Importance level
1.1.11	eventTrapSameCount (11)	Counter32	The number of times that the same event occurred
1.1.12	eventTrapFinalGenerationDate (12)	DisplayString	Time of last occurrence
1.1.13	eventTrapThreadFlag (13)	INTEGER	Event flag
1.2	eventTrapOption (2)	-	Additional event information trap
1.2.1	eventTrapOptionFSName (1)	DisplayString	File system name
1.2.2	eventTrapOptionMntPoint (2)	DisplayString	Mount point
1.2.3	eventTrapOptionFileCount (3)	Counter64	Number of files (inodes)
1.2.4	eventTrapOptionFileWarnThld (4)	Counter64	Warning threshold (number of inodes)
1.2.5	eventTrapOptionAvail (5)	Counter64	Unused capacity (KB)
1.2.6	eventTrapOptionAvailWarnThld (6)	Counter64	Warning threshold (KB)
1.2.7	eventTrapOptionFunction (7)	DisplayString	Function name
2	stdExMibCoreTrap (2)	-	Information about core notification traps
2.1	coreTrapEntry (1)	-	Details about core notification traps
2.1.1	coreTrapTrapDate (1)	DisplayString	Time of trap occurrence
2.1.2	coreTrapCHAName (2)	DisplayString	Node host name

ID	Object name	Type	Meaning
2.1.3	coreTrapCHANumber (3)	DisplayString	Node number
2.1.4	coreTrapRaidNumber (4)	DisplayString	Device ID
2.1.5	coreTrapGenerationDate (5)	DisplayString	Time of occurrence
2.1.6	coreTrapDirectoryFileName (6)	DisplayString	Directory name or file name
2.1.7	coreTrapSize (7)	Integer32	Size (bytes)
2.1.8	coreTrapSystemDiskFreeSpace (8)	INTEGER	Free space (MB) on the system disk
2.1.9	coreTrapSystemDiskUse (9)	INTEGER	Usage rate (%) of the system disk

There are 4 values (Information, Warning, Error, and Fatal Error) for the severity level (eventTrapImportanceDeg (10)) for the SNMP trap event that is sent by the MIB object for stdExMibEventTrap (1).

The following table shows the meanings and values for eventTrapImportanceDeg (10).

Table G-32 Severity level for the 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 *Error Codes* manual, and then take appropriate action.

Also, for details about messages sent to the SNMP manager by SNMP trapping, see the *Error Codes* manual.



Acronyms

This appendix lists the acronyms used in the HDI manuals.

- [Acronyms used in the HDI manuals](#)

Acronyms used in the HDI manuals

The following acronyms are used in the HDI manuals.

ABE	Access Based Enumeration
ACE	access control entry
ACL	access control list
AES	Advanced Encryption Standard
AJP	Apache JServ Protocol
API	application programming interface
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
BDC	Backup Domain Controller
BMC	baseboard management controller
CA	certificate authority
CHA	channel adapter
CHAP	Challenge-Handshake Authentication Protocol
CIFS	Common Internet File System
CIM	Common Information Model
CLI	command line interface
CPU	central processing unit
CSR	certificate signing request
CSV	comma-separated values
CTL	controller
CU	control unit
CV	custom volume
DAACL	discretionary access control list
DAR	Direct Access Recovery
DB	database
DBMS	database management system
DC	domain controller
DDNS	Dynamic Domain Name System
DEP	data execution prevention
DES	Data Encryption Standard
DFS	distributed file system
DHCP	Dynamic Host Configuration Protocol

DIMM	dual in-line memory module
DLL	dynamic-link library
DN	distinguished name
DNS	Domain Name System
DOM	Document Object Model
DOS	Disk Operating System
DRAM	dynamic random access memory
DSA	digital signal algorithm
DTD	Document Type Definition
ECC	error-correcting code
EUC	Extended UNIX Code
FC	Fibre Channel
FC-SP	Fibre Channel - Security Protocol
FIB	forwarding information base
FIFO	First In, First Out
FQDN	fully qualified domain name
FTP	File Transfer Protocol
FV	Fixed Volume
FXP	File Exchange Protocol
GbE	Gigabit Ethernet
GID	group identifier
GMT	Greenwich Mean Time
GPL	GNU General Public License
GUI	graphical user interface
HBA	host bus adapter
H-LUN	host logical unit number
HPFS	High Performance File System
HSSO	HiCommand single sign-on
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	input/output
ICAP	Internet Content Adaptation Protocol
ICMP	Internet Control Message Protocol
ID	identifier

IP	Internet Protocol
IP-SW	IP switch
JDK	Java Development Kit
JIS	Japanese Industrial Standards
JSP	JavaServer Pages
KDC	Key Distribution Center
LACP	Link Aggregation Control Protocol
LAN	local area network
LBA	logical block addressing
LCD	Local Configuration Datastore
LDAP	Lightweight Directory Access Protocol
LDEV	logical device
LDIF	LDAP Data Interchange Format
LDKC	logical disk controller
LED	light-emitting diode
LF	Line Feed
LTS	long term support
LU	logical unit
LUN	logical unit number
LUSE	logical unit size expansion
LVI	Logical Volume Image
LVM	Logical Volume Manager
MAC	Media Access Control
MD5	Message-Digest algorithm 5
MIB	management information base
MMC	Microsoft Management Console
MP	microprocessor
MSS	maximum segment size
MTU	maximum transmission unit
NAS	Network-Attached Storage
NAT	network address translation
NDMP	Network Data Management Protocol
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIC	network interface card

NIS	Network Information Service
NTFS	New Technology File System
NTP	Network Time Protocol
OID	object identifier
ORB	object request broker
OS	operating system
PAP	Password Authentication Protocol
PC	personal computer
PCI	Peripheral Component Interconnect
PDC	Primary Domain Controller
PDU	protocol data unit
PID	process identifier
POSIX	Portable Operating System Interface for UNIX
PP	program product
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
RAM	random access memory
RAS	Reliability Availability Serviceability
RCS	Revision Control System
RD	relational database
RFC	Request for Comments
RID	relative identifier
RPC	remote procedure call
RSA	Rivest, Shamir, and Adleman
SACL	system access control list
SAN	storage area network
SAS	Serial Attached SCSI
SATA	serial ATA
SAX	Simple API for XML
SCSI	Small Computer System Interface
SFTP	SSH File Transfer Protocol
SHA	secure hash algorithm
SID	security identifier
SJIS	Shift JIS
SLPR	Storage Logical Partition

SMB	Server Message Block
SMD5	Salted Message Digest 5
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SP	service pack
SSD	solid-state drive
SSH	Secure Shell
SSHA	Salted Secure Hash Algorithm
SSL	Secure Sockets Layer
SSO	single sign-on
SVGA	Super Video Graphics Array
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOS	type of service
TTL	time to live
UAC	User Account Control
UDP	User Datagram Protocol
UID	user identifier
UNC	Universal Naming Convention
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
UTF	UCS Transformation Format
VDEV	Virtual Device
VLAN	virtual LAN
VLL	Virtual LVI/LUN
WADL	Web Application Description Language
WAN	wide area network
WINS	Windows Internet Name Service
WORM	Write Once, Read Many
WS	workstation
WWN	World Wide Name

WWW	World Wide Web
XDR	External Data Representation
XFS	extended file system
XML	Extensible Markup Language



Glossary

This glossary explains the terms used in the HDI manuals.

A

ACE

An entry in an ACL. An ACE sets access permissions for directories and files for each user and group. ACE formats differ depending on the ACL type.

ACL

A list of all the ACEs for a particular directory or file. An ACL defines the access permissions for a particular directory or file.

ACL type

The type of file system or file that is supported by the ACL. The ACL types that can be used in HDI systems are the Advanced ACL type (compatible with NTFS ACL), and the Classic ACL type (compatible with POSIX ACL).

Anti-Virus Enabler

A program used to scan, in real time, for viruses in data shared with users by way of CIFS in an HDI system.

B

Backup Restore

A program used for backing up data in an HDI file system.

backup server

A server that manages backup and restore operations by using backup management software.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

C

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.

cluster management LU

An LU that is assigned to a node and stores settings information, such as cluster configuration information and file system information.

command device

A control device used to receive commands that control storage systems.

Configuration Manager

A program used to set up an HDI system and manage file system operations.

D

Data Control

One of the programs on a node OS.

data port

A node port that is used to connect to the front-end LAN.

device file

A user LU. For more information, see *user LU*.

Device Manager

A program that manages disk resources and the hardware configuration of storage systems in an integrated manner.

Dynamic Provisioning

A function that virtually allocates volumes of a given capacity to a host independent of the physical capacity of the storage system.

Dynamic Tiering

This storage system functionality automatically reallocates data based on I/O load.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

F

failback

The relocation of a failed-over resource group back to its original node in the cluster after an error has been recovered on the node or maintenance on the node is complete.

failover

The relocation of a resource group to the other node in a cluster when an error occurs on a node or when maintenance on a node is required. Failovers enable continuous operation of the services provided by an HDI system.

File Sharing

One of the programs on a node OS.

fixed IP address

An IP address set for a specific interface in a node.

front-end LAN

A LAN used by a client to access the data stored in a storage system.

H

HBase Storage Mgmt Common Service

The Web-container service for Hitachi Command Suite Common Component.

HBase Storage Mgmt Web Service

The Web-server service for Hitachi Command Suite Common Component.

Hitachi Command Suite Common Component

A component that provides functions, such as being able to log on to the GUI, outputting management server integrated logs, and Web services, common to all Hitachi File Services Manager and Hitachi Command Suite products.

Hitachi Content Platform (HCP)

A system used for managing and storing data for long periods of time. File system data created in an HDI system can be migrated to an HCP system.

Hitachi Data Ingestor (HDI)

A system that uses storage systems and nodes to provide a file-sharing service.

Hitachi File Services Manager

A program necessary for the system administrator to operate or manage an HDI system from a GUI.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

I

interface

A logical network interface assigned to a port.

L

LDEV

A unit of storage that is created by logically partitioning a storage area within a parity group of a storage system. Although referred to as an *LDEV* in File Services Manager, it is referred to as a *logical unit (LU)* in Hitachi AMS2000 or HUS100 series storage systems.

logical volume

An area created by using a volume manager to divide a volume group into one or more areas. In HDI systems, this area corresponds to a file system created by using the volume manager.

LU

An LDEV that is assigned to a port in a storage system.

LUN

A management number assigned to each LU in a storage system. Although referred to as an *LUN* in File Services Manager, it is referred to as an *H-LUN* in the Hitachi AMS2000 or HUS100 series storage systems.

LUN Expansion

Functionality for expanding the capacity of an LU by integrating multiple LUs into one.

LVM

A type of volume manager. For more information, see *volume manager*.

M

maintenance personnel

Hitachi engineers who maintain HDI systems.

management console

A computer used by the system administrator to operate File Services Manager.

management LAN

A LAN used by the system administrator to operate and manage an HDI system.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

management server

A computer on which Hitachi File Services Manager is installed. The management server can also be used as a management console.

media

Recording media, such as magnetic tape, for storing backed up data.

media server

A server that controls a tape device installed outside the storage system.

N**NFS**

A protocol that provides file-sharing services to UNIX users.

node

A device that is connected to a storage system and that is used as a file server. Two nodes make up a cluster.

O**OS disk**

A logical disk area in a node, that stores the OS and programs that run on the OS.

P**physical node**

A node that makes up part of a processing node.

Primary Server Base

A program that provides Web server functionality.

processing node

A logical group made up of nodes. If nodes are set up in a cluster, the cluster is treated as a processing node.

Q**quota**

The maximum block space and maximum number of inodes available to a user. In an HDI system, limits can be set and managed for each file system or each directory.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

R

resource group

A management unit used to manage multiple resources (such as NFS share settings, CIFS share settings, file system information, and virtual IP address information) as a group. Services can be started and stopped for each resource group. If an error occurs, failover is performed for each resource group.

S

scan server

A server that scans, by way of a LAN, CIFS-shared data in an HDI system for viruses.

subtree quota

Subtree quotas are used to control the amount of block usage and inode usage for each directory. Subtree quotas can also be set for users and groups.

system administrator

A user who manages an HDI system. The system administrator sets up an HDI system and monitors system operations and error information.

system LU

A collective term for the OS disks and the cluster management LU.

T

tape device

A device for storing multiple types of storage media.

target

A unit used to manage multiple LUs as one group so that a node can uniquely recognize the LUs of a storage system.

trunking

A technology used to create a virtual network interface from a group of ports. HDI allows you to configure a network by using virtual network interfaces that are assembled by using trunking.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

U

user LU

A generic term for an LU that is assigned to a node and that stores user data such as file system information. A user LU is also called a *device file* or an *LU* (excluding the system LU).

user LUN

A management number assigned to each user LU. A user LUN is also called a *device file number*.

user mapping

The process of assigning a user ID and group ID to a user registered in a domain controller when the user accesses a CIFS share.

V

virtual IP address

An IP address used by a user when connecting to a service running on a resource group. By using a virtual IP address, the user can continue to use the service even if an error occurs on a node and the resource group fails over to the other properly-running node.

volume group

An area that consists of one or more LUs that have been grouped together by a volume manager. A volume group is made up of one file system.

volume manager

Functionality for volume management. In the HDI system, LVM is used as the volume manager. This functionality enables you to create volume groups combining LUs and to create logical volumes out of volume groups.

W

WORM

An abbreviation for "Write Once, Read Many". The WORM status indicates that data cannot be modified. A file whose status is changed to the WORM status is called a WORM file, and a file system in which any files can be changed to a WORM file is called a WORM file system.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	---	-------------------	---	-------------------	-------------------	---	---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	---	---	---

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

Index

A

- access
 - CIFS client logs 4-10
 - setting up environment for CIFS client 4-2
 - setting up environment for NFS client 4-12
- Access Protocol Configuration dialog box C-217
- account
 - adding 2-2
 - changing password 2-2
- Account Lock dialog box C-312
- Account Lock window C-311
- Activate License dialog box C-293
- Active Directory
 - joining domain 4-2
 - rejoining domain 4-5
- Add Processing Node dialog box C-82
- Add Share dialog box C-38
- Add User dialog box C-300
- adding
 - account 2-2
 - LU path 12-3
 - routing information 9-4
- application window C-307

B

- backing up
 - system configuration manually 8-2
 - system configuration regularly 8-2
 - tape device 7-2
- Backup Configuration dialog box C-171
- built-in account 1-2

C

- capacity
 - expanding file system 6-2
 - limiting file share usage 6-2
 - limiting group usage 6-3
 - limiting user usage 6-3
- cascaded trunking 9-9
- Change Authentication Method dialog box C-301
- Change Password dialog box C-304
- Change Permission dialog box C-305
- Change Share Quota dialog box C-19
- changing
 - account password 2-2
 - LU path 12-3
 - negotiation mode 9-5
 - node host name 9-3
 - node IP address 9-2
 - policy for migrating data to HCP 3-4
 - port assigned to LU 12-2
 - schedule for migrating data to HCP 3-4
- Check for Errors dialog box C-163
- Cluster Management dialog box C-268
- combining link aggregation and link alternation 9-9
- command, setting up environment 13-2
- Configuration Wizard C-317
- Configure Proxy Server dialog box C-282
- configuring workgroup 4-7
- confirmation dialog box B-10
- connecting additional storage system 12-7
- Create and Share File System dialog box C-103
- Create File System dialog box C-126
- creating shared directory 3-2

- D**
- data, showing on HCP 5-2
 - deleting
 - LU path 12-3
 - routing information 9-4
 - detaching storage system 12-9
 - dialog box
 - confirmation B-9
 - operation B-7
 - results B-11
- E**
- Edit File System dialog box C-44
 - Edit HDvM Settings dialog box C-335
 - Edit Message dialog box C-314
 - Edit Node dialog box C-85
 - Edit Profile dialog box C-303
 - Edit Quota dialog box C-55
 - Edit Share dialog box C-7
 - end user
 - GUI operation D-1
 - error email notifications 10-7
 - Expand File System dialog box C-52
 - expanding file system capacity 6-2
- F**
- FC path, reconfiguring 12-5
 - file server, import from 3-5
 - file system, expanding 6-2
 - File Systems window C-33
 - file-system window C-62
 - Filter dialog box B-7
- G**
- groups of MIB objects G-3
 - GUI
 - confirmation B-10
 - Hitachi File Services Manager main window B-4
 - Filter B-7
 - notes B-2
 - operation by end user D-1
 - results (when operation ends in an error) B-11
 - results (when operation ends normally) B-11
- H**
- HCP
 - changing migration policy 3-4
 - changing migration schedule 3-4
 - showing previous data 5-2
 - HCP-name window C-294
 - HDvM Connection Management dialog box C-334
 - Health Monitor window C-137
 - host name, changing for node 9-3
- I**
- identifying users by user mapping 4-8
 - import
 - file server 3-5
 - improving GUI operation for large system 4-12
 - IP address, changing for node 9-2
- J**
- joining
 - Active Directory domain 4-2
 - NT domain 4-5
- L**
- limiting
 - capacity used by file share 6-2
 - capacity used by group 6-3
 - capacity used by user 6-3
 - link aggregation 9-8
 - combining with link alternation 9-9
 - link alternation 9-8
 - combining with link aggregation 9-9
 - performing manually 9-10
 - Local Users dialog box C-150
 - logging on 1-2
 - LU
 - changing port 12-2
 - reconfiguring path 12-3
- M**
- MIB object G-1
 - responding to SNMP get request G-3
 - used for SNMP trap G-69
 - migration

- changing policy 3-4
- changing schedule 3-4
- Migration Tasks dialog box C-336
- Mount File System dialog box C-54

N

- negotiation mode, changing 9-5
- Network & System Configuration dialog box C-178
- NT domain, joining 4-5

O

- operation, improving for large system 4-12

P

- Password dialog box C-310
- Password window C-309
- Permissions window C-306
- physical-node window C-91
- policy, changing for migrating data to HCP 3-4
- port, changing assigned to LU 12-2
- Processing Nodes window C-78
- processing-node window C-86
- Proxy Server Settings window C-281

R

- reconfiguring
 - FC path 12-5
 - LU path 12-3
- reference
 - Other HDI data 3-3
- rejoining Active Directory domain 4-5
- replacing switch 12-7
- reserved words F-1
- restoring data from tape device 7-4
- results dialog box (when operation ends in an error) B-11
- results dialog box (when operation ends normally) B-11
- RID 4-9
- routing information
 - adding 9-4
 - deleting 9-4

S

- schedule, changing for migrating data to HCP 3-4
- Security window C-308
- setting
 - link aggregation 9-8
 - link alternation 9-8
- setting up
 - access environment from CIFS client 4-2
 - access environment from NFS client 4-12
 - environment for command 13-2
 - link configuration 9-8
 - public key certificate 13-2
 - virus scanning 7-2
 - VLAN 9-10
- share window C-21
- shared directory, creating 3-2
- Shares window C-5
- showing
 - previous data on HCP 5-2
- SNMPv2
 - using 10-2
- SNMPv3
 - using 10-3
- software
 - updating 14-3
- storage system
 - connecting additional 12-7
 - detaching 12-9
- storage-system-name window C-295
- structure for standard MIB objects G-2
- window B-6
- switch, replacing 12-7
- system configuration
 - backing up manually 8-2
 - backing up regularly 8-2
- System Software Installation Wizard C-148
- System Software window C-147

T

- tape device
 - backing up data 7-2
 - restoring data 7-4

U

- updating

- software 14-3
- user mapping 4-8
- User Profile window C-316
- user-ID window C-302
- Users and Permissions window C-296
- Users window C-297
- using
 - SNMPv2 10-2
 - SNMPv3 10-3

V

- Virus Scan Server Configuration dialog box C-283
- virus scanning setup 7-2
- VLAN ID 9-10
- VLAN setup 9-10

W

- Warning Banner window C-313
- workgroup, configuring 4-7

Hitachi Data Systems

Corporate Headquarters

2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.

www.hds.com

Regional Contact Information

Americas

+1 408 970 1000

info@hds.com

Europe, Middle East, and Africa

+44 (0)1753 618000

info.emea@hds.com

Asia Pacific

+852 3189 7900

hds.marketing.apac@hds.com



MK-90HDI038-18