Hitachi Data Ingestor

6.4.5-01

CLI Administrator's Guide

This manual describes the command syntax used in Hitachi Data Ingestor (HDI) system.
The purpose of this manual is to enable readers to understand command operations, and to run and manage an HDI system.

Contents

ix

Preface

This manual describes the command syntax used in Hitachi Data Ingestor (HDI) system.

The purpose of this manual is to enable readers to understand command operations, and to run and manage an HDI system.

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

☐ Accessing product documentation

☐ Getting help

☐ Comments

Intended audience

This manual is intended for system administrators who wish to run and manage an HDI system using commands.

Readers of this manual 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

Product version

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

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on Hitachi Vantara Support Connect: https://knowledge.hitachivantara.com/Documents.

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 name	Description
Hitachi Data Ingestor Installation and Configuration Guide, MK-90HDICOM002	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, as well as the environment settings for an external server.

Manual name	Description
Hitachi Data Ingestor Cluster Getting Started Guide, MK-90HDICOM001	This manual explains how to set up an HDI system in a cluster configuration.
Hitachi Data Ingestor Cluster Administrator's Guide, MK-90HDI038	This manual provides procedures for using HDI systems in a cluster configuration, as well as provides GUI references.
Hitachi Data Ingestor Cluster Troubleshooting Guide, MK-90HDI029	This manual provides troubleshooting information for HDI systems in a cluster configuration.
Hitachi Data Ingestor Single Node Getting Started Guide, MK-90HDI028	This manual explains how to set up an HDI system in a single-node configuration.
Hitachi Data Ingestor Single Node Administrator's Guide, MK-90HDI039	This manual explains the procedures for using HDI systems in a single-node configuration, as well as provides GUI references.
Hitachi Data Ingestor Single Node Troubleshooting Guide, MK-90HDI030	This manual provides troubleshooting information for HDI systems in a single-node configuration.
Hitachi Data Ingestor CLI Administrator's Guide (This manual)	This manual describes the syntax of the commands that can be used for HDI systems in a cluster configuration or a single-node configuration.
Hitachi Data Ingestor API References, MK-90HDI026	This manual explains how to use the API for HDI systems in a cluster configuration or a single-node configuration.
Hitachi Data Ingestor Error Codes, MK-90HDI005	This manual contains messages for HDI systems in a cluster configuration or a single-node configuration.
Hitachi Data Ingestor File System Protocols (CIFS/ NFS) Administrator's Guide, MK-90HDI035	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.

Referenced documents

Hitachi Virtual Storage Platform G1000

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

Hitachi Virtual Storage Platform Fx00 models

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

Hitachi Virtual Storage Platform Gx00 models

- *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 AMS2000 series

- *Hitachi Data Ingestor Array Features Administrator's Guide for Hitachi AMS2000/HUS100 series*

Abbreviation conventions

This manual uses the following abbreviations for product names:

Abbreviation	Full name or meaning
Active Directory	Active Directory(R)
Dynamic Provisioning	Hitachi Dynamic Provisioning
Dynamic Tiering	Hitachi Dynamic Tiering
File Services Manager	A generic name for the following: • 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: • Hitachi Unified Storage 150 • Hitachi Unified Storage 130 • Hitachi Unified Storage 110

Abbreviation	Full name or meaning
HUS VM	Hitachi Unified Storage VM
ShadowImage	A generic name for the following: • ShadowImage • ShadowImage in-system replication
TrueCopy	A generic name for the following: • TrueCopy • TrueCopy Asynchronous • TrueCopy Extended Distance • TrueCopy remote replication
Universal Storage Platform V/VM	A generic name for the following: • Hitachi Universal Storage Platform V • Hitachi Universal Storage Platform VM
Virtual Storage Platform	Hitachi Virtual Storage Platform
VSP Fx00 models	A generic name for the following: • Hitachi Virtual Storage Platform F350 • Hitachi Virtual Storage Platform F370 • Hitachi Virtual Storage Platform F400 • Hitachi Virtual Storage Platform F600 • Hitachi Virtual Storage Platform F700 • Hitachi Virtual Storage Platform F800 • Hitachi Virtual Storage Platform F900
VSP G1000	Hitachi Virtual Storage Platform G1000
VSP Gx00 models	A generic name for the following: • Hitachi Virtual Storage Platform G200 • Hitachi Virtual Storage Platform G350 • Hitachi Virtual Storage Platform G370 • Hitachi Virtual Storage Platform G400 • Hitachi Virtual Storage Platform G600 • Hitachi Virtual Storage Platform G700 • Hitachi Virtual Storage Platform G800 • Hitachi Virtual Storage Platform G900
Windows	Microsoft(R) Windows(R) Operating System
Windows 7	A generic name for the following: • Microsoft(R) Windows(R) 7 Professional • Microsoft(R) Windows(R) 7 Professional x64 Edition • Microsoft(R) Windows(R) 7 Ultimate

If you want to reference other manuals, note that hereinafter in this manual, the *Hitachi Data Ingestor Cluster Administrator's Guide* and *Hitachi Data Ingestor Single Node Administrator's Guide* are referred to as the

Administrator's Guide, and the *Hitachi Data Ingestor Cluster Troubleshooting Guide* and the *Hitachi Data Ingestor Single Node Troubleshooting Guide* are referred to as the *Troubleshooting Guide*. See the appropriate manual as needed.

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**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `copy` *source-file target-file* *Note:* Angled brackets (< >) are also used to indicate variables.
`screen/code`	Indicates text that is displayed on screen or entered by the user. Example: `# pairdisplay -g oradb`
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `# pairdisplay -g <group>` *Note:* Italic font is also used to indicate variables.
[ ] 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. Example: `{[A] [B]}` indicates that you must specify either A or B, or both.
| 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.
<u>underline</u>	Indicates the default value. Example: `[a	b]`
...	The item or items preceding the ellipsis (...) can be repeated. To specify multiple items, use a comma (,) to delimit them. Example: `A,B...` indicates that `B` can be specified as many times as necessary after `A`.

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
1 block	-	512 bytes

Accessing product documentation

Product user documentation is available on Hitachi Vantara Support Connect: https://knowledge.hitachivantara.com/Documents. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

Hitachi Vantara Support Connect is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for Hitachi Vantara 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.hitachivantara.com, register, and complete your profile.

Comments

Please send us your comments on this document to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara Corporation.

Thank you!

Preface

1

Before Using Commands

This chapter describes what a system administrator needs to know before using commands, including operations that can be performed by using commands, the prerequisites for using commands, how to execute commands, common options, return values, and cautionary notes on using commands.

☐ Operations that can be performed by using commands

☐ Commands that can be used depending on the system configuration

☐ Prerequisites for using commands

☐ Command execution

☐ Common options

☐ Notes on operations (required reading before using commands)

Operations that can be performed by using commands

A system administrator can use commands to operate or manage a Hitachi Data Ingestor (HDI) system. The following table describes the operations that can be performed by using commands:

Table 1-1 Operations that can be performed by using commands

Operation		Command	Reference	Procedure
Managing public keys used by SSH				
--	Viewing public key information	`sshkeylist`	sshkeylist (List public key information) on page 2-590	--
	Registering a public key[#]	`sshkeyadd`	sshkeyadd (Register a public key) on page 2-587	Registering a public key on page 3-3
	Deleting a public key[#]	`sshkeydel`	sshkeydel (Delete a public key) on page 2-589	--
Managing common keys used for local data encryption				
--	Displaying a key to be saved outside the system as a common key used for local data encryption	`encdisplaykey`	encdisplaykey (Display a key to be saved outside the system as a common key used for local data encryption) on page 2-304	--
	Restoring a common key used for local data encryption	`encrecoverkey`	encrecoverkey (Restore a common key used for local data encryption) on page 2-306	--
	Verifying a common key used for local data encryption	`encverifykey`	encverifykey (Verify a common key used for local data encryption) on page 2-307	--

Operation		Command	Reference	Procedure
Manage common key codes for encryption of data stored on an HCP system				
--	Display common key codes for encryption of data stored on an HCP system to save them outside of the system	hcpdisplaykey y	hcpdisplaykey (Displaying the common encryption key used for data stored on an HCP system to save the data outside of the system) on page 2-401	--
	Restore common key codes for encryption of data stored on an HCP system	hcprecoverke y	encrecoverke y (Restore a common key used for local data encryption) on page 2-306	--
	Verify common key codes for encryption of data stored on an HCP system	hcpverifykey	encverifykey (Verify a common key used for local data encryption) on page 2-307	--
Public key certificate-related settings				
--	Create a private key and a certificate signing request (CSR).	certctl	certctl (Public key certificate-related settings) on page 2-144	--
	Create the keystore	certctl	certctl (Public key certificate-related settings) on page 2-144	--
	Set up a public key certificate in a node.	certctl	certctl (Public key certificate-related settings) on page 2-144	--
	Initialize a public key certificate that is set up in a node.	certctl	certctl (Public key certificate-related	--

Operation		Command	Reference	Procedure
			settings) on page 2-144	
Changing the password of the management server				
--	Changing the password of the management server	`hnasmpasswd`	hnasmpasswd (Change the password of the management server) on page 2-411	Changing the password of the management server on page 3-4
Managing the security enhancement				
--	Enable the security enhancement	`secureshellc tl`	secureshellctl (Enable the security enhancement) on page 2-586	--
	Viewing the security enhancement settings	`secureshellc tl`	secureshellctl (Enable the security enhancement) on page 2-586	--
Managing a cluster				
--	Viewing the status of a cluster	`clstatus`	clstatus (Display cluster status) on page 2-232	--
	Stopping a cluster	`clstop`	clstop (Stop a cluster) on page 2-236	Stopping a cluster on page 3-5
	Starting a cluster	`clstart`	clstart (Start a cluster) on page 2-231	Starting a cluster on page 3-6
	Viewing the status of node(s)	`ndstatus`	ndstatus (Display node status) on page 2-496	--
	Stopping a node	`ndstop`	ndstop (Stop a node) on page 2-498	Stopping a node on page 3-7
	Starting a node	`ndstart`	ndstart (Start a node) on page 2-495	Starting a node on page 3-9
	Viewing the status of resource group(s)	`rgstatus`	rgstatus (Display resource group status)	--

Operation	Command	Reference	Procedure
		on page 2-568	
Stopping a resource group	rgstop	rgstop (Stop a resource group) on page 2-571	Stopping a resource group on page 3-9
Starting a resource group	rgstart	rgstart (Start a resource group) on page 2-566	Starting a resource group on page 3-10
Changing the executing node of a resource group	rgmove	rgmove (Change the execution node of a resource group) on page 2-565	Changing the execution node of a resource group on page 3-11
Disabling resource group monitoring	rgmon	rgmon (Disable and restart resource group monitoring) on page 2-563	Disabling resource group monitoring on page 3-13
Restarting resource group monitoring	rgmon	rgmon (Disable and restart resource group monitoring) on page 2-563	Restarting resource group monitoring on page 3-13
Managing failover-related timeout values	clctl	clctl (Set cluster processing values) on page 2-228	Changing failover-related timeout values on page 3-14
Controlling the OS on a node			
-- Stopping the OS on a node	nasshutdown	nasshutdown (Stop the OS on a node) on page 2-482	Stopping the OS on a node on page 3-15
Restarting the OS on a node	nasreboot	nasreboot (Restart the OS on a node) on page 2-480	Restarting the OS on a node on page 3-16

Operation		Command	Reference	Procedure
	Starting the OS on the other node in the cluster	`nasboot`	nasboot (Start the OS on the other node in the cluster) on page 2-473	Starting the OS on the other node in the cluster on page 3-16
	Emergency shutdown of the OS on a node	`emergencyshutdown`	emergencyshutdown (Emergency shutdown on a node) on page 2-303	--
Managing services				
--	Viewing the operating status of a service	`svstatus`	svstatus (Display the operating status of a service) on page 2-615	--
	Stopping a service#	`svctl`	svctl (Control a service) on page 2-611	Stopping a service on page 3-17
	Starting a service#	`svctl`	svctl (Control a service) on page 2-611	Starting a service on page 3-18
	Restarting a service#	`svctl`	svctl (Control a service) on page 2-611	Restarting a service on page 3-18
	Viewing the automatic startup settings for a service	`svstartuplist`	svstartuplist (Display automatic startup settings for a service) on page 2-612	--
	Switching the automatic startup settings for a service#	`svstartupset`	svstartupset (Switch the automatic startup settings for a service) on page 2-614	Switching the automatic startup settings for a service on page 3-19
	Viewing the FTP service configuration	`ftpget`	ftpget (Display the FTP service configuration) on page 2-391	--

Before Using Commands

Operation	Command	Reference	Procedure
Changing the FTP service configuration[#]	ftpset	ftpset (Change the FTP service configuration) on page 2-392	Changing the FTP service configuration on page 3-19
Viewing the TFTP service configuration	tftpget	tftpget (Display the TFTP service configuration) on page 2-647	--
Changing the TFTP service configuration[#]	tftpset	tftpset (Change the TFTP service configuration) on page 2-648	--
Viewing the file lock information for an NFS client host	nfslockslist	nfslockslist (List file lock information for an NFS client host) on page 2-526	--
Deleting the file lock information for an NFS client host[#]	nfslocksclear	nfslocksclear (Delete file lock information for an NFS client host) on page 2-525	--
Viewing the contents of the keytab file for Kerberos authentication	nfskeytablist	nfskeytablist (List the contents of the keytab file for Kerberos authentication) on page 2-520	--
Adding a keytab file for Kerberos authentication[#]	nfskeytabadd	nfskeytabadd (Add a keytab file for Kerberos authentication) on page 2-518	Adding a keytab file for Kerberos authentication on page 3-56
Deleting principal information from the keytab file for Kerberos authentication[#]	nfskeytabdel	nfskeytabdel (Delete principal information from the	--

Operation	Command	Reference	Procedure
		keytab file for Kerberos authentication) on page 2-519	
Flushing the NFS cache[#]	`nfscacheflush`	nfscacheflush (Flush NFS caches) on page 2-501	--
Viewing the NFS environment settings	`nfsoptlist`	nfsoptlist (Display the NFS environment settings) on page 2-529	--
Setting the NFS environment[#]	`nfsoptset`	nfsoptset (Set the NFS environment) on page 2-531	--
Viewing the NFS daemon information	`nfsstatus`	nfsstatus (Display NFS daemon information) on page 2-539	--
Viewing the port number allocation method for the NFS service	`nfssvget`	nfssvget (Display the port number allocation method for the NFS service) on page 2-540	--
Changing the port number allocation method for the NFS service[#]	`nfssvset`	nfssvset (Change the port number allocation method for the NFS service) on page 2-542	--
Viewing the directory used for saving the CIFS access log	`cifslogctl`	cifslogctl (Manage CIFS access log information) on page 2-197	--
Setting the directory used for saving the CIFS access log[#]	`cifslogctl`	cifslogctl (Manage CIFS access log information)	Setting the directory used for saving the CIFS access

Operation	Command	Reference	Procedure
Removing the setting for saving the CIFS access log into a directory[#]	cifslogctl		--
Saving the latest CIFS access log information[#]	cifslogctl		
Changing the settings for collecting the CIFS-service performance analysis log	cifsoptlist		--
Viewing the configuration definition for the CIFS service	cifsoptlist		--
Changing the configuration definition for the CIFS service[#]	cifsoptset		--
Changing the collection settings for the service performance statistics	perfmonctl		--
Viewing the collection settings for the service performance statistics	perfmonctl		--
System setup			

	Operation	Command	Reference	Procedure
--	Viewing interface information	`iflist`	iflist (List interface information) on page 2-453	--
	Adding an interface	`ifadd`	ifadd (Add an interface) on page 2-444	Adding an interface on page 3-22
	Changing an interface	`ifedit`	ifedit (Edit an interface) on page 2-449	Changing an interface on page 3-23
	Deleting an interface	`ifdel`	ifdel (Delete an interface) on page 2-447	--
	Viewing routing information	`routelist`	routelist (List routing information) on page 2-582	--
	Adding routing information	`routeadd`	routeadd (Add routing information) on page 2-574	Adding routing information on page 3-24
	Deleting routing information	`routedel`	routedel (Delete routing information) on page 2-577	--
	Changing the setting for reverse path filtering[#]	`routefilterctl`	routefilterctl (Set reverse path filtering) on page 2-580	Changing the setting for reverse path filtering on page 3-25
	Viewing the interface information for BMC ports	`bmcctl`	bmcctl (Manage BMC port interfaces) on page 2-136	--
	Editing BMC port interfaces	`bmcctl`	bmcctl (Manage BMC port interfaces) on page 2-136	Editing the interface information for BMC ports on page 3-25
	Viewing the interface information for private maintenance ports	`pmctl`	pmctl (Manage	--

Operation	Command	Reference	Procedure
		private maintenance port interfaces) on page 2-548	
Editing the interface information for private maintenance ports#	pmctl	pmctl (Manage private maintenance port interfaces) on page 2-548	Editing the interface information for private maintenance ports on page 3-26
Viewing the network settings	nasnetstat	nasnetstat (Display the network setting information) on page 2-475	Viewing the network settings on page 3-27
Checking the connection with a specified host	nasping	nasping (Display the connection to a specified host) on page 2-478	Checking the connection with a specified host on page 3-28
Viewing the path that leads to a specified host	nastraceroute	nastraceroute (Display the path that leads to the specified host) on page 2-483	Viewing the path that leads to a specified host on page 3-29
Checking that IP addresses and MAC addresses correspond	nasipneigh	nasipneigh (Check that IP addresses and MAC addresses correspond) on page 2-474	Checking the correspondence between IP addresses and MAC addresses on page 3-29
Deleting the logs generated at command execution	eraselog	eraselog (Delete the logs generated at command execution) on page 2-308	--
Viewing the status and configuration of an FC path	fpstatus	fpstatus (Display the status and configuration of an FC path)	--

Operation	Command	Reference	Procedure
		on page 2-316	
Switching the status of an FC path to `Online`[#]	`fponline`	fponline (Switch an FC path to Online) on page 2-314	Switching the status of an FC path to Online on page 3-30
Switching the status of an FC path to `Offline`[#]	`fpoffline`	fpoffline (Switch an FC path to Offline) on page 2-312	--
Changing the setting for automatic switching of an FC path status to `Online`[#]	`fpctl`	fpctl (Manage FC path settings) on page 2-309	Changing the setting for automatic switching of an FC path status to Online on page 3-31
Changing the setting for the load balancing function[#]	`fpctl`	fpctl (Manage FC path settings) on page 2-309	Changing the setting for the load balancing function on page 3-31
Viewing the information of user LUNs	`lumaplist`	lumaplist (Display the information of user LUNs) on page 2-468	--
Changing the setting for automatically assigning LDEV numbers to user LUNs	`lumapctl`	lumapctl (Manage the assignment of user LUNs) on page 2-464	Changing the setting for automatically assigning LDEV numbers to user LUNs on page 3-32
Assigning an LDEV number to a user LUN	`lumapadd`	lumapadd (Assign user LUNs) on page 2-463	Assigning an LDEV number to a user LUN on page 3-32
Deleting the assignment of a user LUN	`lumapdelete`	lumapdelete (Delete the assignment of user LUNs) on page 2-466	--

Before Using Commands

Operation	Command	Reference	Procedure
Viewing the time settings	timeget	timeget (Display the time settings) on page 2-650	--
Setting up an NTP server	timeset	timeset (Set the time settings) on page 2-651	Setting up an NTP server on page 3-33
Setting the node time[#]	timeset	timeset (Set the time settings) on page 2-651	Setting the node time on page 3-34
Changing the message displayed at login by using SSH	welcomemsgchange	welcomemsgchange (Change the message displayed at login by using SSH) on page 2-675	Changing the message displayed at login by using SSH on page 3-34
Adding virtual IP addresses	altipadd	altipadd (Add virtual IP addresses) on page 2-15	--
Deleting added virtual IP addresses	altipdel	altipdel (Delete added virtual IP addresses) on page 2-17	--
Viewing information about added virtual IP addresses	altiplist	altiplist (Display added virtual IP addresses) on page 2-19	--
Configuring the interface for when using DHCP	dhcpset	dhcpset (Setting the interface for when using DHCP) on page 2-273	--
Re-configuring the interface for when using DHCP	dhcpreload	dhcpreload (Reconfiguring the interface when using DHCP) on page 2-271	--
Viewing the DHCP status	dhcpget	dhcpget (Display the	--

Operation	Command	Reference	Procedure
		status of DHCP settings) on page 2-270	
Configuring UPnP	upnpctl	upnpctl (UPnP settings) on page 2-657	--
Outputting the system's operating information, and changing the settings related to the output of the system's operating information	sysinfoget	sysinfoget (Output the operating information of the system and specify settings related to output) on page 2-618	--
Managing the real-time scan function			
-- Registering the scan software to be used[#]	avascanengin eset	avascanengin eset (Select the scan software to be used) on page 2-124	Registering the scan software to be used on page 3-35
Registering scan server information[#]	avaserveradd	avaserveradd (Add scan server information) on page 2-126	Registering scan server information on page 3-36
Changing the scan server information[#]	avaserveredi t	avaserveredit (Change scan server information) on page 2-128	--
Deleting the scan server information[#]	avaserverdel	avaserverdel (Delete scan server information) on page 2-127	--
Setting a scan condition[#]	avaconfedit	avaconfedit (Set scan conditions) on page 2-115	Setting scan conditions on page 3-36
Setting extensions for the files to be scanned or the files not to be scanned[#]	avaextension sedit	avaextensions edit (Set extensions for the files to be	--

Operation		Command	Reference	Procedure
			scanned or the files not to be scanned) on page 2-122	
	Enabling the real-time scan service[#]	avaservicestart	avaservicestart (Enable the real-time scan service) on page 2-129	Enabling the real-time scan service on page 3-37
	Viewing the status of the real-time scan service	avaservicestatus	avaservicestatus (Display the status of the real-time scan service) on page 2-130	--
	Disabling the real-time scan service[#]	avaservicestop	avaservicestop (Disable the real-time scan service) on page 2-133	--
Managing local users and local groups				
--	Viewing user information	usrlist	usrlist (List user information) on page 2-664	--
	Registering a user	usradd	usradd (Add a user) on page 2-659	Registering a user on page 3-38
	Deleting a user	usrdel	usrdel (Delete a user) on page 2-663	--
	Batch-registering users	usradd	usradd (Add a user) on page 2-659	Batch-registering users on page 3-39
	Batch-deleting users	usrdel	usrdel (Delete a user) on page 2-663	--
	Viewing group information	grplist	grplist (List group information) on page 2-398	--
	Registering a group	grpadd	grpadd (Add a group) on page 2-393	Registering a group on page 3-40

Operation		Command	Reference	Procedure
	Deleting a group	`grpdel`	grpdel (Delete a group) on page 2-396	--
	Batch-registering groups	`grpadd`	grpadd (Add a group) on page 2-393	Batch-registering groups on page 3-41
	Batch-deleting groups	`grpdel`	grpdel (Delete a group) on page 2-396	--
Managing a file system				
--	Viewing file system information	`fslist`	fslist (List file system information) on page 2-372	--
	Creating a file system	`fscreate`	fscreate (Create a file system) on page 2-322	Creating a file system on page 3-42
	Mounting a file system	`fsmount`	fsmount (Mount a file system) on page 2-381	Mounting a file system on page 3-43
	Unmounting a file system	`fsumount`	fsumount (Unmount a file system) on page 2-390	Unmounting a file system on page 3-44
	Expanding a file system	`fsexpand`	fsexpand (Expand a file system) on page 2-356	Expanding a file system on page 3-45
	Deleting a file system	`fsdelete`	fsdelete (Delete a file system) on page 2-348	--
	Changing file system settings	`fsedit`	fsedit (Change the file system settings) on page 2-349	Changing file system settings on page 3-47
	Enabling the sending of warnings related to file system usage	`fsfullmsg` or `fsctl`	fsfullmsg (Manage the warning notification functionality for file system usage) on page 2-360 or	Enabling a warning notification related to file system usage on page 3-48

Operation	Command	Reference	Procedure
		fsctl (Manage an active file system) on page 2-335	
Enabling automatic failover that is performed when a file system is blocked	`fsautofo` or `fsctl`	fsautofo (Manage the automatic failover functionality used when a file system is blocked) on page 2-320 or fsctl (Manage an active file system) on page 2-335	Enabling automatic failover that is performed when a file system is blocked on page 3-49
Changing the settings to enable recording of the file creation time	`fsctl`	fsctl (Manage an active file system) on page 2-335	Changing the settings to enable recording of the file creation time on page 3-50
Viewing the device files that can be used	`lulist`	lulist (List available device files information) on page 2-460	--
Connecting a file system	`fsimport`	fsimport (Connect a file system) on page 2-365	--
Disconnecting a file system	`fsexport`	fsexport (Disconnect a file system from the HDI system) on page 2-359	--
Checking the integrity of and repairing a file system	`fsrepair`	fsrepair (Check the integrity of and repair a file system) on page 2-386	--
Releasing the unused area of virtual LUs	`dpreclaim`	dpreclaim (Release the unused area of virtual LUs)	--

Operation		Command	Reference	Procedure
			on page 2-299	
Viewing the number of files that can be created		fsifreeget	fsifreeget (Display the number of files that can be created) on page 2-363	--
References or specifies parameters related to inodes		fsinodectl	fsinodectl (Management of Inodes) on page 2-366	--
Viewing information about the files that are using the inode area		fsiusedlist	fsiusedlist (Display information about the files that are using the inode area) on page 2-370	--
Reconfiguring the inode area		fsinodespace	fsinodespace (Reconfigure the inode area) on page 2-369	--
Moves file expansion attributes		fsmoveattr	fsmoveattr (Moving extension attributes from the inode area) on page 2-383	--
Managing WORM tasks		wormctl	wormctl (Manage WORM tasks) on page 2-677	--
Managing directories				
--	Viewing the directory attributes	dirlist	dirlist (List directory attributes) on page 2-286	--
	Creating a directory	dircreate	dircreate (Create a directory) on page 2-275	--
	Changing the directory attributes	diredit	diredit (Change directory	--

Operation		Command	Reference	Procedure
			attributes) on page 2-280	
	Deleting a directory	dirdel	dirdel (Delete a directory) on page 2-278	--
Managing volume groups				
--	Viewing the capacity of a volume group	diskfreeget	diskfreeget (Display the capacity of a volume group) on page 2-298	--
	Viewing information about a volume group	vgrlist	vgrlist (Display information about volume groups) on page 2-671	--
	Creating a volume group	vgrcreate	vgrcreate (Create a volume group) on page 2-667	--
	Expanding a volume group	vgrexpand	vgrexpand (Expand a volume group) on page 2-669	--
	Deleting a volume group	vgrdelete	vgrdelete (Delete a volume group) on page 2-668	--
	Repairing a volume group	vgrrepair	vgrrepair (Repair a volume group) on page 2-674	--
Managing an NFS share				
--	Viewing information about NFS shares	nfslist	nfslist (List NFS share information) on page 2-521	--
	Creating an NFS share	nfscreate	nfscreate (Create an NFS share) on page 2-502	Creating an NFS share on page 3-51

Operation	Command	Reference	Procedure
Editing information about an NFS share	`nfsedit`	nfsedit (Edit NFS share information) on page 2-512	Editing information about an NFS share on page 3-53
Deleting an NFS share	`nfsdelete`	nfsdelete (Delete NFS shares) on page 2-511	--
Backing up information about NFS shares	`nfsbackup`	nfsbackup (Back up NFS share information) on page 2-499	Backing up information about NFS shares on page 3-54
Restoring information about NFS shares	`nfsrestore`	nfsrestore (Restore NFS share information) on page 2-535	Restoring information about NFS shares on page 3-55
Managing a CIFS share			
-- Viewing information about CIFS shares	`cifslist`	cifslist (List CIFS share information) on page 2-187	--
Creating a CIFS share	`cifscreate`	cifscreate (Create a CIFS share) on page 2-151	Creating a CIFS share on page 3-57
Editing information about a CIFS share	`cifsedit`	cifsedit (Edit CIFS share information) on page 2-170	Editing information about a CIFS share on page 3-59
Deleting a CIFS share	`cifsdelete`	cifsdelete (Delete a CIFS share) on page 2-166	--
Backing up information about CIFS shares	`cifsbackup`	cifsbackup (Back up CIFS share information) on page 2-149	Backing up information about CIFS shares on page 3-60

Before Using Commands

Operation		Command	Reference	Procedure
	Restoring information about CIFS shares	`cifsrestore`	cifsrestore (Restore CIFS share information) on page 2-218	Restoring information about CIFS shares on page 3-62
Managing an ACL				
--	Viewing ACL settings	`dirgetacl`	dirgetacl (Display ACL information) on page 2-282	--
	Setting an ACL (for a file system of the Advanced ACL type)	`dirsetacl`	dirsetacl (Set ACLs) on page 2-289	Setting an ACL (for a file system of the Advanced ACL type) on page 3-66
	Setting an ACL (for a file system of the Classic ACL type)	`dirsetacl`	dirsetacl (Set ACLs) on page 2-289	Setting an ACL (for a file system of the Classic ACL type) on page 3-67
Managing quotas for each file system				
--	Setting quotas for users for each file system	`quotaset`	quotaset (Set quotas for each file system) on page 2-557	Setting quotas for users for each file system on page 3-69
	Setting quotas for groups for each file system	`quotaset`	quotaset (Set quotas for each file system) on page 2-557	Setting quotas for groups for each file system on page 3-69
	Setting the default quota for a file system	`quotaset`	quotaset (Set quotas for each file system) on page 2-557	Setting the default quota for a file system on page 3-70
	Setting a quota grace period for a file system	`quotaset`	quotaset (Set quotas for each file system) on page 2-557	Setting a quota grace period for a file system on page 3-71
	Setting the quota monitoring method for a file system	`quotaset`	quotaset (Set quotas for each file	Setting the quota monitoring method for a

Operation		Command	Reference	Procedure
			system) on page 2-557	file system on page 3-72
	Viewing the quota information set for a file system	`quotaget`	quotaget (Display the quota information set for each file system) on page 2-551	--
Managing subtree quotas				
--	Setting a quota for a directory	`stquotaset`	stquotaset (Set quotas for each directory) on page 2-603	Setting a quota for a directory on page 3-73
	Setting quotas for users for each directory	`stquotaset`	stquotaset (Set quotas for each directory) on page 2-603	Setting quotas for users for each directory on page 3-74
	Setting quotas for groups for each directory	`stquotaset`	stquotaset (Set quotas for each directory) on page 2-603	Setting quotas for groups for each directory on page 3-75
	Setting the default quota for a directory	`stquotaset`	stquotaset (Set quotas for each directory) on page 2-603	Setting the default quota for a directory on page 3-76
	Applying a quota to an existing directory	`stquotaset`	stquotaset (Set quotas for each directory) on page 2-603	Applying a quota to an existing directory on page 3-77
	Setting a quota grace period for a directory	`stquotaset`	stquotaset (Set quotas for each directory) on page 2-603	Setting a quota grace period for a directory on page 3-78
	Setting the quota monitoring method for each directory	`stquotaset`	stquotaset (Set quotas for each directory) on page 2-603	Setting the quota monitoring method for each directory on page 3-79

Operation		Command	Reference	Procedure
	Viewing the quota information set for directories	`stquota`	stquota (Display the quota information set for each directory) on page 2-591	--
	Viewing the user or group quota information set for a directory	`stquotalist`	stquotalist (List the quota information set for users or groups for each directory) on page 2-599	--
Managing user mapping information				
--	Viewing the IDs and names that are mapped by using RIDs	`umapidget`	umapidget (Get IDs and names mapped using RIDs) on page 2-655	--
Managing system settings				
--	Viewing the save status of the system LUs	`syslusavestatus`	syslusavestatus (Display the save status of system LUs) on page 2-631	--
	Saving system LUs and outputting the system settings file to the home directory	`syslusave`	syslusave (Save system LUs) on page 2-628	Saving system LUs and outputting the system settings file to the home directory on page 3-81
	Saving system LUs and outputting the system settings file to a file system	`syslusave`	syslusave (Save system LUs) on page 2-628	Saving system LUs and outputting the system settings file to a file system on page 3-82
	Viewing the settings for periodic saving for the system LU	`sysluscheduleget`	syslusscheduleget (Display the periodic-	--

Operation		Command	Reference	Procedure
			saving settings for the system LU) on page 2-635	
	Changing the settings for periodic saving for the system LU	`sysluschedul eset`	sysluschedule set (Specify the periodic-saving settings for the system LU) on page 2-637	Changing the settings for periodic saving for the system LU on page 3-84
	Restoring the system LUs	`syslurestore`	syslurestore (Restore system LUs) on page 2-620	Restoring the system LUs on page 3-85
Managing the home directory for the SSH account				
--	Deleting a file stored in the home directory[#]	`rmfile`	rmfile (Delete a file stored in the home directory) on page 2-573	--
Managing a node				
--	Viewing the status of hardware	`hwstatus`	hwstatus (Display the hardware status) on page 2-438	--
	Resetting a node	`nncreset`	nncreset (Reset a node) on page 2-543	--
	Viewing the status of the other node in the cluster	`peerstatus`	peerstatus (Display the status of the other node in the cluster) on page 2-544	--
Setting up HCP linkage				
--	Viewing information about the migration-destination HCP system	`archcpget`	archcpget (Display information about the migration destination HCP system)	--

Operation	Command	Reference	Procedure
		on page 2-45	
Changing the information of the migration destination HCP system	archcpset	archcpset (Set information about the migration destination HCP system) on page 2-47	Changing the information of the migration destination HCP system on page 3-86
Deleting information about the migration-destination HCP system	archcpdel	archcpdel (Delete information about the migration destination HCP system) on page 2-44	--
Changing the HCP communication setting	arcsslctl	arcsslctl (Set the method of communication with the HCP system) on page 2-111	Changing the HCP communication setting on page 3-87
Viewing the migration task information	arcmiglist	arcmiglist (Display information about migration tasks) on page 2-65	--
Creating the migration task	arcmigset	arcmigset (Create migration tasks) on page 2-70	--
Changing the migration task setting	arcmigedit	arcmigedit (Change the settings of a migration task) on page 2-57	--
Deleting the migration task	arcmigdel	arcmigdel (Delete migration tasks) on page 2-56	--
Enabling the migration task	arcmigctl	arcmigctl (Enable	--

Operation	Command	Reference	Procedure
		migration tasks) on page 2-55	
Executes the migration task immediately	arcmigrun	arcmigrun (Execute the migration task immediately) on page 2-69	--
Cancels the processing of migration	arcmigstop	arcmigstop (Stop migration currently being executed) on page 2-82	--
Displays the execution results of migration tasks	arcmigstatus	arcmigstatus (Display the execution results of the migration task) on page 2-78	--
Displays the paths of files for which migration succeeded or failed	arcmigresult	arcmigresult (Display the paths of files for which migration succeeded or failed) on page 2-68	--
Viewing the stub status of a file	arcfstatus	arcfstatus (Display the stub status of a file) on page 2-43	--
Viewing proxy server information	arcproxyget	arcproxyget (Display proxy server information) on page 2-88	--
Changing proxy server information	arcproxyset	arcproxyset (Set proxy server information) on page 2-89	Changing proxy server information on page 3-87
Deleting proxy server information	arcproxydel	arcproxydel (Delete proxy server information)	--

Operation	Command	Reference	Procedure
		on page 2-87	
Viewing the threshold at which stub processing is performed	arcreplimitg et	arcreplimitget (Display the threshold at which stub processing is performed) on page 2-91	--
Changing the stub threshold	arcreplimits et	arcreplimitset (Set the threshold at which stub processing is performed) on page 2-92	Changing the stub threshold on page 3-88
Checking the access to an HCP system	hcpaccesstes t	hcpaccesstest (Check the access to the HCP system) on page 2-399	--
Viewing information about operations performed on an HCP system when a file is deleted	hcpobjdelget	hcpobjdelget (Display the data deletion settings in the HCP system when files are deleted) on page 2-403	--
Setting operations performed on an HCP system when a file is deleted	hcpobjdelset	hcpobjdelset (Data deletion settings in the HCP system when files are deleted) on page 2-404	--
Restoring a file system whose data has been migrated to the HCP system	arcrestore	arcrestore (Restore a file system whose data has been migrated to the HCP system) on page 2-102	--
Viewing the URL for the storage location of a file in an HCP system	arcurlget	arcurlget (Display the URL for the storage location of data in an HCP system)	--

Operation	Command	Reference	Procedure
		on page 2-114	
Rebuilding management information for a file system	arccorrection	arccorrection (Rebuild management information for a file system) on page 2-36	--
Viewing or deleting the task log information	arcresultctl	arcresultctl (Manage task log information) on page 2-106	--
Setting the initial mode for tasks	arcmodectl	arcmodectl (Set initial mode for tasks) on page 2-83	--
Viewing the progress status of task pre- and post-processing	arctaskstatus	arctaskstatus (Display the progress status of task pre- and post-processing) on page 2-113	--
Checking the integrity of or restoring files that have been migrated by using HCP linkage	hcporphanrestore	hcporphanrestore (Check the integrity of and recover the files in both the HDI and HCP systems) on page 2-405	--
Viewing cache resident policies	arcresidentpolicylist	arcresidentpolicylist (Display cache resident policies) on page 2-97	--
Setting cache resident policies	arcresidentpolicyset	arcresidentpolicyset (Set a cache resident policy) on page 2-99	--
Deleting cache resident policies	arcresidentpolicydel	arcresidentpolicydel (Delete	--

Operation	Command	Reference	Procedure
		a cache resident policy) on page 2-96	
Viewing files pinned in the cache	`arcresidentl ist`	arcresidentlist (Display pinned files) on page 2-95	--
Viewing the execution results of cache resident processing	`arcresidentr esult`	arcresidentresult (Display the results of cache resident processing) on page 2-101	--
Changing the settings for collecting information about pinned files	`arcresidentc tl`	arcresidentctl (Setting for acquiring information about pinned files) on page 2-94	--
Viewing the settings for collecting information about pinned files	`arcresidentc tl`	arcresidentctl (Setting for acquiring information about pinned files) on page 2-94	--
Managing roaming for home-directory-roaming file systems	`archdctl`	archdctl (managing roaming for home-directory-roaming file systems) on page 2-50	--
Recalling a file	`arcfrecall`	arcfrecall (Recalling a file) on page 2-41	--
Deleting the data and mapping information for a file system that was linked to the HCP system at the share level	`arcstdel`	arcstdel (Delete the data and mapping information for a file system linked to the HCP system at the share level)	--

Operation	Command	Reference	Procedure
		on page 2-86	
View capacity allocated for file systems linked with an HCP system	arcresvget	arcresvget (Displaying the reserved space for file systems that link to the HCP system) on page 2-108	--
Set capacity allocated for file systems linked with an HCP system	arcresvset	arcresvset (Setting the reserved space for file systems that link to the HCP system) on page 2-109	--
Changing the settings for custom scheduling of the file version restore functionality	arccustomschlctl	arccustomschlctl (Settings related to custom schedules of the file version restore functionality) on page 2-39	--
Viewing the settings for custom scheduling of the file version restore functionality	arccustomschlctl	arccustomschlctl (Settings related to custom schedules of the file version restore functionality) on page 2-39	--
Viewing the settings for the Active File Migration function	arcactmigctl	arcactmigctl (Settings related to the Active File Migration function) on page 2-21	--
Changing the settings for the Active File Migration function	arcactmigctl	arcactmigctl (Settings related to the	--

Operation		Command	Reference	Procedure
			Active File Migration function) on page 2-21	
	Viewing the settings for the Large File Transfer function	`arclftctl`	arclftctl (Settings related to the Large File Transfer function) on page 2-52	--
	Changing the settings for the Large File Transfer function	`arclftctl`	arclftctl (Settings related to the Large File Transfer function) on page 2-52	--
Managing a data import from another file server				
--	Viewing data import definition information of other file servers	`datamigrateconflist`	datamigrateconflist (Display data import definition information) on page 2-249	--
	Adding data import definition information of another file server	`datamigrateconfadd`	datamigrateconfadd (Add data import definition information) on page 2-241	Adding data import definition information about another file server on page 3-89
	Editing data import definition information of another file server	`datamigrateconfedit`	datamigrateconfedit (Set data import definition information) on page 2-246	--
	Starting a data import to an HDI system from another file server	`datamigratestart`	datamigratestart (Start a data import) on page 2-259	Starting an import from another file server on page 3-90
	Viewing the results of a data import to an HDI system from another file server	`datamigratestatus`	datamigratestatus (Display the results of the import process) on page 2-261	--

Operation	Command	Reference	Procedure
Deleting data import definition information of another file server	`datamigratec onfdel`	datamigrateco nfdel (Delete data import definition information) on page 2-244	--
Checking access to import sources	`datamigratea ccesstest`	datamigrateac cesstest (Check accessibility of import-source file servers) on page 2-239	--
Changing the method for importing data from another file server to an HDI system	`datamigratec tl`	datamigratect l (Change how to import data) on page 2-253	--
Viewing the threshold at which a data import from another file server is suspended or resumed	`datamigrateli imitget`	datamigrateli mitget (Display the threshold at which data importation is suspended or resumed) on page 2-256	--
Setting the threshold at which a data import from another file server is suspended or resumed	`datamigrateli imitset`	datamigrateli mitset (Set the threshold at which a data import is suspended or resumed) on page 2-257	--
Verifying import definition information	`datamigratet est`	datamigratete st (Verify import definition information) on page 2-266	--
Viewing the settings for the operation mode of imports	`datamigratea ccessctl`	datamigrateac cessctl (Setting the operation mode for imports) on page 2-237	--

Operation		Command	Reference	Procedure
	Changing the settings for the operation mode of imports	`datamigrateaccessctl`	datamigrateaccessctl (Setting the operation mode for imports) on page 2-237	--
Managing migration and import settings				
--	Viewing migration or import settings	`arcconflist`	arcconflist (Display the data migration or import) on page 2-33	--
	Changing migration and import settings	`arcconfedit`	arcconfedit (Configure the data migration or import) on page 2-24	Changing data import settings on page 3-90
Managing dump files				
--	Specifying whether to acquire dump files[#]	`dumpset`	dumpset (Specify whether to acquire dump files) on page 2-302	--
	Deleting dump files[#]	`dumpdel`	dumpdel (Delete dump files) on page 2-301	--
Managing version information				
--	Viewing the version	`versionlist`	versionlist (Display the version) on page 2-666	--
Managing TLS				
--	Changing the TLS settings	`tlsctl`	tlsctl (Settings for TLS) on page 2-653	--
	Viewing the TLS setting	`tlsctl`	tlsctl (Settings for TLS) on page 2-653	--
Account management				

	Operation	Command	Reference	Procedure
--	Initializing account passwords#	`adminpasswd`	adminpasswd (Initialize account passwords) on page 2-14	--
	Initialize the account settings#	`adminctl`	adminctl (Account management) on page 2-14	--
	Cancel account lockout#	`adminctl`	adminctl (Account management) on page 2-14	--
Managing RAID cards				
--	Viewing information about write operations to the cache memory on RAID cards	`cachedbadbbu get`	cachedbadbbu get (Display information about RAID card cache operations) on page 2-140	--
	Configuring the setting for write operations to the cache memory on RAID cards	`cachedbadbbu set`	cachedbadbbu set (Configure the setting for RAID card cache operations) on page 2-142	--
Managing the diagnostics schedule for the internal RAID battery or super capacitor				
--	Viewing the diagnostics schedule for the internal RAID battery or super capacitor	`bbuschlget`	bbuschlget (Display the diagnostics schedule for an internal RAID battery or a super capacitor) on page 2-134	--
	Setting the diagnostics schedule for the internal RAID battery or super capacitor	`bbuschlset`	bbuschlset (Set the diagnostics schedule of the internal RAID battery or the super	--

Operation		Command	Reference	Procedure
			capacitor) on page 2-135	
Managing user disks created from internal hard disks				
--	Viewing the RAID level of a user disk created from internal hard disks	`internalraid levelget`	internalraidlevelget (Display the RAID level of user disks created from internal hard disks) on page 2-458	--
	Setting the RAID level of a user disk created from internal hard disks	`internalraid levelset`	internalraidlevelset (Set the RAID level of a user disk created from an internal hard disk) on page 2-459	--
	Deleting a user disk created from internal hard disks and associated mapping information	`internallude lete`	internalludelete (Delete a user disk from an internal hard disk) on page 2-457	--
Managing the NDMP server				
--	Controlling the NDMP server[#]	`ndmpcontrol`	ndmpcontrol (Control the NDMP server) on page 2-487	Controlling the NDMP server on page 3-92
	Changing the NDMP server password[#]	`ndmppasswd`	ndmppasswd (Change the NDMP server password) on page 2-493	Changing the NDMP server password on page 3-93
	Changing the NDMP server configuration information[#]	`ndmpconfig`	ndmpconfig (Display or modify NDMP server configuration information) on page 2-485	Changing the NDMP server configuration information on page 3-93
	Changing the conditions for interrupting an offline backup	`ndmpfsconfig`	ndmpfsconfig (Change the conditions for interrupting an offline backup) on page 2-490	Changing the conditions for interrupting an offline backup on page 3-94

Operation		Command	Reference	Procedure
Managing a tape drive				
--	Viewing the information about tape drives	`tapelist`	tapelist (Display information about tape drives) on page 2-644	--
	Registering tape drives collectively	`tapeadd`	tapeadd (Register tape drive information) on page 2-641	Registering tape drives collectively on page 3-96
	Enabling registration information of a tape drive	`tapeadd`	tapeadd (Register tape drive information) on page 2-641	Registering tape drives individually on page 3-97
	Unregistering tape drive information	`tapedel`	tapedel (Unregister registered tape drive information) on page 2-643	Unregistering tape drive information on page 3-98
Using the functionality for linking with array volume replication functions				
--	Viewing the CCI instance numbers currently being used	`horcconflist`	horcconflist (Display the CCI instance numbers currently being used) on page 2-412	--
	Viewing the configuration information about a device file	`horcdevlist`	horcdevlist (Display configuration information about a device file) on page 2-413	--
	Disconnecting the copy-destination file system from a node	`horcexport`	horcexport (Disconnect the copy-destination file system from a node) on page 2-419	--

Operation	Command	Reference	Procedure
Suppressing access from clients to the copy-source file system	horcfreeze	horcfreeze (Suppress access from clients to the copy-source file system) on page 2-420	--
Connecting the copy-destination file system to the node when a volume manager is not being used	horcimport	horcimport (Connect the copy-destination file system to the node when a volume manager is not being used) on page 2-422	--
Deleting CCI logs[#]	horclogremove	horclogremove (Delete CCI logs) on page 2-424	--
Viewing the CCI environment variable	horcprintenv	horcprintenv (Display the CCI environment variable) on page 2-425	--
Adding a CCI instance	horcsetconf	horcsetconf (Add a CCI instance) on page 2-426	--
Setting up or modifying the CCI environment variable[#]	horcsetenv	horcsetenv (Set up or modify the CCI environment variable) on page 2-427	--
Re-opening access from clients to the copy-source file system	horcunfreeze	horcunfreeze (Re-open access from clients to the copy-source file system) on page 2-430	--
Deleting a CCI instance	horcunsetconf	horcunsetconf (Delete a CCI	--

Operation	Command	Reference	Procedure
		instance) on page 2-431	
Deleting the CCI environment variable[#]	horcunsetenv	horcunsetenv (Delete the CCI environment variable) on page 2-432	--
Reserving device files	horcvmdefine	horcvmdefine (Reserve device files) on page 2-433	--
Releasing device files	horcvmdelete	horcvmdelete (Release device files) on page 2-434	--
Connecting the copy-destination file system to the node when a volume manager is being used	horcvmimport	horcvmimport (Connect a copy-destination file system to a node when a volume manager is being used) on page 2-436	--

#

This operation is applied to the node on which the command is executed. In cluster configurations, this command must be executed on both nodes.

Commands that can be used depending on the system configuration

The commands that a system administrator can use differ depending on the HDI system configuration.

The following table describes the commands that can be used depending on the system configuration.

Table 1-2 Commands that can be used depending on the system configuration

Command	When using a cluster configuration	When using a single-node configuration
adminctl	Y	Y

Command	When using a cluster configuration	When using a single-node configuration
adminpasswd	Y	Y
altipadd	Y	--
altipdel	Y	--
altiplist	Y	--
arcactmigctl	Y	Y
arcconfedit	Y	Y
arcconflist	Y	Y
arccorrection	Y	Y
arccustomschlctl	Y	Y
arcfrecall	Y	Y
arcfstatus	Y	Y
archcpdel	Y	Y
archcpget	Y	Y
archcpset	Y	Y
archdctl	Y	Y
arclftctl	Y	Y
arcmigctl	Y	Y
arcmigdel	Y	Y
arcmigedit	Y	Y
arcmiglist	Y	Y
arcmigresult	Y	Y
arcmigrun	Y	Y
arcmigset	Y	Y
arcmigstatus	Y	Y
arcmigstop	Y	Y
arcmodectl	Y	Y
arcproxydel	Y	Y
arcproxyget	Y	Y
arcproxyset	Y	Y
arcreplimitget	Y	Y
arcreplimitset	Y	Y
arcresidentctl	Y	Y
arcresidentlist	Y	Y

Command	When using a cluster configuration	When using a single-node configuration
arcresidentpolicydel	Y	Y
arcresidentpolicylist	Y	Y
arcresidentpolicyset	Y	Y
arcresidentresult	Y	Y
arcrestore	Y	Y
arcresultctl	Y	Y
arcresvget	Y	Y
arcresvset	Y	Y
arcsslctl	Y	Y
arcstdel	Y	Y
arctaskstatus	Y	Y
arcurlget	Y	Y
avaconfedit	Y	Y
avaextensionsedit	Y	Y
avascanengineset	Y	Y
avaserveradd	Y	Y
avaserverdel	Y	Y
avaserveredit	Y	Y
avaservicestart	Y	Y
avaservicestatus	Y	Y
avaservicestop	Y	Y
bbuschlget	--	Y
bbuschlset	--	Y
bmcctl	Y	Y
cachedbadbbuget	--	Y
cachedbadbbuset	--	Y
certctl	Y	Y
cifsbackup	Y	Y
cifscreate	Y	Y
cifsdelete	Y	Y
cifsedit	Y	Y
cifsinfogetctl	Y	Y
cifslist	Y	Y

Before Using Commands

Command	When using a cluster configuration	When using a single-node configuration
cifslogctl	Y	Y
cifsoptlist	Y	Y
cifsoptset	Y	Y
cifsrestore	Y	Y
clctl	Y	--
clstart	Y	--
clstatus	Y	--
clstop	Y	--
datamigrateaccessctl	Y	Y
datamigrateaccesstest	Y	Y
datamigrateconfadd	Y	Y
datamigrateconfdel	Y	Y
datamigrateconfedit	Y	Y
datamigrateconflist	Y	Y
datamigratectl	Y	Y
datamigratelimitget	Y	Y
datamigratelimitset	Y	Y
datamigratestart	Y	Y
datamigratestatus	Y	Y
datamigratetest	Y	Y
dhcpget	--	Y
dhcpreload	--	Y
dhcpset	--	Y
dircreate	Y	Y
dirdel	Y	Y
diredit	Y	Y
dirgetacl	Y	Y
dirlist	Y	Y
dirsetacl	Y	Y
diskfreeget	--	Y
dpreclaim	Y	Y
dumpdel	Y	Y
dumpset	Y	--

Command	When using a cluster configuration	When using a single-node configuration
emergencyshutdown	Y	Y
encdisplaykey	Y	Y
encrecoverkey	Y	Y
encverifykey	Y	Y
eraselog	Y	Y
fpctl	Y	Y
fpoffline	Y	Y
fponline	Y	Y
fpstatus	Y	Y
fsautofo	Y	--
fscreate	Y	Y
fsctl	Y	Y
fsdelete	Y	Y
fsedit	Y	Y
fsexpand	Y	Y
fsexport	Y	--
fsfullmsg	Y	Y
fsifreeget	Y	Y
fsimport	Y	--
fsinodectl	Y	Y
fsinodespace	Y	Y
fsiusedlist	Y	Y
fslist	Y	Y
fsmount	Y	Y
fsmoveattr	Y	Y
fsrepair	Y	Y
fsumount	Y	Y
ftpget	Y	Y
ftpset	Y	Y
grpadd	Y	Y
grpdel	Y	Y
grplist	Y	Y
hcpaccesstest	Y	Y

Before Using Commands

Command	When using a cluster configuration	When using a single-node configuration
hcpdisplaykey	Y	Y
hcpobjdelget	Y	Y
hcpobjdelset	Y	Y
hcporphanrestore	Y	Y
hcprecoverkey	Y	Y
hcpverifykey	Y	Y
hnasmpasswd	Y	--
horcconflist	Y	--
horcdevlist	Y	--
horcexport	Y	--
horcfreeze	Y	--
horcimport	Y	--
horclogremove	Y	--
horcprintenv	Y	--
horcsetconf	Y	--
horcsetenv	Y	--
horcunfreeze	Y	--
horcunsetconf	Y	--
horcunsetenv	Y	--
horcvmdefine	Y	--
horcvmdelete	Y	--
horcvmimport	Y	--
hwstatus	Y	Y
ifadd	Y	Y
ifdel	Y	Y
ifedit	Y	Y
iflist	Y	Y
internalludelete	--	Y
internalraidlevelget	--	Y
internalraidlevelset	--	Y
lulist	Y	Y
lumapadd	Y	--
lumapctl	Y	--

Command	When using a cluster configuration	When using a single-node configuration
lumapdelete	Y	--
lumaplist	Y	Y
nasboot	Y	--
nasipneigh	Y	Y
nasnetstat	Y	Y
nasping	Y	Y
nasreboot	Y	Y
nasshutdown	Y	Y
nastraceroute	Y	Y
ndmpconfig	Y	Y
ndmpcontrol	Y	Y
ndmpfsconfig	Y	Y
ndmppasswd	Y	Y
ndstart	Y	--
ndstatus	Y	--
ndstop	Y	--
nfsbackup	Y	Y
nfscacheflush	Y	Y
nfscreate	Y	Y
nfsdelete	Y	Y
nfsedit	Y	Y
nfskeytabadd	Y	Y
nfskeytabdel	Y	Y
nfskeytablist	Y	Y
nfslist	Y	Y
nfslocksclear	Y	Y
nfslockslist	Y	Y
nfsoptlist	Y	Y
nfsoptset	Y	Y
nfsrestore	Y	Y
nfsstatus	Y	Y
nfssvget	Y	Y
nfssvset	Y	Y

Before Using Commands

Command	When using a cluster configuration	When using a single-node configuration
nncreset	Y	Y
peerstatus	Y	--
perfmonctl	Y	Y
pmctl	Y	Y
quotaget	Y	Y
quotaset	Y	Y
rgmon	Y	--
rgmove	Y	--
rgstart	Y	Y
rgstatus	Y	Y
rgstop	Y	Y
rmfile	Y	Y
routeadd	Y	Y
routedel	Y	Y
routefilterctl	Y	Y
routelist	Y	Y
secureshellctl	Y	Y
sshkeyadd	Y	Y
sshkeydel	Y	Y
sshkeylist	Y	Y
stquota	Y	Y
stquotalist	Y	Y
stquotaset	Y	Y
svctl	Y	Y
svstartuplist	Y	Y
svstartupset	Y	Y
svstatus	Y	Y
sysinfoget	Y	Y
syslurestore	Y	Y
syslusave	Y	Y
syslusavestatus	Y	Y
sysluscheduleget	Y	Y
syslusscheduleset	Y	Y

Command	When using a cluster configuration	When using a single-node configuration
tapeadd	Y	--
tapedel	Y	--
tapelist	Y	--
tftpget	Y	Y
tftpset	Y	Y
timeget	Y	Y
timeset	Y	Y
tlsctl	Y	Y
umapidget	Y	Y
upnpctl	--	Y
usradd	Y	Y
usrdel	Y	Y
usrlist	Y	Y
versionlist	Y	Y
vgrcreate	--	Y
vgrdelete	--	Y
vgrexpand	--	Y
vgrlist	--	Y
vgrrepair	--	Y
welcomemsgchange	Y	Y
wormctl	Y	Y

Legend:
    Y: Can be used, --: Cannot be used.

Prerequisites for using commands

The following conditions must be met before you can use commands:

- For operations with a cluster configuration, a cluster configuration needs to be defined.

  For details on how to define a cluster configuration, see the *Administrator's Guide*.

- At least one public key is registered for the SSH account (nasroot).

  The first public key is registered by using the GUI. For details about how to use the GUI to register a public key, see the *Administrator's Guide*.

Command execution

Commands can be executed by logging in to the node, or from a remote host. However, to execute commands interactively, we recommend that you log in to the node itself.

To execute a command, use `nasroot` as an SSH account and specify any one of the following: the unique IP address of the node or the host name.

To execute any of the following commands listed in "Table 1-1 Operations that can be performed by using commands on page 1-2" In a cluster configurations, we recommend that you specify the virtual IP address in case of a failover.

- File system management commands
- Directory management commands
- NFS sharing management commands
- CIFS sharing management commands
- ACL management commands
- File system-specific quota management commands
- Subtree quota management commands
- HCP linkage setup commands (excluding those executed without specifying a file system name)
- Import management commands
- Volume replication linking function operation commands (excluding those executed without specifying a file system name)

You can also execute multiple commands automatically by creating a shell script on a remote host. For details on how to create a shell script, see the documentation for the remote host OS.

Executing commands by logging in to a node

This section explains how to log in to a node to execute commands. Note that the procedure assumes that an SSH public key has already been registered.

To log in to a node to execute commands:

1. Log in to the target node.
   If you want to log in from a UNIX machine, execute the `ssh` command.

   ```
   ssh -2 user-name-of-the-ssh-account@IP-address or host-name
   ```

   If you want to log in from a Windows computer, use PuTTY.

   Note:
      If the KAQM14179-W message appears after you execute the `ssh` command, take appropriate action according to the message.

2. Use the `sudo` command to execute commands.
   The following shows an example of executing a command.

In this example, you will execute the `fscreate` command.

```
$ sudo fscreate FS_1 lu1A
```

3. Use the `exit` command to log out.

```
$ exit
```

Executing commands from a remote host

This section explains how to execute commands from a remote host.

To execute commands from a UNIX machine, execute the `ssh` and `sudo` commands.

```
ssh -2 user-name-of-the-ssh-account@IP-address or host-name sudo command-to-be-
executed
```

To execute commands remotely from a Windows computer, execute either of the following commands.

When using the `plink.exe` and `sudo` commands:

```
plink.exe -ssh -2 -i private-key ssh-account-user-name@IP-address or host-
name sudo command-to-be-executed
```

When using the `putty.exe` command and the file containing the `sudo` command that is to be executed on an HDI system:

```
putty.exe -ssh -2 -i private-key ssh-account-user-name@IP-address or host-
name -m file-name
```

Common options

This section describes the options that are commonly used for many commands.

`--`

None of the characters following this option are treated as options. For example, if you want to specify a cluster name `-h`, enter `-- -h`.

`-h`

Specify this to view the command format.

`-nomsg`

Specify this to suppress the output of messages by a command to the standard output and standard error output.

`-y`

Specify this to suppress the output of confirmation messages.

Notes on operations (required reading before using commands)

Keep the following points in mind when you execute commands:

- Do not use a command that is not explained in this manual.
- Normally, do not perform GUI operations while commands are being used to perform operations in an HDI system.
- You must check the result after executing a command.
- If the CIFS service configuration definition settings do not allow the CIFS share settings to be automatically reloaded and you execute one of the following commands, restart the CIFS service on the node on which you executed the command:

  - `cifscreate`
  - `cifsedit`
  - `cifsdelete`
  - `cifsoptset`
  - `cifsrestore`

  If, during degenerated operation, you perform operations related to the CIFS share, restart the CIFS service on both nodes after the failback is finished.

  Unless you restart the CIFS service, the new settings of the CIFS share are not applied to a client environment until the CIFS client logs into the machine again or connects to the file share again.

  Even if a client environment is set up to automatically reloaded CIFS share settings, changes made to CIFS share settings in the CIFS service configuration definition might not be automatically applied to the client environment. If new CIFS share settings are not automatically applied, they will be applied the next time a CIFS client logs in to the PC or a connection with the file share is re-established.

  For details on how to check the CIFS service configuration definition, see the *Administrator's Guide*. For details on how to restart the CIFS service, see Restarting a service on page 3-18. For details on how to fail back, see Changing the execution node of a resource group on page 3-11.

- Extended options set by the `cifsoptset` command are not backed up or restored by the `cifsbackup` command or the `cifsrestore` command. If the settings were changed from the defaults, reconfigure them by using the `cifsoptset` command.
- Once you start HDI system operations, do not delete the definition of host names or network names specified as the NFS share public destination. If you do need to delete the definition of host names or network names, delete the NFS share beforehand or make sure that the host name or network name specified as the NFS share public destination is not included in the deletion definitions.
- When you register or delete a public key, always perform the operation for both of the nodes that make up a cluster. If you perform different

operations for the nodes, you might no longer be able to log in by specifying a virtual IP address.

- When you execute a command, do not perform any other operation until the command processing is complete. In addition, do not allow more than one system administrator to log in and perform operations at the same time. If any other operation is performed while a command is being processed, the operation performed later might cause an error.

- If you execute a command in an SSH client, do not close the client window before the command processing is complete. If you close the window before the processing is complete, the command processing might stop, resulting in an abnormal system state.

- If the management process for the file system is interrupted due to, for example, the operating system not running, you might be unable to repeat the same operation. In this case, refresh the processing node or execute the `fslist` command to check the status of the file system before following the instructions in the message.

- Executing multiple commands for an NDMP server or tape drive might cause an error.

- If you execute any of the following commands during a backup or restore operation, an error might occur:

  o `ndmpconfig`

  o `ndmpcontrol`

  o `ndmpfsconfig`

  o `tapeadd`

  o `tapedel`

  o `tapelist`

- When a command accepts one of the following signals, the signal will be blocked.

Table 1-3 List of signals to be blocked with a command

Signal value	Signal name	Description
1	`SIGHUP`	e.g. SSH disconnection
2[#]	`SIGINT`	e.g. **Ctrl + C**
3	`SIGQUIT`	e.g. **Ctrl + **
15	`SIGTERM`	e.g. Shutdown

#: The `SIGINT` signal can be used to cancel the processing of the following commands:

o `dpreclaim`

o `fsautofo`

o `fsctl`

o `fsfullmsg`

o `fsrepair`

- ○ `quotaget`
- ○ `stquota`
- ○ `stquotalist`
- ○ `stquotaset`
- If command processing is canceled, it might take time to complete the cancellation processing.
- When a resource group is started in an HDI system, resources for which failure is detected are blocked, and the resource group is comprised of the remaining valid resources. When a resource group is partially blocked, services on the node are provided with some services stopped. In this case, when the `clstatus` command or `rgstatus` command is executed, since `Online / No error` is displayed as the resource group status, resource group error information cannot be checked.

  A resource group might become partially blocked in the following situations:

  - ○ When HDI system operation starts
  - ○ When failover or failback occurs
  - ○ When a resource group is restarted

  If the above operations are performed, or the status of the resource group displayed as `Online / No error` when the `clstatus` command or `rgstatus` command is executed even though the user cannot access the file system, the system messages need to be checked in the **List of RAS Information** page (for `List of messages`) of the Check for Errors dialog box to see whether partial resource group blocking has occurred. The system administrator must check whether the KAQG72006-E message is output within the system messages.

  Note that depending on the resource type, other resources using a blocked resource might also be blocked. For example, when a logical volume is blocked, file systems created on the blocked logical volume are also blocked. In this case, the KAQG72006-E message is output for each blocked resource.

  For details on how to check system messages, see the *Administrator's Guide*.

- When you want to execute a command, do not specify non-ASCII characters in any argument unless indicated. If the command's output result contains non-ASCII characters, it might not be displayed properly.

  You can use multibyte unicode (UTF-8) characters for the following items:

  - ○ Path names (except for NFS shared directory paths)
  - ○ CIFS share names
  - ○ Comments for CIFS shares
  - ○ User or group names that are assigned by user mapping

- If commands take a long time to finish and you cannot determine the cause, there might be a problem in the FC cable connections between the HDI node and the storage system. Check the connections, and if you

cannot locate the problem, view the system messages and log files to check whether a failure occurred.

- To specify an IPv6 IP address, enclose the value in square brackets (`[` `]`).

  Example: `[2001:2c0:418:10::0]`

  Note, however, that the following IP addresses cannot be set:

  `::ffff:`*IPv4-address*, `::`*IPv4-address*, `::1/128`, `::/0`, `::/128`, `fe80::/10`, or `ff00::/8`

  Note that IPv6 IP addresses are registered and displayed in abbreviated form.

- 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.

- Displayed items may change after a node upgrade. For this reason, when analyzing command output results after a node upgrade, review the scripts.

- If a group is specified as an owner of a file or directory, the owner of a file or directory will be managed as `__groupowner` (user ID: 4294967292).

2

Command Reference

This chapter describes the syntax of commands. Execute the commands using the procedures described in Chapter 3, Command Operations on page 3-1.

☐ adminctl (Account management)

☐ adminpasswd (Initialize account passwords)

☐ altipadd (Add virtual IP addresses)

☐ altipdel (Delete added virtual IP addresses)

☐ altiplist (Display added virtual IP addresses)

☐ arcactmigctl (Settings related to the Active File Migration function)

☐ arcconfedit (Configure the data migration or import)

☐ arcconflist (Display the data migration or import)

☐ arccorrection (Rebuild management information for a file system)

☐ arccustomschlctl (Settings related to custom schedules of the file version restore functionality)

☐ arcfrecall (Recalling a file)

☐ arcfstatus (Display the stub status of a file)

☐ archcpdel (Delete information about the migration destination HCP system)

Command Reference

Command Reference

Command Reference

- ☐ fsexport (Disconnect a file system from the HDI system)

- ☐ fsfullmsg (Manage the warning notification functionality for file system usage)

- ☐ fsifreeget (Display the number of files that can be created)

- ☐ fsimport (Connect a file system)

- ☐ fsinodectl (Management of Inodes)

- ☐ fsinodespace (Reconfigure the inode area)

- ☐ fsiusedlist (Display information about the files that are using the inode area)

- ☐ fslist (List file system information)

- ☐ fsmount (Mount a file system)

- ☐ fsmoveattr (Moving extension attributes from the inode area)

- ☐ fsrepair (Check the integrity of and repair a file system)

- ☐ fsumount (Unmount a file system)

- ☐ ftpget (Display the FTP service configuration)

- ☐ ftpset (Change the FTP service configuration)

- ☐ grpadd (Add a group)

- ☐ grpdel (Delete a group)

- ☐ grplist (List group information)

- ☐ hcpaccesstest (Check the access to the HCP system)

- ☐ hcpdisplaykey (Displaying the common encryption key used for data stored on an HCP system to save the data outside of the system)

- ☐ hcpobjdelget (Display the data deletion settings in the HCP system when files are deleted)

- hcpobjdelset (Data deletion settings in the HCP system when files are deleted)

- hcporphanrestore (Check the integrity of and recover the files in both the HDI and HCP systems)

- hcprecoverkey (Restoring the common key used for encryption of data stored on an HCP system)

- hcpverifykey (Verifying common keys used for encryption of data stored on an HCP system)

- hnasmpasswd (Change the password of the management server)

- horcconflist (Display the CCI instance numbers currently being used)

- horcdevlist (Display configuration information about a device file)

- horcexport (Disconnect the copy-destination file system from a node)

- horcfreeze (Suppress access from clients to the copy-source file system)

- horcimport (Connect the copy-destination file system to the node when a volume manager is not being used)

- horclogremove (Delete CCI logs)

- horcprintenv (Display the CCI environment variable)

- horcsetconf (Add a CCI instance)

- horcsetenv (Set up or modify the CCI environment variable)

- horcunfreeze (Re-open access from clients to the copy-source file system)

- horcunsetconf (Delete a CCI instance)

- horcunsetenv (Delete the CCI environment variable)

- horcvmdefine (Reserve device files)

- horcvmdelete (Release device files)

- ☐ horcvmimport (Connect a copy-destination file system to a node when a volume manager is being used)

- ☐ hwstatus (Display the hardware status)

- ☐ ifadd (Add an interface)

- ☐ ifdel (Delete an interface)

- ☐ ifedit (Edit an interface)

- ☐ iflist (List interface information)

- ☐ internalludelete (Delete a user disk from an internal hard disk)

- ☐ internalraidlevelget (Display the RAID level of user disks created from internal hard disks)

- ☐ internalraidlevelset (Set the RAID level of a user disk created from an internal hard disk)

- ☐ lulist (List available device files information)

- ☐ lumapadd (Assign user LUNs)

- ☐ lumapctl (Manage the assignment of user LUNs)

- ☐ lumapdelete (Delete the assignment of user LUNs)

- ☐ lumaplist (Display the information of user LUNs)

- ☐ nasboot (Start the OS on the other node in the cluster)

- ☐ nasipneigh (Check that IP addresses and MAC addresses correspond)

- ☐ nasnetstat (Display the network setting information)

- ☐ nasping (Display the connection to a specified host)

- ☐ nasreboot (Restart the OS on a node)

- ☐ nasshutdown (Stop the OS on a node)

- ☐ nastraceroute (Display the path that leads to the specified host)

- ndmpconfig (Display or modify NDMP server configuration information)

- ndmpcontrol (Control the NDMP server)

- ndmpfsconfig (Change the conditions for interrupting an offline backup)

- ndmppasswd (Change the NDMP server password)

- ndstart (Start a node)

- ndstatus (Display node status)

- ndstop (Stop a node)

- nfsbackup (Back up NFS share information)

- nfscacheflush (Flush NFS caches)

- nfscreate (Create an NFS share)

- nfsdelete (Delete NFS shares)

- nfsedit (Edit NFS share information)

- nfskeytabadd (Add a keytab file for Kerberos authentication)

- nfskeytabdel (Delete principal information from the keytab file for Kerberos authentication)

- nfskeytablist (List the contents of the keytab file for Kerberos authentication)

- nfslist (List NFS share information)

- nfslocksclear (Delete file lock information for an NFS client host)

- nfslockslist (List file lock information for an NFS client host)

- nfsoptlist (Display the NFS environment settings)

- nfsoptset (Set the NFS environment)

- nfsrestore (Restore NFS share information)

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

adminctl (Account management)

Synopsis

```
adminctl --reset [-y]
adminctl --unlock [-y]
```

Description

Initialize the following accounts:

- System administrator account for the GUI in a single-node configuration
- Account used for accessing HDI system via API

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Options and arguments

`--reset`

Specify this option to initialize the account settings. This option performs the following processing:

- Password initialization (To set the initial password, use `chang3me!`)
- Lock release (If the account is locked)

`--unlock`

Specify this option to cancel account lockout.

Return values

Table 2-1 Return values of the adminctl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
99	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

adminpasswd (Initialize account passwords)

Synopsis

```
adminpasswd --reset
```

Description

Forcibly initializes the passwords for the following accounts:

- System administrator account for the GUI in a single-node configuration
- Account used for accessing HDI system via API

To set an initial password, `change3me!` is used.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Return values

Table 2-2 Return values of the adminpasswd command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
99	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

altipadd (Add virtual IP addresses)

Synopsis

```
altipadd -s [virtual-IP-address1a[,virtual-IP-address1b...]]:
   [virtual-IP-address2a[,virtual-IP-address2b...]] interface
altipadd -h
```

Description

This command adds virtual IP addresses to an interface. This command adds up to three virtual IP addresses to a resource group for each interface. A maximum of 256 virtual IP addresses can be set in a cluster, including the virtual IP addresses that were specified when setting up the interfaces.

Before executing this command, make sure that the OSs on both nodes are running and that the cluster and the resource groups on both nodes are running normally or are stopped.

The following are the conditions for specifying an IP address:

- Specify an IP address that has the same network address as the interface.

- If an IP address that was used for another interface is specified, communication might not be possible until the ARP cache of external devices, such as routers and other servers, is updated.
- You cannot specify an IPv6 address.
- You cannot specify an IP address in the following networks:

  - 127.0.0.0 to 127.255.255.255
  - The network that contains the IP address set for the maintenance port
    You can use the `pmctl` command to check the network that contains the IP address set for the maintenance port.
  - The network that contains the IP address set for the heartbeat port
    You can use the `clstatus` command to check the network that contains the IP address set for the heartbeat port.

Note:

> You cannot change or delete the settings associated with an interface to which a virtual IP address has been added by using this command until all the virtual IP addresses are deleted with the `altipdel` command.

Options and arguments

`-s` [*virtual-IP-address1a*[,*virtual-IP-address1b*...]]:[*virtual-IP-address2a*[,*virtual-IP-address2b*...]]

> Specify this by using a colon (:) to connect the virtual IP address of the resource group on the node that you are logged into and the virtual IP address of the resource group on the other node. Use commas (,) to separate multiple IP addresses specified for a resource group.
>
> Be sure to specify a virtual IP address for at least one of the resource groups on the nodes.

interface

> Specify the name of the port to which the interface is set.
>
> You can specify the following port names. Specify an integer of 0 or more for *number*.

  - `eth` *number*
  - `agr` *number*
  - `rdn` *number*
  - `xgbe` *number*

> If a tagged VLAN is used, specify it in the format below. Note that the range of VLAN IDs you can specify is from 1 to 4094.
>
> *port-name*.*VLAN-ID*

Return values

Table 2-3 Return values of the altipadd command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 66[#], 70, 71[#], 74, 75	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
66[#], 71[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#
   The command ended abnormally due to multiple causes.

Example

To add virtual IP addresses to the data port `eth12`

- The addresses to be added to the node on which the command will be executed are `192.168.5.100` and `192.168.5.101`.
- The addresses to be added to the other node are `192.168.5.102` and `192.168.5.103`.

```
$ sudo altipadd -s 192.168.5.100,192.168.5.101:192.168.5.102,192.168.5.103
eth12
```

altipdel (Delete added virtual IP addresses)

Synopsis
```
altipdel -s [virtual-IP-address1a[,virtual-IP-address1b...]]:
   [virtual-IP-address2a[,virtual-IP-address2b...]]
   [-f] [-V] interface
altipdel --all [-f] [-V]
altipdel -h
```

Description

This command deletes virtual IP addresses added with the `altipadd` command.

Before executing this command, make sure that the OSs on both nodes are running and that the cluster and the resource groups on both nodes are running normally or are stopped. Be sure to notify the clients using virtual IP addresses in advance that they will be deleted.

Options and arguments

`--all`

Specify this to delete all virtual IP addresses that have been added by using the `altipadd` command.

`-f`

Specify this to prevent a confirmation message from appearing.

`-s` [*virtual-IP-address1a*[,*virtual-IP-address1b*...]]:[*virtual-IP-address2a*[,*virtual-IP-address2b*...]]

Specify this by using a colon (`:`) to connect the virtual IP address of the resource group on the node that you are logged into and the virtual IP address of the resource group on the other node. Use commas (`,`) to separate multiple IP addresses specified for a resource group.

Be sure to specify a virtual IP address for at least one of the resource groups on the nodes.

`-V`

Specify this to display the progress of the deletion processing.

interface

Specify the name of the port to which the interface is set.

If a tagged VLAN is used, specify it in the format below.

port-name.*VLAN-ID*

Return values

Table 2-4 Return values of the altipdel command

Return value	Description
0	Normal termination
1[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
1[#], 10, 66[#], 70, 71[#], 74, 75	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
66[#], 71[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

altiplist (Display added virtual IP addresses)

Synopsis

```
altiplist [--del delimiter] [interface]
altiplist -h
```

Description

Displays a list of the virtual IP address added with the `altipadd` command.

Options and arguments

`--del` *delimiter*

Specify this when you want to separate virtual IP addresses with a delimiter made up of alphanumeric characters, symbols, or spaces.

interface

To view information about a specific interface, specify the name of the corresponding port.

If a tagged VLAN is used, specify it in the format below.

port-name.VLAN-ID

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-5 Information displayed when executing the altiplist command

Item	Description
Interface	Displays information about the interface.

Item	Description
	If a tagged VLAN is used, information is displayed in the following format: `port-name.VLAN-ID`
node-number(*host-name*)[#]	Displays information about the node you are logged in to in the cluster. Information is displayed in the following format: `node-number(host-name)`
`Service IP addr`[#]	Displays the virtual IP addresses of the node you are logged in to. A hyphen (-) is displayed when no virtual IP addresses have been added by using the `altipadd` command.
node-number(*host-name*)[#]	Displays information about the other node in the cluster. Information is displayed in the following format: `node-number(host-name)`
`Service IP addr`[#]	Displays the virtual IP addresses of the other node in the cluster. A hyphen (-) is displayed when no virtual IP addresses have been added by using the `altipadd` command.

\#

   Only virtual IP addresses added by using the `altipadd` command are displayed.

Return values

Table 2-6 Return values of the altiplist command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10, 70, 71`[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`71`[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Command Reference

Return value	Description
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

arcactmigctl (Settings related to the Active File Migration function)

Synopsis (for cluster configurations)

```
arcactmigctl --file-system file-system-name
    --stabilize {enable|disable}
arcactmigctl --file-system file-system-name
    --work-space {device-file-name[,device-file-name...]|remove|
recovery}
arcactmigctl [--file-system file-system-name]
```

Synopsis (for single node configurations)

```
arcactmigctl --file-system file-system-name
    --stabilize {enable|disable}
arcactmigctl --file-system file-system-name
    --work-space {[+]capacity|remove|recovery}
arcactmigctl [--file-system file-system-name]
```

Synopsis (to reference the command syntax)

```
arcactmigctl -h
```

Description

Changes the settings for the Active File Migration function. You can also use the command to view the current setting. You cannot change the settings if migration is in progress.

Options and arguments

`--file-system` *file-system-name*

Specify the name of the target file system. If you specify only this option, the current settings for the target file system are displayed.

`--stabilize {enable|disable}`

Specify whether to use the Active File Migration function.

Note that using the Active File Migration function might negatively affect performance during file system accesses.

enable

Specify this if you want to use the Active File Migration function. The default is `enable`.

`disable`

Specify this if you do not want to use the Active File Migration function. Note that this setting cannot be specified if the Large File Transfer function is enabled.

`--work-space {`*`device-file-name`*`[,`*`device-file-name`*`...]|remove| recovery}`

The above syntax is for cluster configurations.

Specify the work space that is required to use the Active File Migration function and Large File Transfer function. If you specify a work space for this option, the `--stabilize` option is also set as `enable`.

`device-file-name``[,`*`device-file-name`*`...]`

Specify the LU number that is used for the work space. For example, if the device file path is `/dev/enas/luXX`, specify `luXX`. When specifying multiple items, separate each item with a comma (`,`). You can specify a maximum of 128 device files. Make sure that the total number of device files that constitute the work space and file system does not exceed 256. Note that we recommend that you specify the total size of the device files so that the 10GB.

`remove`

Specify this to remove the setting of the work space. Note that this setting cannot be specified if the Large File Transfer function is enabled.

`recovery`

Specify this if a failure occurs in the configuration process for the work space.

`--work-space {[+]`*`capacity`*`|remove|recovery}`

The above syntax is for single-node configurations.

Specify the work space that is required to use the Active File Migration function and Large File Transfer function. If you specify a work space for this option, the `--stabilize` option is also set as `enable`.

`[+]`*`capacity`*

Specify the capacity of the work space (unit: GB). To specify the overall capacity, specify the capacity without (+). To specify the storage capacity to be added by each expansion, specify the capacity with (+). Make sure that the capacity of the work space does not exceed 1,048,576 GB.

`remove`

Specify this to remove the setting of the work space. Note that this setting cannot be specified if the Large File Transfer function is enabled.

`recovery`

Specify this if a failure occurs in the configuration process for the work space.

The recommended value for the capacity of the work space differs depending on the capacity of the file system. For details about the recommended value of a work space, see the *Installation and Configuration Guide*.

In addition, if you omit all options, the current setting details of all file systems that are mounted on the node on which the command was executed will be displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-7 Information displayed when executing the arcactmigctl command

Item	Description
File system	Displays the file system name.

File stabilization	Displays the setting status of the Active File Migration function.
	
	`Enable`
	
	    The Active File Migration function is enabled.
	
	`Disable`
	
	    The Active File Migration function is disabled.
	
	`Error`
	
	    An error occurred in the work space or the resource group has stopped.
	
	`-`
	
	    Displayed when no work space has been set.

Work space	In a cluster configuration, the device files that constitute the work space is displayed in hexadecimal notation. In a single-node configuration, the capacity of the work space is displayed (units: GB). If the work space is not set, a hyphen (-) is displayed. If `(Error)` is displayed at the end, the processing for configuring the work space might have been interrupted. Execute the `arcactmigctl` command with the `--work-space recovery` option.
Used work space	The usage of the work space is displayed in the following format: `used-work-space unit (work-space-usage%)` If the used size of the work space cannot be obtained, a hyphen (-) is displayed.

Return values

Table 2-8 Return values of the arcactmigctl command

Return value	Description
0	Normal termination
1, 2#, 3	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2#, 11, 14, 15, 21, 22, 23, 24, 25, 26, 28, 29, 30, 54, 63, 64, 72, 74, 78, 82, 83, 84, 86, 87, 88, 89, 96	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
56, 57, 80	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
79, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
The command ended abnormally due to multiple causes.

arcconfedit (Configure the data migration or import)

Synopsis

```
arcconfedit [[--thread-min minimum-number-of-threads]
   [--thread-max maximum-number-of-threads]
   --thread-pool {archive|other|all}]
   [--retry-max maximum-number-of-retries]
   [--transfer-speed transfer-speed]
   [--comm-timeout communication-timeout-value]
   [--conn-timeout connection-timeout-value]
   [--low-speed minimum-transfer-speed]
   [--low-speed-time period-for-monitoring-transfer-speed]
   [--update-retry-max maximum-number-of-data-migration-retries-when-
migrating]
   [--update-retry-interval data-migration-retry-interval-when-
migrating]
   [--comm-compression {enable|disable}]
   [--file-server-retry-max maximum-number-of-retries]
   [--file-server-comm-timeout communication-timeout-value]
   [--migrate-replace-owner user-name]
   [--update-force-migration {enable|disable}]
   [--homedir-conflict-hold data-retention-period]
   [--versioning {everytime|onceaday}]
   [--stubbing-priority {normal|high}]
   [--stubbing-check {enable|disable}]
   [--reconn-interval waiting-time-for-reconnection]
   [--sharing-conflict-hold data-retention-period]
```

```
     [--sharing-conflict-dir {system|user}]
     [--cloud-vss-thread-max] number-of-read-ahead-threads
arcconfedit -h
```

Description

Configures the settings used for both data migrations from the HDI system to the HCP system and for data imports from other file servers to the HDI system.

You can specify the following items when migrating data to an HCP system:

- The maximum and minimum numbers of threads in each thread pool
- The number of read-ahead threads in which a file system uses the Volume Shadow Copy Service[#]
- The maximum number of retries for communication with the HCP system
- Transfer speed to the HCP system per thread
- The timeout value for communication with the HCP system
- Whether to compress HTTP messages for communication with HCP systems
- The timeout value for the connection with the HCP system
- The minimum transfer speed to the HCP system per thread
- The period for monitoring the transfer speed to the HCP system per thread
- The maximum number of data migration retries performed when migrating data to an HCP system
- The data migration retry interval when migrating data to an HCP system
- The setting for forcibly migrating data to the HCP system
- The period for retaining the data for which contention occurred between HDI systems that share data on an HCP system

#
   To access information about the previous versions of files that use the Volume Shadow Copy Service, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

You can specify the following items when importing data from another file server:

- The maximum and minimum numbers of threads in each thread pool
- The maximum number of retries for communication with another file server
- The timeout value for communication with another file server
- The alternative account that is assigned to files if the owner user names of the files cannot be resolved

Options and arguments

`--cloud-vss-thread-max` *number-of-read-ahead-threads*

Specify this option to set the number of read-ahead threads in which a file system uses the Volume Shadow Copy Service. Specify a value in the range of 1 to 2,000. Make sure that the value does not exceed the maximum number of threads in the thread pool that is not used for data migration to HCP. The default value is 60.

`--comm-compression {enable|disable}`

Specify whether HTTP messages are compressed for communication with HCP systems.

`enable`

Specify this to compress HTTP messages for communication with HCP systems. The default is `enable`.

`disable`

Specify this to not compress HTTP messages for communication with HCP systems.

`--comm-timeout` *communication-timeout-value*

Specify the timeout value for communication with the HCP system per thread in the range from 60 to 2,147,483,647 (units: seconds). The default value is 10800. If a timeout occurs while migrating a large file, specify a larger value.

`--conn-timeout` *connection-timeout-value*

Specify the timeout value for the connection with the HCP system per thread in the range from 60 to 2,147,483,647 (units: seconds). The default value is 300.

`--file-server-comm-timeout` *communication-timeout-value*

Specify the timeout value for communication with another file server per thread in the range from 60 to 2,147,483,647 (units: seconds). The default value is 300. If a timeout occurs during a data import from another file server because the directory being imported contains too many files, specify a larger value.

`--file-server-retry-max` *maximum-number-of-retries*

Specify, in the range from 0 to 5, the maximum retry count per thread for when communication cannot be established with another file server. The default value is 1. The system retries at 15-second intervals.

`--homedir-conflict-hold` *data-retention-period*

Specify, in the range from 1 through 14 (units: days), how long to retain data in the `.conflict` directory created in the home directory of a home-directory-roaming file system. The default value is 4.

Files deleted after the retention period expires cannot be viewed from other HDI systems. Therefore, specify the same value for each HDI system.

`--migrate-replace-owner` *user-name*

Specify the user name assigned as the alternate account for the files being imported if the user names for the owners of the files cannot be resolved.

The user name that you specify can have no more than 256 alphanumeric characters. However, if the domain the alternate account is assigned to is not the domain to which the HDI system is assigned, or if the HDI system is assigned to multiple domains, specify the domain name in addition to the user name in the following format:

domain-name\user-name

The domain name that you specify can have no more than 155 characters. The characters that you can use are alphanumeric characters and the following symbols: double quotation marks ("), apostrophes ('), asterisks (*), plus signs (+), commas (,), forward slashes (/), colons (:), semicolons (;), left angle brackets (<), equal signs (=), right angle brackets (>), question marks (?), left square brackets ([), backslashes (\), right square brackets (]), and vertical bars (|). Spaces are not permitted.

Note:

Specify this option when files could not be imported because a name could not be resolved by a domain controller or mapping file processing failed. If you use this option in other situations, unintended accounts might be assigned as the owners of files that you are importing.

After files with the alternate account assigned to them are imported, we recommend that you execute the command by specifying a null string ("" or '') as the value for this option to clear the alternate account setting. If you do not clear the setting, the previously set alternate account might be used unintentionally the next time a data import is performed.

`--low-speed` *minimum-transfer-speed*

Specify the minimum transfer speed to the HCP system per thread in the range from 0 to 2,147,483,647 (units: bytes per second). If the transfer speed to the HCP system falls below this minimum value, a timeout occurs. If `0` is specified for this value, a timeout will not occur, regardless of the transfer speed. The default value is 11,650. If a timeout occurs frequently because the network transfer speed is too slow, specify a smaller value.

`--low-speed-time` *period-for-monitoring-transfer-speed*

Specify the period for monitoring the transfer speed to the HCP system per thread in the range from 0 to 2,147,483,647 (units: seconds). If the transfer speed in this period falls below the minimum value specified in the `--low-speed` option, a timeout occurs for communication with the HCP system. If `0` is specified for this value, a timeout will not occur, regardless of the transfer speed. If the period specified in the `--comm-timeout` option is shorter than the period specified in this option, a timeout occurs based on the period specified in the `--comm-timeout` option. The default value is 180.

`--reconn-interval` *waiting-time-for-reconnection*

Specify the waiting time for reconnecting to the HCP system from 0 to 2,147,483,647 (units: seconds). To ensure that client access performance is not affected by repeated communication errors with the HCP system, if the waiting time has not elapsed since detection of a communication error, the attempt to connect to the HCP system ends with an error and does not make a new connection.

If the value of `0` is specified, a connection is made to the HCP system, even if no response was received from the HCP system. The default setting is `0`.

Note:

If you specify a value that is too low, the reconnection interval becomes too short and client access performance is affected. Therefore, we recommend that you specify a value larger than the value specified for the `--low-speed-time` option. Note, however, that if temporary communication errors are concentrated in a short period (for example, in cases where the HCP system is linked over the network), ensure that you specify a value of `60` or less, to eliminate situations in which clients are waiting for reconnection due to temporary communication errors.

`--retry-max` *maximum-number-of-retries*

Specify, in the range from 0 to 5, the maximum retry count for when communication cannot be established with the HCP system or when the HCP system returns an error message requesting a retry. The default value is 1. The first time communication cannot be established, the system waits 15 seconds before retrying. The second time, the system waits 30 seconds, and the third and subsequent times, the system waits 60 seconds.

`--sharing-conflict-hold` *data-retention-period*

Specify the duration for retaining data in the `.conflict` or `.conflict_longpath` directory created just below the mount point of the read-write-content-sharing file system, in the range from 1 to 365 (units: days). The default value is 4.

`--sharing-conflict-dir {system|user}`

Specify the directory in which a file in conflict with an update from a different location is saved when the operating the read-write-content-sharing file system.

`system`

Specify this to save a file in conflict with an update from a different location in the `.conflict` directory created just below the mount point of the file system.

`user`

Specify this to save a file in conflict with an update from a different location in the directory in which the file in conflict was originally stored. The default setting is `user`.

Hitachi Data Ingestor CLI Administrator's Guide

Note:

If the path length of a file in conflict with an update from a different location exceeds 187 characters, the file will not be saved in the directory in which the file in conflict was originally stored, but will be saved in the `.conflict_longpath` directory created just below the mount point of the file system. For details about the `.conflict_longpath` directory, see the *Installation and Configuration Guide*.

`--stubbing-check {enable|disable}`

Specify whether to enhance error checking before performing file stubbing.

`enable`

Specify this to enhance error checking before performing file stubbing. The default is `enable`.

`disable`

Specify this not to enhance error checking before performing file stubbing.

`--stubbing-priority {normal|high}`

Specify this to select the stubbing priority.

When I/O requests are received from a large number of clients at the same time or when the number of threads for migration is increased, the stubbing process might not be able to secure enough free disk space. In this case, we recommend that you increase the stubbing priority.

`normal`

Specify this to perform stubbing at the normal priority. The default is `normal`.

`high`

Specify this to increase the stubbing priority. With a higher priority, the stubbing process takes precedence over the processing of I/O requests from the clients.

`--thread-max` *maximum-number-of-threads*

Specify the maximum number of threads in the range from 1 to 2,000. The maximum number of threads must be equal to or larger than the minimum number of threads. The default value is 60. Change this setting to balance the load on the HCP system, the HDI system, the network, import-source servers during imports, recall processing, and data imports from other file servers.

Note:

Increasing the number of threads might reduce the time required for migration processing or recall processing, but on the other hand, might also increase the load on the entire system, including the network. Before you change this setting, take the load of the entire system into account.

`--thread-min` *minimum-number-of-threads*

> Specify the minimum number of threads in the range from 1 to 2,000. The minimum number of threads must be equal to or smaller than the maximum number of threads. The default value is 20. Change the setting to balance the load on the HCP system, the HDI system, the network, import-source servers during imports, recall processing, and data imports from other file servers.

`--thread-pool {archive|other|all}`

> Specify the type of thread pools whose maximum and minimum number of threads you want to change. This option must be specified when the `--thread-min` option and the `--thread-max` options are specified.

> `archive`
>
> > Thread pools used for data migrations to an HCP system

> `other`
>
> > Thread pools used for purposes other than data imports to an HCP system (the thread pools used for data migrations from another file server, recall processing, extending the retention period, or deleting files)

> `all`
> > Any type of thread pool

`--transfer-speed` *transfer-speed*

> Specify the transfer speed to the HCP system during migrations and recall processing per thread in the range from 0 to 134,217,728 (units: bytes per second). If `0` is specified, transfer speed is unlimited. The default value is 0.

> Note that this option adjusts the maximum amount of data that can be transferred over the network at a time; it does not adjust the performance of migrations or recall processing. For example, if the maximum number of threads set for `--thread-pool archive` is 60 and the maximum transfer speed set for `--transfer-speed` is 10 MB/s, then the amount of data that can be transferred over the network at one time is set to 600 MB/s or less, even though the performance of migrations will be considerably less than that value.

`--update-force-migration {enable|disable}`

> Specify whether a file that is being updated by a client when the system checks whether the file can be migrated is forcibly migrated to the HCP system.

> This option can be specified when the HCP system that is linked to is version 4.1 or later.

> When data is forcibly migrated, because the data is migrated while it is being updated, some user data might not be recoverable by restoring the data migrated to the HCP system. For this reason, files that are forcibly migrated are migrated again the next time a migration is performed. When data is forcibly migrated, the KAQM37384-W message is output. Files and directories that have been forcibly migrated can be viewed by

executing the `arcresultctl` command with the `--failedlist` option, or by viewing the **Task Information** tab of the **Migration Task** page in the Migration Tasks dialog box.

enable

Specify this to force data being updated to be migrated.

disable

Specify this to not migrate data that is being updated. The default is `disable`.

`--update-retry-interval` *data-migration-retry-interval-when-migrating*

Specify, in the range from 0 to 30 (units: seconds), the retry interval per thread for when data migration to an HCP system cannot be performed because files are being updated by clients. The default value is 5.

`--update-retry-max` *maximum-number-of-data-migration-retries-when-migrating*

Specify, in the range from 0 to 20, the maximum retry count per thread for when data migration to an HCP system cannot be performed because files are being updated by clients. The default value is 1.

`--versioning {everytime|onceaday}`

Specify this to set the timing at which to create a past version directories, if past versions of the files migrated to HCP are made accessible from the clients.

everytime

Specify this to create a directory every time migration is performed. The default is `everytime`.

onceaday

Specify this to create a directory only once a day, when the first migration of the day is performed.

If the migration task is executed more than once a day, you can retain past versions longer by changing the option from `everytime` to `onceaday`. For details about the execution interval of the migration task and the retention period of past versions, see the *Installation and Configuration Guide*.

If no options are specified, the command normally terminates without updating the definition file.

Return values

Table 2-9 Return values of the arcconfedit command

Return value	Description
0	Normal termination

Return value	Description
1, 2, 3, 4	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
66, 67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
13, 70, 71#, 73	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
71#	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Examples

To set the minimum number of threads in the thread pools used for data migrations to an HCP system to 10 and the maximum number of threads in the thread pools to 30:

```
$ sudo arcconfedit --thread-min 10 --thread-max 30 --thread-pool archive
```

To set the minimum transfer speed to the HCP system to 11,650 bytes per second and the period for monitoring the transfer speed to 180 seconds:

```
$ sudo arcconfedit --low-speed 11650 --low-speed-time 180
```

To set the period for monitoring the transfer speed to the HCP system to 250 seconds, and the waiting time for reconnection to 300 seconds:

```
$ sudo arcconfedit --low-speed-time 250 --reconn-interval 300
```

To set the maximum number of retries performed when migrating data to the HCP system to 10, and to set the retry interval to 20 seconds:

```
$ sudo arcconfedit --update-retry-max 10 --update-retry-interval 20
```

To set the maximum number of retries for communication with another file server to 3, and to set the timeout value to 150 seconds:

```
$ sudo arcconfedit --file-server-retry-max 3 --file-server-comm-timeout 150
```

arcconflist (Display the data migration or import)

Synopsis

```
arcconflist [-h]
```

Description

Displays the settings used for both data migrations from the HDI system to the HCP system and for data imports from other file servers to the HDI system.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-10 Information displayed when executing the arcconflist command

Item	Description
Thread configuration	Displays thread information.
archive	Displays the settings of the thread pools used for data migrations to an HCP system. Thread max The maximum number of threads Thread min The minimum number of threads
other	Displays the settings of the thread pools used for purposes other than data migrations to an HCP system (the thread pools used for data imports from another file server, recall processing, extending the retention period, or deleting files). Thread max The maximum number of threads Thread min The minimum number of threads
Cloud VSS thread max	Displays the number of read-ahead threads in which a file system uses the Volume Shadow Copy Service.
HCP communication configuration	Displays information about communication with the HCP system.
Retry max	Displays the maximum retry count for when the HCP system cannot be connected or when the HCP system returns an error message requesting a retry.

Item	Description
Transfer speed(byte/s)	Displays the transfer speed to the HCP system per thread (units: bytes per second).
Timeout(s)	Displays the timeout value for communication with the HCP system per thread (units: seconds).
Connect timeout(s)	Displays the timeout value for the connection with the HCP system per thread (units: seconds).
Low speed(byte/s)	Displays the minimum transfer speed to the HCP system per thread (units: bytes per second).
Low speed time(s)	Displays the period for monitoring the transfer speed to the HCP system per thread (units: seconds).

Compression	Displays the setting for the compression of HTTP messages for communication with HCP systems.
	enable
	    Displayed if HTTP messages are compressed for communication with HCP systems.
	disable
	    Displayed if HTTP messages are not compressed for communication with HCP systems.

Reconnection interval(s)	Displays the waiting time for reconnecting to the HCP system (units: seconds).
Migration configuration	Displays information about migrations when data is migrated to the HCP system.
Update retry max	Displays the maximum number of update retries per thread for when data migration to the HCP system cannot be performed.
Update retry interval(s)	Displays the update retry interval per thread for when data migration to the HCP system cannot be performed (units: seconds).

Update force migration	Displays the setting for forcibly migrating data to the HCP system.
	enable
	    Displayed when data that is currently being updated by a client can be forcibly migrated to the HCP system.
	disable
	    Displayed when data that is currently being updated by a client cannot be forcibly migrated to the HCP system.

Versioning configuration	Displays information about the file version restore function.
Versioning	Displays the timing for when a past version directories is created. everytime This is displayed if a directory is created every time the migration task is executed. onceaday

Command Reference

Item	Description
	This is displayed if a directory is created only once a day, when the first migration task of the day is performed.
Stubbing configuration	Displays information about the file stubbing.
Priority	Displays the stubbing priority. `normal` This is displayed when the stubbing is performed with normal priority. `high` This is displayed when the stubbing is performed with a priority higher than normal.
Stubbing check	Displays whether error checking is enhanced before file stubbing is performed. `enable` This is displayed if error checking is enhanced before file stubbing is performed. `disable` This is displayed if error checking is not enhanced before file stubbing is performed.
Home-directory-roaming configuration	Displays information about the home-directory-roaming file system.
Hold interval (days)	Displays how long to retain data in the `.conflict` directory created in the home directory of the home-directory-roaming file system (units: days).
File Server communication configuration	Displays information about communication when importing data from another file server.
Retry max	Displays the maximum number of retries per thread for when communication cannot be established with another file server.
Timeout(s)	Displays the timeout value for communication with another file server per thread (units: seconds).
Migrate replace owner	Displays the user name assigned as the alternate account if the user names of the owners of the files being imported cannot be resolved. If no alternate account is used, `Do not use` is displayed.
Read-write-content-sharing configuration	Displays information about the read-write-content-sharing file system.
Hold interval (days)	Displays the duration for retaining data in the `.conflict` or `.conflict_longpath` directory created just below the mount point of the file system (units: days).
Conflict directory	Displays the directory in which a file in conflict with an update from a different location is saved. `system`

Item	Description
	This information is displayed when a file in conflict with an update from a different location is saved in the `.conflict` directory created just below the mount point of the file system.
	`user`
	This information is displayed when a file in conflict with an update from a different location is saved in the directory in which the file in conflict was originally stored.

Return values

Table 2-11 Return values of the arcconflist command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
66, 67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arccorrection (Rebuild management information for a file system)

Synopsis

```
arccorrection [-t {update-only|all}] [--background] [-V]
   --file-system file-system-name
arccorrection -h
```

Description

This command rebuilds the task management information (about migration task) for a file system, and the autocommit management information for a WORM file system.

When you execute this command, all the files in the file system are retrieved and the management information is rebuilt. Therefore, the processing time increases according to the number of files in the file system. Access to the file system might be slowed down during retrieval, so you must execute this command when the load on the entire system is light.

The occasions to execute this command are as follows:

- If management information loses its integrity, execute this command to recover that information. Execute this command when instructed to do so in the description about error message handling, or if you are instructed by maintenance personnel. Also execute this command if power is interrupted, because the management information might be incomplete.

- If a failure in the HCP results in lost HCP data, execute this command with the `-t all` option specified to re-migrate all the data in the file system.

If a failover or power failure occurs while management information is being rebuilt, processing is paused. Re-mount the file system to automatically continue processing.

Options and arguments

`--background`

Specify this option to rebuild management information in the background.

`--file-system` *file-system-name*

Specify the name of the file system whose management information is to be rebuilt. The specified file system must be mounted as read-write.

`-t {update-only|all}`

Specify the data to be migrated to the HCP system if you want to rebuild management information for a file system whose data has been migrated to the HCP system. If this option is not specified, only data that has not been migrated to the HCP system after the data is created or updated is migrated.

Specify `update-only` to rebuild management information for a home-directory-roaming file system.

`update-only`

Specify this to migrate only data that has not been migrated to the HCP system after the data is created or updated.

`all`

Specify this to migrate all data in HDI file systems to recover HCP data.

Because all the data is migrated, initial migration (after rebuilding the management information) takes more time. Additionally, attempting to access files in old directories while HCP data is lost will result in an error. Therefore, if you execute this command with this option specified, all the old directories are deleted.

Notes:

- If stub processing is enabled for a file system that migrates data to the HCP system (that is, the threshold at which stub processing is performed is not set to 0 GB), stub files and directories cannot be restored. Attempting to migrate or access stub files without the HCP data will result in an error.

- If you execute the `arccorrection` command with the `-t all` option specified when the Large File Transfer function is enabled, processing might take a long time. Therefore, if you specify the `-t all` option, before executing the `arccorrection` command, use the `arclftctl` command to disable the Large File Transfer function and use the `arcmigedit` command to specify the settings so that migration is not stopped.

`-V`

Specify this to display the progress of rebuilding management information. Note that the `-V` option is ignored if both the `-V` and `--background` options are specified.

Note:

If this command is executed when either of the statements below is true, processing completes successfully, but management information is not rebuilt. Wait a while and retry the operation.

- Management information is being rebuilt.

- Management information has been rebuilt for the file system whose data was migrated to the HCP system, but stub processing has not been performed yet.

- Files or directories that have one or more line feed codes in their paths are not included in the tasks. To identify the files or directories that are not included in the tasks, specify the `-regex` option from an NFS client, and then execute the `find` command.

When using the `find` commands:

```
find ./  -regex ".*/\.history" -prune -or -regex ".*/\.snaps" -prune -
or -regex ".*/\.lost\\+found" -prune -or -regex ".*/\.system_gi" -
prune -or -regex ".*[^M
].*" -print
```

Line feed codes are the CR code and LF code. In the above example, `^M` indicates the CR code. Type **Ctrl** + **v** and then **Ctrl** + **m** to display `^M`. The LF code is used after `^M`. Type **Ctrl** + **v** and then **Ctrl** + **j** to display it.

Return values

Table 2-12 Return values of the arccorrection command

Return value	Description
0	Normal termination

Return value	Description
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 4, 8, 10, 12, 15, 68	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
60, 65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
66, 97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To specify the `--background` option to rebuild the management information in the background:

```
$ sudo arccorrection --background --file-system fs1
```

arccustomschlctl (Settings related to custom schedules of the file version restore functionality)

Synopsis
```
arccustomschlctl [-y] {--respective|--cumulative}
arccustomschlctl
arccustomschlctl -h
```

Description

Specify the method used to select the past-version directories to be retained when custom schedules of the file version restore functionality are used. The command can also be used to view the current setting. For details about how to select the past-version directories to be retained, see the *Installation and Configuration Guide*.

The values specified for this command apply to the entire system. In cluster configurations, this command also executes processing on the other node in the cluster.

Note:

    To change the method used to select the past-version directories to be retained, make sure that you perform the following procedure:

1. Use the GUI to disable the migration task schedules for all file systems that use custom schedules.

2. Use the `arccustomschlctl` command to change the method used to select the past-version directories to be retained.

3. Use the GUI or the `fsedit` command to change the settings of custom schedules as needed.

When you use the `fsedit` command, make sure that you check the retention period of past-version directories and specify at least the recommended value for the days calculated by the formula. For details about the formula for recommended values of the retention period, see the *Installation and Configuration Guide*.

4. Use the GUI to reset the migration task schedules.

Options and arguments

`--cumulative`

> Specify this to select the past-version directories to be retained in cumulative mode.

`--respective`

> Specify this to select the past-version directories to be retained in respective mode. By default, respective mode is selected.

If you omit all options, the current setting is displayed.

Displayed information

The following table lists the information displayed when this command is executed.

Table 2-13 Information displayed when the arccustomschlctl command is executed

Item	Description

`Custom schedule mode`	Displays the method used to select the past-version directories to be retained when the custom schedules is used.
	
	`Respective`
	
	    The respective mode.
	
	`Cumulative`
	
	    The cumulative mode.

Return values

Table 2-14 Return values of the arccustomschlctl command

Return value	Description
`0`	Normal termination

Return value	Description
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
70, 71	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcfrecall (Recalling a file)

Synopsis

```
arcfrecall [-q] [--background] --file file-path
arcfrecall --status --file file-path
arcfrecall -h
```

Description

Recalls the data of a file system where the data from another HDI system is referenced as read-only, before a client accesses the file. The data is recalled before a client accesses the file. You can also use the command to display information about recall processing for a specified file. After this command terminates recall processing, use the `--status` option to check the progress and confirm that the data is recalled.

For details on recalling to HDI, see the *Installation and Configuration Guide*.

If recall processing does not terminate after an excessive amount of time, execute the command with the `--status` option specified to check the progress of recalling the data. The time required to recall the data varies depending on the network environment and other factors.

You can interrupt the command processing by pressing **Ctrl** + **C**, unless the command is executed with the `--background` option specified.

Options and arguments

`--background`
    Specify this option to recall the file in the background.
    You cannot specify this option when the `--status` option is specified.

`--file` *file-path*

Specify the absolute path beginning with `/mnt/`.

`-q`

Specify this option to suppress the output of status messages.

You cannot specify this option when the `--status` option is specified.

`--status`

Specify this option to display the size of the file to be recalled and the amount of recalled data.

This option cannot be specified when the `--background` option or `-q` option is specified.

Displayed information

The following table lists the information displayed when you specify the `--status` option and execute the command.

Table 2-15 Information displayed when specifying the --status option and executing the arcfrecall command

Item	Description
`Status of file recall`	Displays whether the specified file has been recalled. `not_finished` The file has not been recalled yet. `finished` The file has been recalled.
`File size`	Displays the file size.
`Disk size`	Displays the amount of recalled data.

Return values

Table 2-16 Return values of the arcfrecall command

Return value	Description
`0`, `6`[#]	Normal termination
`1`, `2`, `3`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`5`, `8`, `10`, `65`, `72`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

> This value returns if the command executed with the `--status` option specified displays `not_finished` for `File recall status`.

arcfstatus (Display the stub status of a file)

Synopsis

```
arcfstatus file-path
arcfstatus -h
```

Description

Displays whether the file is a stub file.

Options and arguments

file-path
> Specify the absolute path for the target file.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-17 Information displayed when executing the arcfstatus command

Item	Description

Migrated	Displays whether the file is a stub file.
	
	 `Yes`
	
	      The file is a stub file.
	
	 `No`
	
	      The file is not a stub file. Note that, even if the file has been migrated, `No` is displayed when the file is not a stub file.

Return values

Table 2-18 Return values of the arcfstatus command

Return value	Description
0	Normal termination (when the file is not a stub file)

Return value	Description
1	Normal termination (when the file is a stub file)
3, 7, 8	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
9, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

archcpdel (Delete information about the migration destination HCP system)

Synopsis

```
archcpdel [--replica-host]
archcpdel -h
```

Description

Deletes the information about the HCP system that is set as the migration destination.

Options and arguments

`--replica-host`

Specify this option to delete only the replica HCP host name from the information about the HCP system. If this option is not specified, the command deletes all the information about the HCP system that has been set.

Return values

Table 2-19 Return values of the archcpdel command

Return value	Description
0	Normal termination

Return value	Description
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 12#, 70, 71	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
12#	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
66, 67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

archcpget (Display information about the migration destination HCP system)

Synopsis

```
archcpget
archcpget --migrate-info [--file-system file-system-name]
archcpget -h
```

Description

Displays the information about the HCP system that is set as the migration destination.

Options and arguments

--file-system *file-system-name*

Specify the file system name to view the migration-destination HCP information for the specific file system.

--migrate-info

Specify this to view information about a namespace, along with information about the migration-destination HCP system.

Displayed information

The following table lists the information displayed when you execute the `archcpget` command.

Table 2-20 Information displayed when executing the archcpget command (without the --migrate-info option)

Item	Description
HCP host name	Displays the HCP host name (FQDN).
Replica HCP host name	Displays the replica HCP host name (FQDN). Nothing is displayed if the replica HCP host name has not been set.
HCP tenant name	Displays the HCP tenant name.
HCP account user	Displays the user name of the data access account used to access all namespaces in the tenant.
External host	Displays the host name or IP address that has been made external and is used to connect to the HCP system.
External replica host	Displays the host name or IP address that has been made external and is used to connect to the replica HCP system.

The following table lists the information displayed when you specify the `--migrate-info` option and execute the command.

Table 2-21 Information displayed when executing the archcpget command (with the --migrate-info option)

Item	Description
HCP host name	Displays the HCP host name (FQDN).
Replica HCP host name	Displays the replica HCP host name (FQDN). Nothing is displayed if the replica HCP host name has not been set.
HCP tenant name	Displays the HCP tenant name.
HCP account user	Displays the user name of the data access account used to access all namespaces in the tenant.
External host	Displays the host name or IP address that has been made external and is used to connect to the HCP system.
External replica host	Displays the host name or IP address that has been made external and is used to connect to the replica HCP system.
namespace	Displays the HCP namespace name.
Filesystem	Displays the file system name.
Total disk capacity(GB)	Displays the file system capacity in GB.
Versioning	Displays whether to allow clients to access the past version of files migrated to the HCP system.

Item	Description

	`Use`
	
	Displayed if the clients are allowed to access the past version of files migrated to the HCP system.
	
	`Do not use`
	
	Displayed if the clients are not allowed to access the past version of files migrated to the HCP system.

`Period to hold(day)`	Displays the retention period for the past version of files migrated to the HCP system. If the clients are not allowed to access the past version of files migrated to the HCP system, `--` is displayed.

Return values

Table 2-22 Return values of the archcpget command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`2, 10, 70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`66, 67`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

archcpset (Set information about the migration destination HCP system)

Synopsis

```
archcpset [--host host-name-of-the-HCP --tenant tenant-name
   --user-name user-name --password password
    [--ex-host host-name-that-has-been-made-external-and-is-used-to-
    connect-to-the-HCP]]
   [--replica-host host-name-of-the-replica-HCP
    [--ex-replica-host host-name-that-has-been-made-external-and-is-
    used-to-connect-to-the-replica-HCP]]
archcpset -h
```

Description

Sets the information about the migration destination HCP system. If HCP information is already set, the command overwrites the information.

The settings for the `archcpset` command can be specified either interactively or by choosing options. If you want to specify settings interactively, execute the command without any options.

The following table lists the information items that can be set interactively.

Table 2-23 Information that can be specified interactively for the archcpset command

Item	Description
`HCP host name`	Specifies the HCP host name (FQDN).
`Replica HCP host name (If replica HCP is not used, simply press the [Enter] key.)`	Specifies the replica HCP host name (FQDN). If you do not want to set the replica HCP host name, specify nothing, and press the **Enter** key.
`HCP tenant name`	Specifies the HCP tenant name.
`HCP account user`	Specifies the user name of the data access account to be used to access all namespaces in the tenant.
`HCP account password`	Specifies the password of the data access account to be used to access all namespaces in the tenant.
`confirm password`	Specifies the password of the data access account to be used to access all namespaces in the tenant again.
`External HCP host name (To communicate with HCP directly, press the [Enter] key.)`	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. If you do not want to set the HCP host name, specify nothing, and press the **Enter** key.
`External Replica HCP host name (To communicate with the replica HCP directly, press the [Enter] key.)`	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. If you do not want to set the replica HCP host name, specify nothing, and press the **Enter** key.

Note:
   The character strings you specify for `HCP account password` and `confirm password` are not displayed.

Options and arguments

`--ex-host` *host-name-that-has-been-made-external-and-is-used-to-connect-to-the-HCP*

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.

`--ex-replica-host` *host-name-that-has-been-made-external-and-is-used-to-connect-to-the-replica-HCP*

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.

`--host` *host-name-of-the-HCP*

Specify the HCP host name (FQDN).

`--password` *password*

Specify the password of the data access account to be used to access all namespaces in the tenant.

`--replica-host` *host-name-of-the-replica-HCP*

Specify the replica HCP host name. If you specify only this option when no HCP information has been set, the command results in an error.

`--tenant` *tenant-name*

Specify the HCP tenant name.

`--user-name` *user-name*

Specify the user name of the data access account to be used to access all namespaces in the tenant.

Return values

Table 2-24 Return values of the archcpset command

Return value	Description
0	Normal termination
1, 2[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2[#], 3, 4, 5, 8, 10, 11, 12[#], 15, 16, 17, 18, 20, 68[#], 70, 71[#], 74, 75, 76[#], 77	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
12[#], 71[#], 72, 73, 76[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
65, 66, 67, 68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation.

Return value	Description
	If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Examples

To interactively set HCP information according to the following conditions:

- The HCP host name (FQDN) is hcp.example.com.
- The replica HCP host name (FQDN) is hcp.example2.com.
- The HCP tenant name is tenant01.
- The user name of the data access account to be used to access all namespaces in the tenant is user01.
- The password of the data access account to be used to access all namespaces in the tenant is hcppass (not displayed).
- The IP address that has been made external and is used to connect to the HCP system is 123.45.67.89.
- The IP address that has been made external and is used to connect to the replica HCP system is 123.45.67.99.

```
$ sudo archcpset
HCP host name : hcp.example.com
Replica HCP host name (If replica HCP is not used, simply press the
[Enter] key.) : hcp.example2.com
HCP tenant name : tenant01
HCP account user : user01
HCP account password :
confirm password :
External HCP host name (To communicate with HCP directly, press the
[Enter] key.) : 123.45.67.89
External replica HCP host name (To communicate with the replica HCP
directly, press the [Enter] key.) : 123.45.67.99
```

To set hcp.example2.com as the replica HCP host name:

```
$ sudo archcpset --replica-host hcp.example2.com
```

archdctl (managing roaming for home-directory-roaming file systems)

Synopsis

```
archdctl [-c] {--roaming|--status} --file-system file-system-name
    [--dir directory-name]
```

```
archdctl [-y] --del --file-system file-system-name
    --dir directory-name
archdctl -h
```

Description

This command sets a directory to be subject to roaming, and displays whether the directory is subject to roaming.

A directory specified in the command must be immediately under the mount point of the home-directory-roaming file system.

Options and arguments

-c

Specify this option to output the current settings, separated by colons (:). Specify this together with the --status option.

--del

Specify this option to delete the home-directory. Specify the argument only when contention for updating home directories among HDIs occurs.

--dir *directory-name*

Specify a directory name. Note that the following directory names cannot be specified because they are used by the system: `.conflict`, `.conflict_longpath`, `.snaps`, `.history`, `.arc`, `.system_gi`, `.system_reorganize`, `lost+found`, and `.lost+found`. If you omit this option, all directories immediately under the mount point of the home-directory-roaming file system, excluding the directories used by the system, become subject to roaming.

--file-system *file-system-name*

Specify the name of the file system in which the target directory exists.

--roaming

Specify this option to set the directory to be subject to roaming.

--status

Specify this option to display whether the directory is subject to roaming.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-25 Information displayed when executing the archdctl command

Item	Description
Start Time	The date and time that the command processing started is displayed in the following format: *date* (format: *YYYY/MM/DD*) *time* (format: *hh*:*mm*:*ss*) (*time-zone*)

Item	Description
Directory	The target directory name is displayed. This item is displayed when the `--status` option is specified.

Roaming	Whether the target directory is subject to roaming is displayed. This item is displayed when the `--status` option is specified.
	
	`on`
	
	    The directory is subject to roaming.
	
	`off`
	
	    The directory is not subject to roaming.

End Time	The date and time that the command processing finished is displayed in the following format: *date* (format: *YYYY/MM/DD*) *time* (format: *hh:mm:ss*) (*time-zone*)

Return values

Table 2-26 Return values of the archdctl command

Return value	Description
0	Normal termination
1, 2	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
3, 5, 8, 10, 11, 68, 69	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66, 67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arclftctl (Settings related to the Large File Transfer function)

Synopsis

```
arclftctl --file-system file-system-name
    {[--enable|--disable] [--lower-limit minimum-file-size]
     [--transfer-part-min minimum-division-size]}
arclftctl [--file-system file-system-name]
arclftctl -h
```

Description

Changes the settings for the Large File Transfer function. You can also use the command to view the current setting.

Note that the recommended value for the work space capacity depends on the file system capacity and whether the Large File Transfer function is used.

For details about the Large File Transfer function and the recommended value for the work space capacity, see the *Installation and Configuration Guide*.

Options and arguments

`--disable`

Specify this option to disable the Large File Transfer function.
Notes:

- In a cluster configuration, after disabling the Large File Transfer function, if you need to reduce the work space capacity when using the Active File Migration function, re-specify the LUs to be used for the work space.

- When you change the settings to disable the Large File Transfer function, the differential data of the files migrated by the function is initialized. Therefore, after you enable the function again, all of the contents of those files are migrated during the first migration.

`--enable`

Specify this option to enable the Large File Transfer function.
This option can be specified if the target file system satisfies the following conditions:

- The file system has a capacity of 100 GB or more.
- The Active File Migration function is enabled.
- The file system is not a home-directory-roaming file system.
- The file system is not a read-write-content-sharing file system.
- The file system does not reference data in another HDI system in read-only mode.

`--file-system` *file-system-name*

Specifies the name of the target file system. If only this option is specified, the command displays the current settings of the target file system.

`--lower-limit` *minimum-file-size*

Specifies the lower threshold for the size of files to which the Large File Transfer function is applied. A value in the range from 50 to 5,242,880 (unit: MB) can be specified. The initial setting is `100`.

Any files that are larger than the value specified for this option are migrated by the Large File Transfer function.

> **Note:** The Large File Transfer function is not applied to stubbed files. Therefore, after executing this command, use the arcresidentpolicyset command to make sure that the minimum size of files to be cache-resident (*B*) is not more than the value specified for this option (*A*).
>
>   B <= A

`--transfer-part-min` *minimum-division-size*

> Specifies the size into which files transferred by using the Large File Transfer function are divided. A value in the range from 5 to 5,120 MB (in multiples of 5) can be specified. The initial setting is `5`.
>
> The value specified for this option is compared with the division file corresponding to the file size in the following table, and whichever is larger is the size that is actually used as the division size during migration.
>
> Note that the division size specified for this option must be larger than the division size corresponding to the file size specified for the `--lower-limit` option.

File size (m : File size)	Division size
50 MB <= *m* <= 50,000 MB	5 MB
50,000 MB < *m* <= 100,000 MB	10 MB
100,000 MB < *m* <= 200,000 MB	20 MB
200,000 MB < *m* <= 400,000 MB	40 MB
400,000 MB < *m* <= 800,000 MB	80 MB
800,000 MB < *m* <= 1,600,000 MB	160 MB
1,600,000 MB < *m* <= 3,200,000 MB	320 MB
3,200,000 MB < *m* <= 5,242,880 MB	640 MB

If all options are omitted, the command displays the current settings of all file systems on the target node.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-27 Information displayed when executing the arclftctl command

Item	Description
`File system`	Displays the file system name.

`Large file transfer`	Displays whether the Large File Transfer function is enabled.
	`Enable`
	    The Large File Transfer function is enabled.
	`Disable`

Item	Description
	The Large File Transfer function is disabled.
Lower limit	Displays the lower threshold value for the size of files to which the Large File Transfer function is applied (unit: MB).
Transfer part min	Displays the minimum division size of files to which the Large File Transfer function is applied (unit: MB).

Return values

Table 2-28 Return values of the arclftctl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 5, 8, 10, 12, 14, 15, 16, 23, 63, 64, 70, 71, 86	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcmigctl (Enable migration tasks)

Synopsis

```
arcmigctl --file-system file-system-name
    --task task-name {--enable|--disable}
arcmigctl -h
```

Description

Specifies whether to enable migration tasks.

Options and arguments

```
--disable
```

Specifies whether to disable migration tasks.

`--enable`
Specifies whether to enable migration tasks.

`--file-system` *file-system-name*
Specify the name of the target file system.

`--task` *task-name*
Specify the name of the target migration task name.

Return values

Table 2-29 Return values of the arcmigctl command

Return value	Description
0	Normal termination
1, 2#, 3	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2#, 5, 8, 10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
67, 68	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
The command ended abnormally due to multiple causes.

arcmigdel (Delete migration tasks)

Synopsis

```
arcmigdel --file-system file-system-name
    [--task task-name [--policy policy-ID]]

arcmigdel -h
```

Description

Deletes migration tasks, or alternatively, individual policy sets in a migration task.

A migration task cannot be deleted if the target file system is a home-directory-roaming file system or read-write-content-sharing file system, or if the migration task was created as a default setting.

Options and arguments

`--file-system` *file-system-name*
Specify the name of the target file system.

`--policy` *policy-ID*
Specify this option to delete individual migration policy sets in a target migration task. If you omit this option and the `--task` option, all migration tasks of the target file system are deleted. If you omit only this option, the migration task specified in the `--task` option is deleted.

`--task` *task-name*
Specify the name of the target migration task.

If you omit this option and the `--policy` option, all migration tasks of the target file system are deleted.

Return values

Table 2-30 Return values of the arcmigdel command

Return value	Description
0	Normal termination
2, 3, 5, 8, 10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcmigedit (Change the settings of a migration task)

Synopsis
```
arcmigedit --file-system file-system-name
    --task task-name
    [--priority {high|middle|low|priority-level}]
    [--comment comment]
arcmigedit --file-system file-system-name
    --task task-name
    --schedule
```

```
       --date date --time time
       --interval execution-interval{M|w|d|h|m}
       [--duration timeout-value]
arcmigedit --file-system file-system-name
   --task task-name
   --policy policy-options[ --policy policy-options...]
arcmigedit -h
```

policy-options:

```
   [--policyid policy-id] filter-options[ filter-options...]
```

filter-options:

```
   {--dir directory-path --dir-operation {sw|nsw}
   |--ext file-extension --ext-operation {is|isnot}
   |--filename file-name --name-operation {is|isnot}
   |--{atime|mtime|ctime}
      {--filedate date --filetime time|date-and-time{d|h}}
      --time-operation {is|isnot|before|after}
   |--size size{b|kb|mb|gb} --size-operation {is|isnot|gt|lt}
   |--mod {new|data|meta} --mod-operation {is|isnot}}
```

Description

Changes the settings of a migration task.

Options and arguments

`--comment` *comment*

Specify this option to set a comment on a migration task. The comment must be no longer than 256 characters and enclosed in double quotation marks (").

You can use alphanumeric characters, exclamation marks (!), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), asterisks (*), plus signs (+), commas (,), hyphens (-), periods (.), forward slashes (/), colons (:), semicolons (;), left angle brackets (<), equal signs (=), right angle brackets (>), question marks (?), at marks (@), left square brackets ([), right square brackets (]), carets (^), underscores (_), grave accent marks (`), left curly brackets ({), vertical bars (|), right curly brackets (}), tildes (~), spaces and multi-byte Unicode (UTF-8) characters.

When using special characters, use the escape characters appropriate for the remote host environment.

`--date` *date*

Specify this option to set a scheduled date in `YYYY/MM/DD` format. The date and time specified in this option or the `--time` option must be a future date and time.

`--duration` *timeout-value*

Specify the maximum length of time for which the migration task can run. You can specify a value from 0 to 60 (units: hours). If you specify 0, no timeout occurs. The default setting (0) cannot be changed if the target

file system is a home-directory-roaming file system or read-write-content-sharing file system.

`--file-system` *file-system-name*

Specify the name of the target file system.

`--interval` *execution-interval*`{M|w|d|h|m}`

Specify this option to set the execution interval for a migration task.

execution-interval

Specify the execution interval for a migration task, in units of `M` (months), `w` (weeks), `d` (days), `h` (hours), or `m` (minutes) all at the same time.

To specify an interval, set an integer value for each unit.

- `M` (*months*) : 1

- `w` (*weeks*) : 1 to 4

- `d` (*days*) : 1 to 6

- `h` (*hours*) : 1 to 23

- `m` (*minutes*) : 10 to 59

For example, if you want to specify an execution interval of one day, specify `1d`.

The execution interval cannot be set to a value exceeding one hour if the target file system is a home-directory-roaming file system (default setting: `1h`) or read-write-content-sharing file system (default setting: `10m`).

`--policy`

Specify this option to add or change a migration policy. You can set a maximum of 10 migration policies. All the files set as migration targets in each policy will be migrated.

A migration policy cannot be added or changed if the target file system is a home-directory-roaming file system or read-write-content-sharing file system.

`--priority {high|middle|low|`*priority-level*`}`

Specify this option to set the priority of a scheduled migration task.

`high`

Specify this to set a `high` priority (equivalent a numerical priority of 3).

`middle`

Specify this to set a `middle` priority (equivalent a numerical priority of 5).

`low`

Specify this to set a `low` priority (equivalent a numerical priority of 7).

priority-level

Specify this to set a numerical priority from a range of 1 to 10. A smaller value indicates a higher priority level.

--schedule

Specify this option to schedule the migration task.

--task *task-name*

Specify the name of the target migration task.

--time *time*

Specify this option to set the scheduled time in hh:mm format. The date and time specified in this option or the --date option must be a future date and time.

policy-options

Specify these options when adding or changing a migration policy.

--policyid *policy-ID*

If you manually specify a policy ID when adding a migration policy, set a policy ID that is no longer than 32 characters. You can use alphanumeric characters and underscores (_). Specify a unique name within a task. If you specify the --policy option and omit this option, a policy ID is issued automatically.

To change a migration policy, specify the target policy ID. When doing so, the existing filter options of the specified policy ID are overwritten; you must therefore add all the necessary filter options.

filter-options

Add filter options as conditions for selecting files to be migrated. You can set a maximum of 20 filter options. All files that satisfy every condition set in the filter options will be migrated.

--dir *directory-path*

Specify this option to use a directory path as a migration condition. Specify the directory path starting from the mount point. For example, specify /mnt/FS1/dir01 for the dir01 directory. Specify the directory path within no more than 4,073 bytes.

--dir-operation {sw|nsw}

Specify this option to define which files will be migrated when a directory path is set as a migration condition.

sw

Specify this option to migrate files that are in the specified directory path.

nsw

Specify this option to migrate files other than those in the specified directory path.

--ext *file-extension*

Specify this option to define files to be migrated when using the file extension as a migration condition. The file extension must be no

Command Reference

longer than 4,095 characters. A period (.) cannot be used in the file extension. You can specify an asterisk (*) or question mark (?) as a wildcard.

`--ext-operation {is|isnot}`

Specify this option to define files to be migrated when using the file extension as a migration condition.

`is`

Specify this option to migrate files that have the specified file extension.

`isnot`

Specify this option to migrate files that do not have the specified file extension.

`--filename` *file-name*

Specify this option to use the file name as a migration condition. The file name must be no longer than 4,095 characters. You can specify an asterisk (*) or question mark (?) as a wildcard.

`--name-operation {is|isnot}`

Specify this option to define files to be migrated when using the file name as a migration condition.

`is`

Specify this to migrate files that have the specified file name.

`isnot`

Specify this to migrate files that do not have the specified file name.

`--{atime|mtime|ctime}`

Specify this option to use the file timestamp (in the local time of a node) as a migration condition.

`atime`

Specify this to use the last access time of a file as a migration condition.

`mtime`

Specify this to use the update time of a file as a migration condition.

`ctime`

Specify this to use the update time of a file attribute as a migration condition.

`--filedate` *date*

Specify this option to set a date in `YYYY/MM/DD` format when using the file timestamp (in the local time of a node) as a migration condition.

`--filetime` *time*

Specify this option to set a time in `hh:mm` format when using the file timestamp (in the local time of a node) as a migration condition.

date-and-time `{d|h}`

Specify this option to set a relative date and time based on the current date and time when using the file timestamp (in the local time of a node) as a migration condition.

`d`

Specify this to set the number of days based on the current date and time.

`h`

Specify this to set the number of hours based on the current date and time.

`--time-operation {is|isnot|before|after}`

Specify this option to define files to be migrated when using the file timestamp (in the local time of a node) as a migration condition.

`is`

Specify this to migrate files whose timestamp is the same as the specified date and time.

`isnot`

Specify this to migrate files whose timestamp is not the same as the specified date and time.

`before`

Specify this to migrate files whose timestamp is earlier than the specified date and time.

`after`

Specify this to migrate files whose timestamp is later than the specified date and time.

`--size `*`size`*`{b|kb|mb|gb}`

Specify this option when using the file size as a migration condition.

`size``{b|kb|mb|gb}`

Specify this to set a file size, in units of `b` (bytes), `kb` (kilobytes), `mb` (megabytes), and `gb` (gigabytes) all at the same time.

To specify a file size, set an integer value for each unit.

- `b` (byte) : 1 to 1,125,899,906,842,624

- `kb` (kilobyte) : 1 to 1,099,511,627,776

- `mb` (megabyte) : 1 to 1,073,741,824

- `gb` (gigabyte) : 1 to 1,048,576

For example, if you want to specify a size of 1 GB, specify `1gb` for the size.

`--size-operation {is|isnot|gt|lt}`

Specify this option to define files to be migrated when the file size is used as a migration condition.

`is`

Specify this to migrate files whose size is the same as the specified size.

`isnot`

Specify this to migrate files whose size is not the same as the specified size.

`gt`

Specify this to migrate files that are larger than the specified size.

`lt`

Specify this to migrate files that are smaller than the specified size.

`--mod {new|data|meta}`

Specify this option to use the file status as a migration condition.

`new`

Specify this to migrate files that have been created.

`data`

Specify this to migrate files in which data has been changed.

`meta`

Specify this to migrate files in which only metadata has been changed.

`--mod-operation {is|isnot}`

Specify this option to define files to be migrated when the file status is used as a migration condition.

`is`

Specify this to migrate files that are of the specified status.

`isnot`

Specify this to migrate files that are not of the specified status.

Return values

Table 2-31 Return values of the arcmigedit command

Return value	Description
0	Normal termination
1, 2#, 3	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2#, 5, 10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
67, 68	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Examples

To change the settings of the existing migration task `daily_migtask` to the following settings:

- The name of the file system is `fs1`.
- The name of the task is `task_priority`.
- The priority of the scheduled migration task is set to `high`.
- The comment for the migration task is set to `daily migration task to back up files`.

```
$ sudo arcmigedit --file-system fs1 --task task_priority --priority high --
comment "daily migration task to backup files"
```

To change the settings of the existing migration task `monthly_migtask` to the following settings:

- The name of the file system is `fs1`.
- The name of the task is `monthly_migtask`.
- The scheduled execution date and time is set to `2018/07/02 03:00`.
- The execution interval for the migration task is set to two weeks.
- The timeout duration for the migration task is set to eight hours.

```
$ sudo arcmigedit --file-system fs1 --task monthly_migtask --schedule --
date 2018/07/02 --time 03:00 --interval 2w --duration 8
```

To change the settings of the existing migration task `weekly_migtask` to the following settings:

- The name of the file system is `fs1`.
- The name of the task is `weekly_migtask`.
- In the existing migration policy `largefile_backup`, the following conditions are specified for selecting files to be migrated:
  - Files that were updated within one week.
  - Files that are larger than 1 GB.

```
$ sudo arcmigedit --file-system fs1 --task weekly_migtask --policy --
policyid largefile_backup --mtime 7d --time-operation after --size 1gb --
size-operation gt
```

arcmiglist (Display information about migration tasks)

Synopsis

```
arcmiglist [--file-system file-system-name
    [--task task-name]]
arcmiglist -h
```

Description

Displays information about migration tasks.

Options and arguments

`--file-system` *file-system-name*

Specify the name of a file system to display information on tasks that are set in the file system. If you specify only this option, this command displays information about all the migration tasks that are set in the file system.

`--task` *task-name*

Specify this option to display specific task information.

If you omit all options, all migration tasks set in all file systems mounted on the execution node are displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-32 Information displayed when executing the arcmiglist command

Item	Description
File System	Displays the file system name.
Migration Task	Displays the migration task name.
Priority(order)	Displays the priority of the scheduled migration task in the following format: • High(*1-2-or-3*) • Middle(*4-5-or-6*) • Low(*7-8-9-or-10*)
Comment	Displays the comment for the migration task. If a comment is not set, `--` is displayed.

Status	Displays whether the migration task is enabled.
	`Enable`
	　　This is displayed when the migration task is enabled.
	`Disable`
	　　This is displayed when the migration task is disabled.

Item	Description
Schedule	Displays the schedule information of the migration task.
Interval	Displays the execution interval of the migration task.
Start-time	Displays the start date and time of the schedule in the following format: *date* (format: *YYYY/MM/DD*) *time* (format: *hh*:*mm*)
Duration	Displays the timeout duration for the migration task.
Policies	Displays information about the migration policy.
Policy (*policy-ID*)	Displays the policy ID of the migration policy.
Condition	Displays conditions for selecting files to be migrated.
Criteria[#]	Displays the types of migration conditions.
Operation[#]	Displays comparison operators.
Value[#]	Displays operands.

[#]

Information displayed in Operation and Value differs depending on the migration-condition type displayed in Criteria. The following shows the displayed combinations of the Criteria, Operation, and Value.

Table 2-33 Information about conditions for selecting files to be migrated when executing the arcmiglist command.

Criteria (migration-condition type)	Operation (Comparison operator)	Value (Operand)
FileExtension	is is not	Displays the file extension.
FileName	is is not	Displays the file name.
LastAccessedTime, LastChangeTime (attributes change time), LastModifiedTime (data modification time)	is is not before after	When a date and time is specified, displays the criteria in the following format: *date* (format: *YYYY/MM/DD*) *time* (format: *hh*:*mm*) When a relative date and time is specified based on the current date and time, displays the criteria in the following format: $now-D*number of days* $now-H*number of hours*
FileSize	is is not greater than	Displays the file size (unit: Byte, KB, MB or GB).

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

Criteria (migration-condition type)	Operation (Comparison operator)	Value (Operand)
	less than	

ModifiedType	is
	is not
		Displays the type of data change.
		
		new
		
		    Displays this when the file has been created.
		
		data
		
		    Displays this when data has been changed.
		
		meta
		
		    Displays this when metadata has been changed.

DirectoryPath	starts with not start with	Displays a directory path.

Return values

Table 2-34 Return values of the arcmiglist command

Return value	Description
0	Normal termination
1, 2[#], 3	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2[#], 5, 10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
67, 68	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

    The command ended abnormally due to multiple causes.

arcmigresult (Display the paths of files for which migration succeeded or failed)

Synopsis

```
arcmigresult --file-system file-system-name
    --task task-name [--run run-ID] [--failedlist]
arcmigresult -h
```

Description

Lists the paths of files for which migration succeeded or failed.

Options and arguments

--failedlist

Specify this option to list the paths of files that could not be migrated. Each path is displayed in the following format:

date (format: *YYYY/MM/DD*) *time* (format: *hh:mm:ss*) *message-ID message file-path*

Omit this option to list the paths of files that were migrated successfully.

--file-system *file-system-name*

Specify the name of the file system for which the target migration task is set.

--run *run-ID*

If you want to specify a migration that was attempted at a specific time, specify the run ID in the following format:

date (format: *YYYY/MM/DD*) – *migration-task-serial-number* (format: *NNN*)

A run ID is automatically assigned each time migration is executed by the migration task. The information about the migration that was executed at a specific time can be displayed by specifying a run ID. You can use the `arcmigstatus` command to check the run ID.

If you omit this option, the most recently executed migration task or the migration task currently being executed is targeted.

--task *task-name*

Specify the name of the target migration task.

Return values

Table 2-35 Return values of the arcmigresult command

Return value	Description
0	Normal termination

Return value	Description
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 5, 8, 12, 17, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcmigrun (Execute the migration task immediately)

Synopsis

```
arcmigrun --file-system file-system-name
    --task task-name [--priority priority-level]
    [--duration timeout-value] [--foreground]
arcmigrun -h
```

Description

Executes the migration task immediately.

Note that this command immediately executes the migration task based on the preset policy, except for the timeout value and priority level.

Options and arguments

--duration *timeout-value*

Specify the maximum length of time for which the migration task can run. You can specify a value from 0 to 60 (units: hours). If you specify 0, no timeout occurs.

If you omit this option, regardless of the setting of the task, the migration task as 0 has been specified will be executed immediately.

--file-system *file-system-name*

Specify the name of the target file system name.

--foreground

Specify this option to execute the migration task in the foreground. If you omit this option, the migration task is executed in the background.

--priority *priority-level*

Specify this option to set the priority of a scheduled migration task from a range of 1 to 10. A smaller value indicates a higher priority level. You can

also specify the string `high`, `middle`, or `low`, which is equivalent to `3`, `5`, or `7`, respectively.

If you omit this option, regardless of the setting of the task, the migration task as `middle` (`5`) has been specified will be executed immediately.

`--task` *task-name*

Specify the name of the target migration task.

Return values

Table 2-36 Return values of the arcmigrun command

Item	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 5, 8, 12, 17, 56, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66, 67, 85	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcmigset (Create migration tasks)

Synopsis

```
arcmigset --file-system file-system-name
   --task --name task-name
      [--priority {high|middle|low|priority-level}]
      [--comment comment]
   --schedule
      --date date
      --time time
      --interval execution-interval{M|w|d|h|m}
      [--duration timeout-value]
   [--policy policy-options[ --policy policy-options...]]
arcmigset -h
```

policy-options:

```
   [--policyid policy-ID] filter-options[ filter-options...]
```

filter-options:

```
{--dir directory-path --dir-operation {sw|nsw}
|--ext file-extension --ext-operation {is|isnot}
|--filename file-name --name-operation {is|isnot}
|--{atime|mtime|ctime}
   {--filedate date --filetime time|date-and-time{d|h}}
   --time-operation {is|isnot|before|after}
|--size size{b|kb|mb|gb} --size-operation {is|isnot|gt|lt}
|--mod {new|data|meta} --mod-operation {is|isnot}}
```

Description

Creates migration tasks. You can set a maximum of 10 migration tasks per file system.

Migration tasks cannot be created on a file system that references data from HDI via linked HCP systems as read-only. You cannot create tasks other than the migration tasks created by default, when the target file system is a home-directory-roaming file system or read-write-content-sharing file system.

Options and arguments

`--comment` *comment*

Specify this option to set a comment on a migration task. The comment must be no longer than 256 characters and enclosed in double quotation marks (").

You can use alphanumeric characters, exclamation marks (!), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), asterisks (*), plus signs (+), commas (,), hyphens (-), periods (.), forward slashes (/), colons (:), semicolons (;), left angle brackets (<), equal signs (=), right angle brackets (>), question marks (?), at marks (@), left square brackets ([), right square brackets (]), carets (^), underscores (_), grave accent marks (`), left curly brackets ({), vertical bars (|), right curly brackets (}), tildes (~), spaces and multi-byte Unicode (UTF-8) characters.

When using special characters, use the escape characters appropriate for the remote host environment.

`--date` *date*

Specify this option to set a scheduled date in `YYYY/MM/DD` format. The date and time specified in this option or the `--time` option must be a future date and time.

`--duration` *timeout-value*

Specify the maximum length of time for which the migration task can run. You can specify a value from 0 to 60 (units: hours). If you specify 0, no timeout occurs.

`--file-system` *file-system-name*

Specify the name of the target file system.

`--interval` *execution-interval*{M|w|d|h|m}

Specify this option to set the execution interval for a migration task.

execution-interval

Specify the execution interval for a migration task, in units of `M` (months), `w` (weeks), `d` (days), `h` (hours), or `m` (minutes) all at the same time.

To specify an interval, set an integer value for each unit.

- `M` (months) : 1

- `w` (weeks) : 1 to 4

- `d` (days) : 1 to 6

- `h` (hours) : 1 to 23

- `m` (minutes) : 10 to 59

For example, if you want to specify an execution interval of one day, specify `1d`.

`--policy`

Specify this option to add a migration policy. You can set a maximum of 10 migration policies. All the files set as migration targets in each policy will be migrated.

If you omit this option, all files in the file system will be migrated.

`--priority {high|middle|low|`*priority-level*`}`

Specify this option to set the priority of a scheduled migration task.

`high`

Specify this to set a `high` priority (equivalent a numerical priority of 3).

`middle`

Specify this to set a `middle` priority (equivalent a numerical priority of 5).

`low`

Specify this to set a `low` priority (equivalent a numerical priority of 7).

priority-level

Specify this to set a numerical priority from a range of 1 to 10. A smaller value indicates a higher priority level.

`--schedule`

Specify this option to schedule the migration task.

`--task --name` *task-name*

Use a maximum of 32 characters to specify the name of the task system. You can use alphanumeric characters and underscores (_). Specify a unique name within a file system.

`--time` *time*

Specify this option to set the scheduled time in `hh:mm` format. The date and time specified in this option or the `--date` option must be a future date and time.

policy-options

Specify this option to add a migration policy.

`--policyid` *policy-ID*

Specify this option to manually set a policy ID. The policy ID must be no longer than 32 characters. You can use alphanumeric characters and underscores (_). Specify a unique name within a task. If you specify the `--policy` option and omit this option, a policy ID is issued automatically.

filter-options

Add filter options as conditions for selecting files to be migrated. You can set a maximum of 20 filter options. All files that satisfy every condition set in the filter options will be migrated.

`--dir` *directory-path*

Specify this option to use a directory path as a migration condition. Specify the directory path starting from the mount point. For example, specify `/mnt/FS1/dir01` for the `dir01` directory. Specify the directory path within no more than 4,073 bytes.

`--dir-operation {sw|nsw}`

Specify this option to define which files will be migrated when a directory path is set as a migration condition.

`sw`

Specify this option to migrate files that are in the specified directory path.

`nsw`

Specify this option to migrate files other than those in the specified directory path.

`--ext` *file-extension*

Specify this option to define files to be migrated when using the file extension as a migration condition. The file extension must be no longer than 4,095 characters. A period (.) cannot be used in the file extension. You can specify an asterisk (*) or question mark (?) as a wildcard.

`--ext-operation {is|isnot}`

Specify this option to define files to be migrated when using the file extension as a migration condition.

`is`

Specify this option to migrate files that have the specified file extension.

`isnot`

Specify this option to migrate files that do not have the specified file extension.

--filename *file-name*

Specify this option to use the file name as a migration condition. The file name must be no longer than 4,095 characters. You can specify an asterisk (*) or question mark (?) as a wildcard.

--name-operation {is|isnot}

Specify this option to define files to be migrated when using the file name as a migration condition.

is

Specify this to migrate files that have the specified file name.

isnot

Specify this to migrate files that do not have the specified file name.

--{atime|mtime|ctime}

Specify this option to use the file timestamp (in the local time of a node) as a migration condition.

atime

Specify this to use the last access time of a file as a migration condition.

mtime

Specify this to use the update time of a file as a migration condition.

ctime

Specify this to use the update time of a file attribute as a migration condition.

--filedate *date*

Specify this option to set a date in YYYY/MM/DD format when using the file timestamp (in the local time of a node) as a migration condition.

--filetime *time*

Specify this option to set a time in hh:mm format when using the file timestamp (in the local time of a node) as a migration condition.

date-and-time {d|h}

Specify this option to set a relative date and time based on the current date and time when using the file timestamp (in the local time of a node) as a migration condition.

d

Specify this to set the number of days based on the current date and time.

h

Specify this to set the number of hours based on the current date and time.

--time-operation {is|isnot|before|after}

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

Specify this option to define files to be migrated when using the file timestamp (in the local time of a node) as a migration condition.

`is`

Specify this to migrate files whose timestamp is the same as the specified date and time.

`isnot`

Specify this to migrate files whose timestamp is not the same as the specified date and time.

`before`

Specify this to migrate files whose timestamp is earlier than the specified date and time.

`after`

Specify this to migrate files whose timestamp is later than the specified date and time.

`--size` *size*`{b|kb|mb|gb}`

Specify this option when using the file size as a migration condition.

size`{b|kb|mb|gb}`

Specify this to set a file size, in units of `b` (bytes), `kb` (kilobytes), `mb` (megabytes), and `gb` (gigabytes) all at the same time.

To specify a file size, set an integer value for each unit.

- `b` (byte) : 1 to 1,125,899,906,842,624

- `kb` (kilobyte) : 1 to 1,099,511,627,776

- `mb` (megabyte) : 1 to 1,073,741,824

- `gb` (gigabyte) : 1 to 1,048,576

For example, if you want to specify a size of 1 GB, specify `1gb` for the size.

`--size-operation {is|isnot|gt|lt}`

Specify this option to define files to be migrated when the file size is used as a migration condition.

`is`

Specify this to migrate files whose size is the same as the specified size.

`isnot`

Specify this to migrate files whose size is not the same as the specified size.

`gt`

Specify this to migrate files that are larger than the specified size.

`lt`

Specify this to migrate files that are smaller than the specified size.

`--mod {new|data|meta}`

Specify this option to use the file status as a migration condition.

`new`

Specify this to migrate files that have been created.

`data`

Specify this to migrate files in which data has been changed.

`meta`

Specify this to migrate files in which only metadata has been changed.

`--mod-operation {is|isnot}`

Specify this option to define files to be migrated when the file status is used as a migration condition.

`is`

Specify this to migrate files that are of the specified status.

`isnot`

Specify this to migrate files that are not of the specified status.

Return values

Table 2-37 Return values of the arcmigset command

Return value	Description
`0`	Normal termination
`1`, `2`[#], `3`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`2`[#], `5`, `8`, `10`, `70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`67`, `68`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`97`, `99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Examples

To set up a migration task to back up files of a specific file extension:

- ○ The name of the file system is `fs1`.
- ○ The name of the task system is `daily_migtask`.
- ○ The scheduled execution date and time is set to `2016/07/01 23:30`.
- ○ The execution interval for the migration task is set to one day.

Command Reference

- The timeout duration of the migration task is set to two hours.
- A migration policy `e1` is set, to migrate files whose file extension is `xls`.
- A migration policy `w1` is set, to migrate files whose file extension is `doc`.
- A migration policy `p1` is set, to migrate files whose file extension is `ppt`.

```
$ sudo arcmigset --file-system fs1 --task --name daily_migtask --schedule
--date 2016/07/01 --time 23:30 --interval 1d --duration 2 --policy --
policyid e1 --ext xls --ext-operation is --policy --policyid w1 --ext doc
--ext-operation is --policy --policyid p1 --ext ppt --ext-operation is
```

To set a migration task that is performed every weekend to migrate large files that have been updated within one week:

- The name of the file system is `fs1`.
- The name of the task system is `weekly_migtask`.
- The scheduled execution date and time is set to `2016/07/02 02:30`.
- The execution interval for the migration task is set to one week.
- The timeout duration of the migration task is set to twelve hours.
- In the migration policy `largefile_backup`, the following migration conditions are set:
  - Files that were updated within one week.
  - Files that are larger than 500 MB.

```
$ sudo arcmigset --file-system fs1 --task --name weekly_migtask --schedule
--date 2016/07/02 --time 02:30 --interval 1w --duration 12 --policy --
policyid largefile_backup --mtime 7d --time-operation before --size 500mb
--size-operation gt
```

To set up a monthly task that migrates specific files and directories:

- The name of the file system is `fs1`.
- The name of the task system is `monthly_migtask`.
- The scheduled execution date and time is set to `2016/07/03 02:30`.
- The execution interval for the migration task is set to one month.
- The timeout duration of the migration task is set to six hours.
- A migration policy `dir_backup` is set, to migrate files located in directory paths that include `backup_src_dir/`.
- A migration policy `name_backup` is set, to migrate files whose name is `important.pdf`.

```
$ sudo arcmigset --file-system fs1 --task --name monthly_migtask --
schedule --date 2016/07/03 --time 02:30 --interval 1M --duration 6 --
policy --policyid dir_backup --dir backup_src_dir/ --dir-operation sw --
policy --policyid name_backup --filename important.pdf --name-operation is
```

arcmigstatus (Display the execution results of the migration task)

Synopsis

```
arcmigstatus [[--detail] --file-system file-system-name
    --task task-name [--day value1[-value2] | --run run-ID]]
arcmigstatus -h
```

Description

Displays the execution results or progress of the migration task.

If you omit all options, the command displays the results of executing the migration tasks that are set for all file systems that are mounted on the execution node. (Migration tasks that have not been executed are ignored.)

Options and arguments

--detail

Specify this to display detailed information about the migration tasks.

--day value1[-value2]

Specify this to limit the range of migration task information to be displayed (units: days). For value1, you can specify 0 to 6 (units: days). For value2, you can specify 1 to 6 (units: days).

To specify a past specific period (units: days) from the current date, specify only value1.

To specify a period (units: days) from a specific day before the current date, specify value1 and value2. For example, if you specify --day 2-5, the command displays the information about the migrations executed during the period from five days before to two days before the current date. Note that value2 must be larger than value1.

--file-system file-system-name

Specify the name of the file system for which the target migration task or tasks are set.

--run run-ID

If you want to specify a migration that was attempted at a specific time, specify the run ID in the following format:

date (format: YYYY/MM/DD) - migration-task-serial-number
(format: NNN)

A run ID is automatically assigned each time migration is executed by the migration task. The information about the migration that was executed at a specific time can be displayed by specifying a run ID.

--task task-name

Specify the name of the migration task for which you want to display information.

Note that if you specify only the `--file-system` and `--task` options or if you omit all options, information is displayed only for migration tasks that were executed recently or are currently being executed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-38 Information displayed when executing the arcmigstatus command

Item	Description
Task name	Displays the name of the migration task.
File system	Displays the name of the file system.
Run ID	Displays the run ID in the following format: *date* (format: *YYYY/MM/DD*) - *migration-task-serial-number* (format: *NNN*) Also, if the migration task being executed is not finished, and as a result, no run ID is assigned, a hyphen (-) is displayed.
Priority(order)	Displays the priority of the scheduled migration task in the following format: • High(*1-2-or-3*) • Middle(*4-5-or-6*) • Low(*7-8-9-or-10*)
Status	Displays the current status of the migration task. Running The migration task is running. Succeeded The migration task terminated normally. PartiallyFailed The migration task finished, but some objects could not be migrated. Failed(*message-ID*) The migration task failed to start. The *message-ID* in parentheses indicates the cause of the failure. Interrupted The processing of the task was interrupted due to timeout, cancellation, failover, or unmounting of the file system. When a task is terminated repeatedly, revise the task timeout duration.
Progress	Displays the progress of the migration task for which `Status` is `Running`. A migration task is processed in the following order: Waiting The migration task is waiting for another migration task to finish. Initializing

Item	Description
	The migration task is starting.
	`Pre-processing(nn/mm)`
	The progress of pre-processing is displayed.
	`Processing filters(nn/mm)`
	The progress of filtering is displayed.
	`Transferring data(nn/mm)`
	The progress of data transfer is displayed.
	`Post-processing(nn/mm)`
	The progress of post-processing is displayed.
	If `Status` is not `Running`, a hyphen (-) is displayed.
`Start time`	Displays the start time of the migration task, in the following format:
	date (format: *YYYY*/*MM*/*DD*) *time* (format: *hh*:*mm*:*ss*)
`End time`	Displays the end time of the migration task, in the following format:
	date (format: *YYYY*/*MM*/*DD*) *time* (format: *hh*:*mm*:*ss*)
	If `Status` is `Running`, a hyphen (-) is displayed.
`Duration(Hour)`	The timeout for migration task processing is displayed (unit: hours).
	Note that if `0` is set for the timeout of migration task processing, or if no timeout is specified, `0` is displayed.
`Target count`	Displays the total number of files and directories to be migrated by the migration task.
	Note that if `Progress` is `Wait`, or `Pre Task` or `Filter`, `0` is displayed.
`Succeeded count`	Displays the total number of files and directories that were migrated successfully.
`Failed count`	Displays the total number of files and directories that could not be migrated.
`Succeeded data size (MB)` [#]	Displays the total size of files (units: MB) that were migrated successfully.
`Failed data size (MB)` [#]	Displays the total size of files (units: MB) that could not be migrated.
`Succeeded count details`	Displays details about files and directories that were successfully migrated.
`New file`	Out of displayed value to `Succeeded count`, displays the number of new files that were migrated successfully.
`Data changes`	Out of displayed value to `Succeeded count`, displays the number of updated files that were migrated successfully.
`Meta data changes`	Out of displayed value to `Succeeded count`, displays the number of files for which metadata was updated.
`Directories`	Out of displayed value to `Succeeded count`, displays the number of directories that were migrated successfully.

Command Reference

Item	Description
Failed count details	Displays details about files and directories that failed to be migrated.
Message ID	Displays the message ID that indicates the reason migration failed.
Count	Displays the total number of files and directories that could not be migrated for the reason indicated by the message ID.
Work space used(GB)	The usage amount of the work space when the migration task is executed is displayed (unit: GB).
	If a migration task is being executed or if you are not using the Active File Migration functionality, a hyphen (-) is displayed. In addition, Overflow is displayed if the capacity of the work space is insufficient, and Error is displayed if a failure has occurred in the work space.

\#
The values are rounded down to 3 decimal places.

Return values

Table 2-39 Return values of the arcmigstatus command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 5, 8, 12, 17, 68[#], 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
The command ended abnormally due to multiple causes.

arcmigstop (Stop migration currently being executed)

Synopsis

```
arcmigstop --file-system file-system-name
    --task task-name
arcmigstop -h
```

Description

Stops migration currently being executed.

To check whether migration ended, use the `arcmigstatus` command.

Options and arguments

`--file-system` *file-system-name*

Specify the name of the file system for which the target migration task is set.

`--task` *task-name*

Specify the name of the target migration task.

Return values

Table 2-40 Return values of the arcmigstop command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 5, 8, 12, 17, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcmodectl (Set initial mode for tasks)

Synopsis

```
arcmodectl --file-system file-system-name
    --init-migration {enable [-t {onlyonce|repeat}]|disable}
arcmodectl --file-system file-system-name
    --init-tiering {enable [-t {onlyonce|repeat}]|disable}
arcmodectl --file-system file-system-name
    --init-snglinst {enable [-t {onlyonce|repeat}]|disable}
arcmodectl --file-system file-system-name
arcmodectl -h
```

Description

Sets whether to use initial mode to execute a migration task. The command can also be used to view the current setting.

If the initial mode is enabled for migration tasks, the data from another HDI system cannot be referenced as read-only. Reference the data as read-only after the tasks finish in the initial mode. Initial mode settings are not restored by system LU restoration. If you restored the system LU, re-set the mode as necessary.

Notes:

- This command cannot be used for home-directory-roaming file systems.

- This command cannot be used for read-write-content-sharing file systems.

- If you specify the settings to use initial mode when the Large File Transfer function is enabled, processing might take a long time when migration is performed the next time. Therefore, if you set initial mode, use the `arclftctl` command to disable the Large File Transfer function and use the `arcmigedit` command to specify the settings so that migration is not stopped.

- Even if you execute tasks in the initial mode, files or directories that have one or more line feed codes in their paths will not be included in the tasks. To identify the files or directories that are not included in the tasks, specify the `-regex` option from an NFS client, and then execute the `find` command.

When using the `find` commands:

```
find ./  -regex ".*/\.history" -prune -or -regex ".*/\.snaps" -prune -
or -regex ".*/\.lost\\+found" -prune -or -regex ".*/\.system_gi" -
prune -or -regex ".*[^M
].*" -print
```

Line feed codes are the CR code and LF code. In the above example, ^M indicates the CR code. Type **Ctrl** + **v** and then **Ctrl** + **m** to display ^M. The LF code is used after ^M. Type **Ctrl** + **v** and then **Ctrl** + **j** to display it.

Options and arguments

`--file-system` *file-system-name*

Specify the name of the file system for which initial mode is set or the settings are viewed. If this option is specified with the `--init-migration`, `--init-tiering`, or `--init-snglinst` option, whether to use initial mode is set. If this option is specified alone, the current settings are displayed.

`--init-migration {enable|disable}`

Specify whether to use initial mode to execute migration tasks. The initial setting is `disable`.

`enable`

Specify to use initial mode.

`disable`

Specify not to use initial mode.

`--init-snglinst {enable|disable}`

This option is not supported.

`--init-tiering {enable|disable}`

This option is not supported.

`-t {onlyonce|repeat}`

Specify the usage of the initial mode when executing a migration task. You can specify this option when `enable` is specified for the `--init-migration` option. If you omit this option, it defaults to `onlyonce`.

`onlyonce`

Specify to use initial mode only the next time a task is executed.

`repeat`

Specify to use initial mode every time a task is executed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-41 Information displayed when executing the arcmodectl command

Item	Description
Initial Migration	Displays whether to use initial mode to execute migration tasks.
	`Enable(onlyonce)`
	Displayed when use initial mode only the next time a task is executed.
	`Enable(repeat)`
	Displayed when use initial mode every time a task is executed.
	`Disable`

Item	Description
	Displayed when initial mode is not used.
Initial Tiering	This item is not supported.
Initial Single Instancing	This item is not supported.

Note: The items whose corresponding tasks are disabled are not displayed.

Return values

Table 2-42 Return values of the arcmodectl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 5, 8, 12, 15, 17, 68, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To enable initial mode for migration tasks for the `fs01` file system:

```
$ sudo arcmodectl --file-system fs01 --init-migration enable
```

To view the initial mode settings for tasks for the `fs01` file system:

```
$ sudo arcmodectl --file-system fs01
Initial Migration        : Enable(onlyonce)
```

arcstdel (Delete the data and mapping information for a file system linked to the HCP system at the share level)

Synopsis

```
arcstdel [-f] --file-system file-system-name --dir directory-name
arcstdel -h
```

Description

Deletes the data and mapping information under the specified directory in a file system linked to the HCP system at the share level. You must execute this command after deleting shares.

Before executing the this command, check the following:

- Make sure that the subtree quota set for the directory under the target share is released.
- If you imported data from other file servers, after importing, make sure that the import definition information is deleted.

Note:
Data deleted by using this command cannot be restored.

Options and arguments

`--dir` *directory-name*

Specify the name of the directory for which you want to terminate the HCP system linkage at the share level.

`-f`

Specify this to prevent a confirmation message from appearing.

`--file-system` *file-system-name*

Specify the name of the file system in which the target directory exists.

Return values

Table 2-43 Return values of the arcstdel command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 5, 10, 15, 18, 65, 66[#], 68, 70, 71	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
66[#], 67, 69	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

arcproxydel (Delete proxy server information)

Synopsis

```
arcproxydel [-h]
```

Description

Deletes information about the proxy server used for communication with HCP.

Return values

Table 2-44 Return values of the arcproxydel command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
70, 71[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
71[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

arcproxyget (Display proxy server information)

Synopsis

```
arcproxyget [-h]
```

Description

Displays information about the proxy server used for communication with HCP.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-45 Information displayed when executing the arcproxyget command

Item	Description
Proxy host	Displays the host name or the IP address of the proxy server.
Proxy port	Displays the port number that the proxy server uses.
Proxy account user	Displays the user name used for proxy server authentication.

Note:
  Only the items that have been set are displayed.

Return values

Table 2-46 Return values of the arcproxyget command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcproxyset (Set proxy server information)

Synopsis

```
arcproxyset [--host host-name] [--port port-number]
    [--user-name user-name --password password]
arcproxyset -h
```

Description

Sets proxy server information if communication with HCP is performed via a proxy server.

The settings for the `arcproxyset` command can be specified either interactively or by choosing options. The setting items for both methods are the same. If you want to specify settings interactively, execute the command without any options.

The following table lists the information items that can be set interactively.

Table 2-47 Information that can be specified interactively for the arcproxyset command

Item	Description
host	Specifies the host name or the IP address of the proxy server. This item must be specified if you are specifying proxy server information for the first time. If this item has not been changed, do not specify anything and then press **Enter**.
port	Specifies the port number to be used in the proxy server. This item must be specified if you are specifying proxy server information for the first time. If this item has not been changed, do not specify anything and then press **Enter**.
user-name	Specifies the user name if a proxy server requiring user authentication is used. To delete information that has already been set, do not specify anything and then press **Enter**. If you specify nothing, the password will also be deleted.
password	Specifies the password when a proxy server requiring user authentication is used. To delete information that has already been set, do not specify anything and then press **Enter**. If you specify nothing, the user name will also be deleted.
confirm password	Specifies the password again. If a password is not being specified, do not specify this item and then press **Enter**.

Note:

   The character strings you specify for `password` and `confirm password` are not displayed.

Options and arguments

`--host` *host-name*

Specify the host name or the IP address of the proxy server. You must specify a host name if this is the first time you are specifying proxy server information. If the host name or IP address has already been set and has not been changed, you can omit the specification.

`--password` *password*

Specify the password for a proxy server that requires user authentication. To delete the current password, specify two double quotation marks (`""`) or two single quotation marks (`''`). If you do so, the user name will also be deleted.

`--port` *port-number*

Specify the port number used by the proxy server. You must specify a port number if you are specifying proxy server information for the first time. If the port number has already been set and has not been changed, you can omit the specification.

`--user-name` *user-name*

Specify the user name if you are using a proxy server that requires user authentication. To delete the current user name, specify two double quotation marks (`""`) or two single quotation marks (`''`). If you do so, the password will also be deleted.

Return values

Table 2-48 Return values of the arcproxyset command

Return value	Description
`0`	Normal termination
`1, 2`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`67`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`71`[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`71`[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

The command ended abnormally due to multiple causes.

Example

To interactively set proxy server information according to the following conditions:

- The host name of the proxy server is `proxy.example.com`.
- The port number used by the proxy server is `8080`.
- The user name used by proxy server authentication is `user01`.
- The password used for proxy server authentication is `proxypass` (not displayed).

```
$ sudo arcproxyset
host: proxy.example.com
port: 8080
user-name: user01
password:
confirm password:
```

arcreplimitget (Display the threshold at which stub processing is performed)

Synopsis

```
arcreplimitget --file-system file-system-name
arcreplimitget -h
```

Description

Displays the threshold (the remaining file system capacity) at which stub processing is performed.

Options and arguments

`--file-system` *file-system-name*
    Specify the name of the file system whose threshold you want to display.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-49 Information displayed when executing the arcreplimitget command

Item	Description
`Replication limit rest size`	Displays the threshold (the remaining file system capacity) at which stub processing is performed as a percentage or in gigabytes.

Return values

Table 2-50 Return values of the arcreplimitget command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`2, 4, 70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcreplimitset (Set the threshold at which stub processing is performed)

Synopsis

```
arcreplimitset --rest-size remaining-amount
   --file-system file-system-name
arcreplimitset -h
```

Description

Specifies the threshold at which stub processing is performed.

When the remaining file system capacity is less than or equal to the threshold value, stub processing is performed on files (in order of the files with the oldest access data and time first) until the remaining file system capacity exceeds the threshold again.

Options and arguments

`--file-system` *file-system-name*

Specify the name of the file system for which the threshold is to be set.

`--rest-size` *remaining-amount*

Specify a remaining file system capacity for the threshold at which stub processing is performed. The value can be specified as a percentage or as a value in gigabytes. For a percentage, specify a value from `5` to `100` followed by `%`. For a value in gigabytes, specify an integer from `0` to the total capacity of the specified file system (a value rounded up to the nearest gigabyte) followed by `g` or `G`. The initial value is `10%`.

Note:

If the remaining amount for the `--rest-size` option is set as a percentage, the value is converted to gigabytes based on the total size of the current file system, and the converted value is used as the actual threshold value. For example, if the size of the file system is 200 GB, and the remaining amount is set to 10%, the threshold value is 20 GB. If you expand the file system to 300 GB, the threshold value becomes 30 GB.

Return values

Table 2-51 Return values of the arcreplimitset command

Return value	Description
0	Normal termination
1, 3	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 4, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To set `20%` as the threshold for the file system named `FS_1`:

```
$ sudo arcreplimitset --rest-size 20% --file-system FS_1
```

To set `100` GB as the threshold for the file system named `FS_2`:

```
$ sudo arcreplimitset --rest-size 100g --file-system FS_2
```

arcresidentctl (Setting for acquiring information about pinned files)

Synopsis

```
arcresidentctl --report {enable|disable}
arcresidentctl
arcresidentctl -h
```

Description

Specifies whether information is to be acquired about the files that are pinned in the cache by cache resident policies. The values specified for this command apply to the entire system. The command can also be used to view the current setting.

In cluster configurations, this command also executes processing on the other node in the cluster.

Options and arguments

`--report {enable|disable}`

Specifies whether to acquire information about pinned files.

`enable`

Specify this to acquire information about pinned files. The default is `enable`.

`disable`

Specify this if you do not want to acquire information about pinned files.

If you omit all options, the current setting is displayed.

Displayed information

The following table lists the information displayed when this command is executed.

Table 2-52 Information displayed when the arcresidentctl command is executed

Item	Description

Reporting function	Displays whether to acquire information about pinned files.
	
	Enable
	
	    This is displayed if the information about pinned files is to be acquired.
	
	Disable
	
	    This is displayed if the information about pinned files is not to be acquired.

Return values

Table 2-53 Return values of the arcresidentctl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 68, 70, 71	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcresidentlist (Display pinned files)

Synopsis

```
arcresidentlist --file-system file-system-name
arcresidentlist -h
```

Description

Displays information about the files pinned in the cache by cache resident policies.

This command can be executed if the acquisition of information about pinned files has been enabled by using the `arcresidentctl` command.

Options and arguments

`--file-system` *file-system-name*

Specify the name of the file system for which pinned files are to be displayed.

Displayed information

The following table lists the information displayed when this command is executed.

Table 2-54 Information displayed when the arcresidentlist command is executed

Item	Description
Date and time the list of pinned files was updated	Displays the date and time that the list of pinned files was refreshed in the following format: *date* (format: *YYYY/MM/DD*) *time* (format: *hh*:*mm*:*ss*)
Size(KB) and File path	Displays the file size and file path of a pinned file in the following format: *file-size*[#] /mnt/*file-system-name*/*file-path* # If the file size is less than 1 KB, 0 is displayed.

Return values

Table 2-55 Return values of the arcresidentlist command

Return value	Description
0	Normal termination
1, 2	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
5, 8, 10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcresidentpolicydel (Delete a cache resident policy)

Synopsis

```
arcresidentpolicydel [-y] [--policy policy-name]
    --file-system file-system-name
arcresidentpolicydel -h
```

Description

Deletes a cache resident policy, which is used to pin files in the cache.

Options and arguments

--file-system *file-system-name*

Specify the name of the file system from which the cache resident policy is to be deleted.

`--policy` *policy-name*

Specify the name of the cache resident policy to be deleted. If you omit this option, all the policies for the specified file systems are deleted.

Return values

Table 2-56 Return values of the arcresidentpolicydel command

Return value	Description
0	Normal termination
1, 2	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
5, 8, 10, 12, 70, 74, 75	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71, 72, 73	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To delete all cache resident policies from the file system named `FS_1`:

```
$ sudo arcresidentpolicydel --file-system FS_1
KAQM37281-Q Are you sure you want to delete the cache resident policy?
(y/n) y
```

arcresidentpolicylist (Display cache resident policies)

Synopsis
```
arcresidentpolicylist [[--policy policy-name]
    --file-system file-system-name]
arcresidentpolicylist -h
```

Description

Displays information about cache resident policies, which are used to pin files in the cache.

Options and arguments

`--file-system` *file-system-name*

Specify the name of the file system for which information about cache resident policies is to be displayed. If you omit this option, policies of all the file systems that are mounted as read/write enabled are displayed.

`--policy` *policy-name*

Specify the name of the cache resident policy whose information is to be displayed. If you omit this option, all policies of the specified file system are displayed.

Displayed information

The following table lists the information displayed when this command is executed.

Table 2-57 Information displayed when the arcresidentpolicylist command is executed

Item	Description
File system	Displays the file system name.
Policy count	Displays the number of policies that are set in the file system. If the number of policies cannot be acquired, Unknown is displayed.
Policy name	Displays the policy name.
Directory	Displays the path of the directory in which all files are pinned in the cache.[#]
Extention	Displays the extensions of the files that are pinned in the cache.[#]
Minimum size	Displays the minimum size of the files that are pinned in the cache.[#]
Maximum size	Displays the maximum size of the files that are pinned in the cache.[#]
Comment	Displays comments for the policy.[#]

\#

This item is not displayed if comments are not specified.

Return values

Table 2-58 Return values of the arcresidentpolicylist command

Return value	Description
0	Normal termination
1, 2	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
12, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcresidentpolicyset (Set a cache resident policy)

Synopsis

```
arcresidentpolicyset [-f] [--dir directory-path]
    [--ext suffix[:suffix...]] [--min minimum-size]
    [--max maximum-size] [--comment comment]
    --policy policy-name --file-system file-system-name
arcresidentpolicyset -h
```

Description

Defines a cache resident policy, which is used to pin files in the cache.

You can specify a maximum of 100 cache resident policies for each file system.

Options and arguments

--comment *comment*

    Specify a comment for the policy to be set by using no more than 256 bytes.

--dir *directory-path*

    Specify, from the mount point, the path of the directory in which all files are pinned in the cache. Cache residency processing is performed for all the files within the specified directory. To set the directory to the `dir02` directory under `/mnt/filesystem01/dir01` (`/mnt/filesystem01/dir01/dir02`), specify `dir01/dir02`. Specify `/mnt/`*file-system-name*`/`*directory-path* in no more than 4,095 bytes.

    A directory that does not exist can also be specified.

`--ext` *suffix*[`:`*suffix*`...`]

Specify the extensions of the files that are pinned in the cache without including a period (`.`). To specify multiple extensions, use a colon (`:`) to separate the extensions. Use no more than 1,024 bytes. The extensions are case sensitive.

`-f`

Specify this to forcibly overwrite the policy when the specified policy name has already been set in the target file system.

`--file-system` *file-system-name*

Specify the name of the file system for which the policy is to be set.

`--max` *maximum-size*

Specify this to pin files in the cache if their file size is equal to or smaller than a specific size. Specify an integer and a unit from 1 KB to 1,024 TB. To specify the unit, add the letter `K` (KB), `M` (MB), `G` (GB), or `T` (TB) after the value. The specified value must be equal to or greater than the minimum size.

`--min` *minimum-size*

Specify this to pin files in the cache if their file size is equal to or greater than a specific size. Specify an integer and a unit from 1 KB to 1,024 TB. To specify the unit, add the letter `K` (KB), `M` (MB), `G` (GB), or `T` (TB) after the value. Specify a value that is no more than the maximum size.

`--policy` *policy-name*

Specify the policy name by using no more than 32 bytes. When you add a policy, the specified name must be unique within the file system.

The specifiable values are alphanumeric characters and underscores (_). Spaces can also be used, but they cannot be used at the beginning or end of the character string.

Return values

Table 2-59 Return values of the arcresidentpolicyset command

Return value	Description
`0`	Normal termination
`1, 2`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`5, 8, 10, 12, 15, 70, 74, 75`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65, 67`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation.

Return value	Description
	If this error occurs repeatedly, contact maintenance personnel.
71, 72, 73	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To set a cache residency policy according to the following conditions:

- The file system name is `FS 1`.
- The extensions of the files that are pinned in the cache are `wmv`, `avi`, `mpg`, and `mov`.
- The comment is `Movie files`.
- The policy name is `Movie`.

```
$ sudo arcresidentpolicyset --ext wmv:avi:mpg:mov --comment "Movie files"
--policy Movie --file-system FS_1
```

arcresidentresult (Display the results of cache resident processing)

Synopsis

```
arcresidentresult --file-system file-system-name
arcresidentresult -h
```

Description

Displays the execution results of cache resident policies, which are used to pin files in the cache.

This command can be executed if the acquisition of information about pinned files has been enabled by using the `arcresidentctl` command.

Options and arguments

`--file-system` *file-system-name*
  Specify the name of the file system for which you want to view the results of cache resident processing.

Displayed information

The following table lists the information displayed when this command is executed.

Table 2-60 Information displayed when the arcresidentresult command is executed

Item	Description
`As of`	Displays the date and time that the list of pinned files was refreshed in the following format: *date* (format: *YYYY/MM/DD*) *time* (format: *hh*:*mm*:*ss*)
`Block capacity(GB)`	Displays the total capacity of the file system in GB after cache residency processing is performed.[#]
`Pinned capacity(GB)`	Displays the total capacity of pinned files in GB after cache residency processing is performed.[#]
`Block used(GB)`	Displays the used capacity of the file system in GB after cache residency processing is performed.[#]

[#]

The values are rounded down to 3 decimal places.

Return values

Table 2-61 Return values of the arcresidentresult command

Return value	Description
0	Normal termination
1, 2	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
5, 8, 10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcrestore (Restore a file system whose data has been migrated to the HCP system)

Synopsis

To restore data to a file system that migrates data to the HCP system at the file system level

```
arcrestore [-f] [-v] [--background [--slow|--normal|--fast]]
    [--datamigrate] [--namespace namespace-name] [--skip]
    --file-system file-system-name
```

For restoring the data from another HDI system to a file system that references the data as read-only at the file system level

```
arcrestore [-f] --file-system file-system-name
```

To restore data to a file system that migrates data to the HCP system at the share level

```
arcrestore [-f] [-v] [--background [--slow|--normal|--fast]]
    [--datamigrate] [--skip] --file-system file-system-name
```

For restoring the data from another HDI system to a file system that references the data as read-only at the share level

```
arcrestore [-f] --file-system file-system-name
    --dir directory-name
```

To restore the data migrated to the HCP system at the file system level to a file system that migrates data to the HCP system at the share level

```
arcrestore [-f] [-v] [--skip] --namespace namespace-name
    --file-system file-system-name --dir directory-name
```

To reference the command syntax

```
arcrestore -h
```

Description

This command restores data migrated to the HCP system to a newly created file system or share.

Use this command by following the error recovery procedures in the *Troubleshooting Guide*.

If you want to restore the HCP data migrated at the file system level to a file system that migrates data to the HCP system at the share level, you need to execute this command for each share.

If you execute this command, target data or the parent directory will be restored when a client accesses data that has not been restored. If you specify the `--background` option, all the files can be restored as a stub file by background processing. If you choose this option, you can specify which operation takes priority (the restore operation or processing of I/O requests from clients) by selecting the restore speed. Select the restore method that best fits the manner in which you run the file system.

Make sure that you check the following points about the file system to which the data is restored:

- If you want to change namespace allocation at the file system level to allocation at the share level, you need to create a directory directly under the file system in advance.
- Specify the same namespace as the namespace set for the specified file system.

- If you also wish to restore past versions of files, specify that the past versions of the files are to be made open to clients.
- Even if you execute this command for a home-directory-roaming file system, the home directory is not restored. The home directory is automatically restored the next time an end-user logs in.
- For the read-write-content-sharing file system, the files and directories in the file system are moved to the `.conflict` directory, and then the HCP data is restored.
- For file systems that migrate data to an HCP system at the share level, the data will be restored by using a namespace quota setting. For use without a namespace quota setting, you need to disable the namespace quota setting when creating a share in the GUI after running this restore command.
- The allocated capacity used by the file system is set as 5% of the file systems total capacity. To change the allocated space settings, use this command to run a restoration, and then execute the `arcresvset` command.

Options and arguments

`--background [--slow|--normal|--fast]`

Specify this to select the restore speed and to restore the data by background processing. By selecting the restore speed, you can specify which operation takes priority (the restore operation or processing of I/O requests from clients). If you specify the `--background` option but omit `--slow`, `--normal`, or `--fast`, the `--normal` option is set.

`--slow`

Specify this to perform a restore at a speed slower than the speed when the `--normal` option is specified (rough guide of the processing time: about twice longer), to make the processing of I/O requests from the clients take priority over the restore operation.

`--normal`

Specify this to restore the data at the normal speed.

`--fast`

Specify this to perform a restore at a speed faster than the speed when the `--normal` option is specified (rough guide of the processing time: about half shorter), to make the restore operation take priority over the processing of I/O requests from the clients.

If you rename a directory while stub files are being restored in the background, some files or directories might not be restored. Note that even if this option is specified, the user files that are under the directories that contain the past versions of files migrated to the HCP system are not restored as stub files.

If a failover occurs while a background restoration process is being performed, the process is paused. You can resume the process by mounting the file system for which files are being restored.

`--datamigrate`

    In the event that a file system error causes data imports from other file servers to be interrupted, specify this to resume the imports after the file system is restored. The file system being restored must be set as the destination to which data is imported from other file servers.

`--dir` *directory-name*

    Specify the directory name if you want to restore the data from another HDI system to a file system that references the data as read-only at the share level or if you want to change the level to allocate the namespace from file system to sharing.

`-f`

    Specify this to prevent the confirmation message from appearing.

`--file-system` *file-system-name*

    Specify the name of the restoration destination file system.

`--namespace` *namespace-name*

    Specify the name of the migration-destination HCP system namespace. Only specify this option before starting migration operations.

`--skip`

    If this command is interrupted due to an error, specify this option to restart processing.

    If files or directories are added to or deleted from the file system to be restored after command processing was interrupted, you cannot specify this option. After rebuilding the file system, execute the command without specifying this option.

`-v`

    Specify this to view detailed information.

Return values

Table 2-62 Return values of the arcrestore command

Return value	Description
0	Normal termination
1, 2[#], 15[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2[#], 3, 4, 5, 8, 9, 10, 11[#], 12, 13, 15[#], 16, 17, 18, 20, 21, 23, 40, 66[#], 67[#], 68[#], 70, 71[#], 74, 75[#], 77	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
11[#], 66[#], 67[#], 68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation.

Return value	Description
	If this error occurs repeatedly, contact maintenance personnel.
71#, 72, 73, 75#, 76	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71#, 97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Example

To restore a file system whose data has been migrated to an HCP system according to the following conditions:

- The name of the restoration destination file system is `fs01`.
- The namespace name of the HCP system is `fs01namespace`.
- Data migrated at the file system level to the HCP system is restored to the restoration destination file system.

```
$ sudo arcrestore -f --file-system fs01 --namespace fs01namespace
```

arcresultctl (Manage task log information)

Synopsis
```
arcresultctl --list --file-system file-system-name
arcresultctl --failedlist --policy policy-name
    --file-system file-system-name
arcresultctl [-y] [-f] --del [--policy policy-name]
    --file-system file-system-name
arcresultctl -h
```

Description

Views or deletes log files that are created for each migration task.

This command can be used on the node on which the target file system is mounted.

Options and arguments

`--del`

Specify this to delete log files.

The log file can be deleted if the processing of the target task has finished. By using the `--failedlist` option, you can check that the time at which the processing of the target task finished is displayed for the target task.

`-f`

Specify this to forcibly delete the log files before the target task processing has finished.

If the `--list` option or the `--failedlist` option is specified, this option is ignored.

`--failedlist`

Specify this to view log file information.

`--file-system` *file-system-name*

Specify the file system name.

`--list`

Specify this to view the list of policies corresponding to log files.

`--policy` *policy-name*

Specify the policy name.

`-y`

Specify this to prevent the confirmation message from appearing.

If the `--list` option or the `--failedlist` option is specified, this option is ignored.

Displayed information

The following table lists the information displayed when you specify the `--list` option and execute the command.

Table 2-63 Information displayed when specifying the --list option and executing the arcresultctl command

Item	Description
File system	Displays the file system name.
Policies	Displays the policy names in ascending order.

The following table lists the information displayed when you specify the `--failedlist` option and execute the command.

Table 2-64 Information displayed when specifying the --failedlist option and executing the arcresultctl command

Item	Description
Task Start Time	Displays the task start time.

Item	Description
Task End Time	Displays the task end time. Displays –, if the information cannot be obtained.
File or directory path, message ID, or message	Displays the task failure information for the files and directories. Displays the task failure information for the files and directories.

Return values

Table 2-65 Return values of the arcresultctl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 5, 8, 10, 30, 31, 32, 68, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcresvget (Displaying the reserved space for file systems that link to the HCP system)

Synopsis

```
arcresvget --file-system file-system-name
arcresvget -h
```

Description

This command displays the reserved space used by a file system that is linked to the HCP system.

Options and arguments

--file-system *file-system-name*

Specify the name of the file system where you want to display the reserved space.

Command Reference

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-66 Information displayed when executing the arcresvget command

Item	Description
Reserved space	The reserved space of the file system is displayed as a percentage or in gigabytes.

Return values

Table 2-67 Return values of the arcresvget command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 4, 5, 8, 10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
67, 69	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcresvset (Setting the reserved space for file systems that link to the HCP system)

Synopsis

```
arcresvset --resv-space reserved-space
   --file-system file-system-name
arcresvset -h
```

Description

This command sets the reserved space used by a file system that is linked to the HCP system. The reserved space default settings for a file system that is

linked to the HCP system is 5%. You can use this command to modify the reserved space.

The blocked space and free space on the file system fluctuate when you set the reserved space with this command. Therefore, after setting the reserved space, review the warning threshold settings for the usage of the file system by using the `fsctl` command, or review the threshold at which stub processing is performed by using the `arcreplimitset` command.

Additionally, if expanded the file system capacity, the reserved space will be calculated based on the total storage capacity of the file system after the expansion.

For more information about allocated capacity used when linking systems with an HCP system, see the *Installation and Configuration Guide*.

Options and arguments

`--file-system` *file-system-name*

Specify the name of the file system where you want to set the reserved space.

`--resv-space` *reserved-space*

Specify the reserved space of the file system. The value can be specified as a percentage or as a value in gigabytes. Percentages will be specified in the form `n%`. The letter n refers to a whole number in the range from 0 to 10. Gigabytes will be displayed with `mg` or `mG`. The letter `m` refers to a whole number in the range from 0 to the file system capacity (in gigabytes) x 0.5. If 0%, 0g, or 0G is specified, the space used by the system is not reserved.

If the reserved space was set as a percentage, the upper limit of the reserved space is 40 GB.

Note that when you upgrade the node from a system version older than 5.2.0-00, the reserved space is set to 0%, even if the existing file system links to the HCP system. If you want to modify the reserved space, use this command to adjust the settings again.

Return values

Table 2-68 Return values of the arcresvset command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 3, 4, 5, 8, 10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If

Return value	Description
	this error occurs repeatedly, contact maintenance personnel.
67, 69	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcsslctl (Set the method of communication with the HCP system)

Synopsis

```
arcsslctl {--enable|--disable}
arcsslctl
arcsslctl -h
```

Description

Sets whether to use HTTPS for communication with HCP. The command can also be used to view the current setting.

Options and arguments

`--disable`

Specify this if HTTPS is not to be used for communication with HCP. In this case, `HTTP` is used instead.

`--enable`

Specify this to use HTTPS for communication with HCP. The initial setting is `--enable`.

If you omit all options, the current setting is displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-69 Information displayed when executing the arcsslctl command

Item	Description

Protocol setting	Displays the currently used protocol.
	
	HTTP
	    HTTP is used.
	
	HTTPS
	    HTTPS is used.

Return values

Table 2-70 Return values of the arcsslctl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
66, 67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
71[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
    The command ended abnormally due to multiple causes.

Example

To disable HTTPS as the method of communication with the HCP:

```
$ sudo arcsslctl --disable
```

Command Reference

arctaskstatus (Display the progress status of task pre- and post-processing)

Synopsis

```
arctaskstatus --file-system file-system-name --policy policy-name
arctaskstatus -h
```

Description

Displays the progress status of pre- or post-processing for a migration task.

Options and arguments

`--file-system` *file-system-name*

    Specify the name of the file system for the task for which the progress status of pre- or post-processing is viewed.

`--policy` *policy-name*

    Specify the name of the policy for the task for which the progress status of pre- or post-processing is viewed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-71 Information displayed when executing the arctaskstatus command during pre- or post-processing

Item	Description
Pre Task Start Time or Post Task Start Time	Displays the time when pre- or post-processing started.
Target Files	Displays the number of files that are processed.
Success Files	Displays the number of files that were successfully processed.
Rename Events	Displays the number of times that files are renamed.
Completion Files	Displays the number of files that were processed and the time the last processing finished.

Table 2-72 Information displayed when executing the arctaskstatus command while task processing is performed, after task processing finishes, or after a task is canceled

Item	Description
Task	Displays the task status.

Item	Description

	`Running`
	    Displayed when the task is running.
	`Completed`
	    Displayed when the last task that finished.
	`Skipped`
	    Displayed when the last task was canceled.

Return values

Table 2-73 Return values of the arctaskstatus command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 5, 8, 10, 30, 68, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

arcurlget (Display the URL for the storage location of data in an HCP system)

Synopsis

```
arcurlget file-path-or-directory-path
arcurlget -h
```

Description

Displays the URL for the storage location of a file migrated to an HCP system by specifying a file or directory in the HDI system. If the file or directory specified is in a file system where the data from another HDI system is referenced as read-only, this command displays the URL for the storage location while synchronizing data migrated to the HCP system. Note that if no data is synchronized, the URL for the storage location will not be displayed.

Note:

If the target file is being migrated, the URL of a storage location might be displayed even when the file has not actually been stored in an HCP system.

Options and arguments

file-path-or-directory-path
Specify the absolute path beginning with `/mnt/` to the target file or directory on the HDI system.

Return values

Table 2-74 Return values of the arcurlget command

Return value	Description
0	Normal termination
1, 2, 3	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
5, 10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

avaconfedit (Set scan conditions)

Synopsis
```
avaconfedit --set item:value[,item:value,...]
avaconfedit [-f] --del ExcludePath
    [:path-excluded-from-scans,path-excluded-from-scans,...]
avaconfedit [-y] --del ExcludePath
    [:path-excluded-from-scans,path-excluded-from-scans,...]
avaconfedit --list {item|all}
avaconfedit -h
```

Description

Sets scan conditions.

Before setting the scan conditions, specify the scan software to be used.

Set the same scan conditions for both nodes in the cluster so that both nodes will have the same settings.

Options and arguments

`--del ExcludePath[:` *path-excluded-from-scans* `,` *path-excluded-from-scans* `,...]`

> Specify this to delete a path that will be excluded from scans. After the `--del` option, specify `ExcludePath` followed by a colon (`:`), and then specify the path you want to delete. To specify multiple paths for exclusion from scans, use a comma (`,`) to separate the paths. If you specify no paths for this option, the command clears the list of paths excluded from scans. Note that this option takes effect when the use of Symantec scan software, McAfee scan software, or Trend Micro InterScan Web Security Virtual Appliance is specified.

`-f`

> Specify this to prevent the confirmation message from appearing.

`--list {` *item* `|all}`

> Specify this to view a scan condition. For details about the items that can be specified, see Table 2-75 Information displayed when the --list option is specified for the avaconfedit command, and information that can be set when the --set option is specified on page 2-116. To view all scan conditions, specify `all`.

`--set` *item* `:` *value* `[,` *item* `:` *value* `,...]`

> Specify this to set a scan condition. After the `--set` option followed by a colon (`:`), specify a value. To specify multiple items and values, separate them with commas (`,`). For details about the items and values that can be specified, see Table 2-75 Information displayed when the --list option is specified for the avaconfedit command, and information that can be set when the --set option is specified on page 2-116.

Displayed information and information that can be set

The following table describes the information displayed when the `--list` option is specified and the information that can be set when the `--set` option is specified.

Table 2-75 Information displayed when the --list option is specified for the avaconfedit command, and information that can be set when the --set option is specified

Item	Description

`AccessType` [#1]	Specify this when a scan is to be performed. The initial setting is `RW`.
	`R`
	    A scan is performed when a CIFS client views a file.
	`W`
	    A scan is performed when a CIFS client updates a file.

Item	Description
	RW A scan is performed when a CIFS client views or updates a file.
ScanType[#2]	Specify the type of the files to be scanned. The initial setting is ALL. INCLUDE Files that have the specified extension are scanned. EXCLUDE Files that have extensions other than the specified extension are scanned. ALL All files are scanned.
ExcludePath[#2]	Specify a path or paths to be excluded from scans. Use no more than 1,023 bytes. You can specify a maximum of 256 paths. You can use alphanumeric characters, exclamation marks (!), double quotation marks ("), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), asterisks (*), plus signs (+), commas, (,), hyphens (-), periods (.), forward slashes (/), colons (:), semicolons (;), left angle brackets (<), equal signs (=), right angle brackets (>), question marks (?), at marks (@), left square brackets ([), backslashes (\), right square brackets (]), carets (^), underscores (_), grave accent marks (`), left curly brackets ({), vertical bars (|), right curly brackets (}), and tildes (~). You can also specify multibyte characters.
EnableLimitSize[#2#3]	Specify whether to set the maximum size of a file that can be scanned. The initial setting is ENABLE. ENABLE The maximum size of a file that can be scanned is set. DISABLE The maximum size of a file that can be scanned is not set.
LimitSize[#2#3]	Specify the maximum size of a file that can be scanned in the range from 1 to 9,999 (units: MB). The initial setting is 2047.
OverSizeAccess[#2#3]	Specify whether to allow clients to access files whose size exceeds the upper limit when a limit is placed on the size of a file that can be scanned. The initial setting is ENABLE. ENABLE Clients are allowed to access files whose size exceeds the upper limit. DISABLE Clients are not allowed to access files whose size exceeds the upper limit.
InfectedAction[#2#4]	Specify the action to be taken when an infected file that cannot be corrected by the scan server is detected. The initial setting is DELETE. ALLOW Allow access from a client to the infected file. DENY Deny access from a client to the infected file.

Item	Description
	DELETE Delete the infected file.

Notify[#2]	Specify whether to send notifications about the detection of infected files when either SNMP or email notifications (containing error information) are enabled. The initial setting is DISABLE.
	
	ENABLE
	
	    Notifications are sent.
	
	DISABLE
	
	    Notifications are not sent.

NotifyType	If SNMP notification or email notification of error information is set up, specify this item to set the notification method for errors that occur during real-time scans. The initial setting is OFF.
	
	OFF
	
	    Notifications are not sent.
	
	ONCEADAY
	
	    Information reported by Anti-Virus Enabler is checked once a day, and a notification is sent when information is output about the files for which an error occurred during a real-time scan. The time for checking for the Anti-Virus Enabler report is set in NotifyTime.
	
	EVERYTIME
	
	    A notification is sent when information about the files for which an error occurred during a real-time scan is output to the Anti-Virus Enabler report.
	
	The following list shows the types of errors for which notifications are sent. Note that, if you specify EVERYTIME, no notification will be sent for server connect error.
	
	scan size exceeded
	
	    This is output when the upper limit on the size of the files to be scanned is exceeded.
	
	scan timeout
	
	    This is output when a timeout occurs during a scan.
	
	internal error
	
	    This is output when an error in internal processing occurs.
	
	server connect error
	
	    This is output when a connection to the scan server cannot be established.
	
	container violation
	
	    This is output when container files cannot be scanned because of the scan server settings.
	
	server too busy
	
	    This is output when there are too many scan requests for the scan server to process.
	
	scan server error
	
	    This is output when an error occurs on the scan server.

Item	Description
NotifyTime	The time for checking for Anti-Virus Enabler report information. The initial setting is `05:00`. This item takes effect when `NotifyType` is set to `ONCEADAY`. For details about Anti-Virus Enabler report information, see the *Installation and Configuration Guide*. Specify the value in `hhmm` format. A value is displayed in `hh:mm` format.

ScanWorm	Specify whether to scan WORM files. The initial setting is `DISABLE`.
	
	ENABLE
	    WORM files are scanned.
	
	DISABLE
	    WORM files are not scanned.

ScanStub	Specify whether to scan stub files. The initial setting is `ENABLE`.
	
	ENABLE
	    Stub files are scanned.
	
	DISABLE
	    Stub files are not scanned.

Timeout	Specify, in a range from 0 to 600 (units: seconds), the timeout value after the HDI system issues a connection request to the scan server. The initial setting is `30`.
ScanTimeout	Specify, in a range from 1 to 1,800 (units: seconds), the timeout value after the HDI system issues a scan request to the scan server. The initial setting is `60`.
StubScanTimeout	Specify, in a range from 0 to 1,800 (units: seconds), the timeout value after the HDI system issues a scan request for stub files to the scan server. The initial setting is `900`.
Retry	Specify, in a range from 0 to 32, the number of times the scan server to be used can be switched if a timeout or an error occurs during connection with the scan server. The initial setting is `1`.

ScanningFailsProcedure	Specify the action to be taken if a scan fails. The initial setting is `ALLOW`.
	
	ALLOW
	    Allows access to the files for which a scan failed.
	
	DENY
	    Denies access to the files for which a scan failed.

ScanServerAllClosedProcedure	Specifies whether to only give a client permission to read files that do not need to be scanned if all scan server connections are closed. The initial setting is `DENY`.
	
	ALLOW
	    Only gives a client permission to read files that do not need to be scanned. This argument is valid when `DENY` is specified for `ScanningFailsProcedure`.
	
	DENY
	    Denies any client access to read a file.

Item	Description
`PollingInterval`	Specify, in a range from 1 to 86,400 (units: seconds), the polling interval for checking the status of the scan server. The initial setting is `300`.
`ScanCacheSize` #2	Specify, in a range from 1 to 64 (units: MB), the cache capacity for storing information about files that are determined by the scan not to be infected. The initial setting is `8`. 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.

`StatInfo`	Specify whether to output Anti-Virus Enabler user statistics. The initial setting is `OFF`.
	
	For details about Anti-Virus Enabler user statistics, see the *Installation and Configuration Guide*.
	
	`ON`
	
	Anti-Virus Enabler user statistics are output.
	
	`OFF`
	
	Anti-Virus Enabler user statistics are not output.

`EnableAccessLog`	Specify whether to output scan execution log information to the Anti-Virus Enabler library trace log file (`antiviruslib.trace`). The initial setting is `ENABLE`.
	
	`ENABLE`
	
	Scan execution log information is output.
	
	`DISABLE`
	
	Scan execution log information is not output.

#1:

   If Trend Micro ServerProtect 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 set `R` for `AccessType`.

#2:

   When Symantec scan software, McAfee scan software, or Trend Micro InterScan Web Security Virtual Appliance is used, this item can be displayed and specified.

#3:

   When Symantec scan software is used to scan a file that is 2 GB or larger, specify the following settings:

   ○ Specify 2,047 or less for `LimitSize`.

   ○ Specify `ENABLE` for both `EnableLimitSize` and `OverSizeAccess`.

If you specify different scan conditions, CIFS clients cannot access files that are 2 GB or more. When a scan fails, the scan server connection is closed.

#4:

When Trend Micro InterScan Web Security Virtual Appliance is used, if an access to a file is blocked due to the scan server setting, the action same as that taken at infected file detection is taken.

Return values

Table 2-76 Return values of the avaconfedit command

Return value	Description
0	Normal termination
1, 2, 3, 4, 17	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 16	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To exclude paths that contain `/mnt/fs01` from a scan:

```
$ sudo avaconfedit --set ExcludePath:/mnt/fs01
```

To set up the scan server according to the following conditions:

- If a timeout or an error occurs during connection to the scan server, the scan server to be used is switched a maximum of two times.
- Access to the files for which a scan failed is denied.

```
$ sudo avaconfedit --set Retry:2,ScanningFailsProcedure:Deny
```

avaextensionsedit (Set extensions for the files to be scanned or the files not to be scanned)

Synopsis

```
avaextensionsedit --add [--noextension {include|exclude}]
    include=extension[:extension...]
    exclude=extension[:extension...]
avaextensionsedit --add [--noextension {include|exclude}]
    {include=extension[:extension...]|
     exclude=extension[:extension...]}
avaextensionsedit [-y] --del [--noextension {include|exclude}]
    include=extension[:extension...]
    exclude=extension[:extension...]
avaextensionsedit [-y] --del [--noextension {include|exclude}]
    {include=extension[:extension...]|
     exclude=extension[:extension...]}
avaextensionsedit --list [include|exclude]
avaextensionsedit -h
```

Description

Sets the extensions for the files to be scanned or the files not to be scanned.

This command can be used when Symantec scan software, McAfee scan software, or Trend Micro InterScan Web Security Virtual Appliance is specified for use.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Options and arguments

`--add [--noextension {include|exclude}] include=` *extension* `[:` *extension* `...]` `exclude=` *extension* `[:` *extension* `...]`

Specify the extensions of the files to be scanned or the files not to be scanned. For *extension*, you can use 0 to 16 characters. A maximum of 255 extensions can be registered. You cannot specify upper-case alphabetic characters. To specify multiple extensions, use a colon (`:`) to separate the extensions. You can specify the following values.

`include=` *extension* `[:` *extension* `...]`

Specify the extension of a file to be scanned. To scan files without extensions, specify `include` for the `--noextension` option.

`exclude=` *extension* `[:` *extension* `...]`

Specify the extension of a file not to be scanned. To exclude files without extensions from a scan, specify `exclude` for the `--noextension` option.

`--del [--noextension {include|exclude}] include=` *extension* `[:` *extension* `...]` `exclude=` *extension* `[:` *extension* `...]`

Specify the extension of a file for which the scan setting will be canceled. To specify multiple extensions, use a colon (:) to separate the extensions. You can specify the following values.

include= *extension* [: *extension* ...]

Specify the extension for which the scan setting will be canceled. To cancel the scan setting for files without extensions, specify `include` for the `--noextension` option.

exclude= *extension* [: *extension* ...]

Specify the extension for which exclusion from a scan is canceled. To cancel exclusion for files without extensions, specify `exclude` for the `--noextension` option.

--list [include|exclude]

Specify this to view the extensions of files to be scanned or files not to be scanned. You can specify the following values:

include

Specify this to view the extensions of files to be scanned.

exclude

Specify this to view the extensions of files not to be scanned.

Omit both `include` and `exclude` to view the extensions of the files to be scanned and the files not to be scanned.

If multiple extensions have been registered, the extensions displayed are separated by a colon (:). If a file without an extension is registered, the file name ends with two colons (::).

Example: `IncludeExtensions :.avw:.ppt::`

Displayed information

The following table lists the information displayed by this command when the `--list` option is specified.

Table 2-77 Information displayed when executing the avaextensionsedit command with the --list option specified

Item	Description
IncludeExtensions	The extensions of files to be scanned are displayed.
ExcludeExtensions	The extensions of files not to be scanned are displayed.

Return values

Table 2-78 Return values of the avaextensionsedit command

Return value	Description
0	Normal termination
1, 2, 3, 17	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 12, 16	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To register files without extensions and with extensions (`.avw` or `.ppt`) as files to be scanned:

```
$ sudo avaextensionsedit --add --noextension include include=avw:ppt
```

To add files that have extensions (`.pdf` or `.txt`) as files not to be scanned:

```
$ sudo avaextensionsedit --add exclude=pdf:txt
```

avascanengineset (Select the scan software to be used)

Synopsis

```
avascanengineset [-y] {TMSP|TMIWSVA|SPE|MAVSE}
avascanengineset -h
```

Description

Selects the scan software to be used.

If the real-time scan service is enabled, you should disable it before executing the command. Note that if you execute this command to change the scan software, scan conditions and scan server information are initialized.

Use the same scan software for both nodes in the cluster so that both nodes will have the same settings.

Options and arguments

`{TMSP|TMIWSVA|SPE|MAVSE}`

> Specify the scan software to be used. You can specify one of the following scan software names:

> `TMSP`
>
>> Specify this to use Trend Micro ServerProtect.

> `TMIWSVA`
>
>> Specify this to use Trend Micro InterScan Web Security Virtual Appliance.

> `SPE`
>
>> Specify this to use Symantec scan software.

> `MAVSE`
>
>> Specify this to use McAfee scan software.

Return values

Table 2-79 Return values of the avascanengineset command

Return value	Description
0	Normal termination
1, 3	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
15	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To specify the use of Symantec scan software:

```
$ sudo avascanengineset SPE
KAQV30072-Q If a different scanning software is chosen, the scan
conditions will be re-initialized and the scan server information will be
deleted.
Are you sure you want to change the scanning software? (y/n)
```

avaserveradd (Add scan server information)

Synopsis

```
avaserveradd scan-server-name:port-number
    [,scan-server-name:port-number...]
avaserveradd -h
```

Description

Adds scan server information.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Options and arguments

scan-server-name : *port-number* [, *scan-server-name* : *port-number* ...]
> Specify the scan server name followed by a colon (:), and then specify the port number to be used for the scan server. To add multiple scan servers, use a comma (,) to separate the scan servers. You can add a maximum of 32 scan servers.

> *scan-server-name*
>> Specify the host name, IP address, or domain name of the scan server.

> *port-number*
>> Specify the port number to be used for the scan server.

Return values

Table 2-80 Return values of the avaserveradd command

Return value	Description
0	Normal termination
1, 3, 5, 17	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To add scan server information under the following conditions:

- The scan server name is `scanserver`.
- The port number used for the scan server is `1024`.

```
$ sudo avaserveradd scanserver:1024
```

avaserverdel (Delete scan server information)

Synopsis

```
avaserverdel [-y] scan-server-name [,scan-server-name...]
avaserverdel [-y] --all
avaserverdel -h
```

Description

Deletes scan server information.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Options and arguments

`--all`

Specify this to delete the information for all scan servers.

scan-server-name `[,` *scan-server-name* `...]`

Specify the host name, IP address, or domain name of the scan server. To specify multiple scan servers for deletion, use a comma (`,`) to separate the scan servers.

Return values

Table 2-81 Return values of the avaserverdel command

Return value	Description
0	Normal termination
1, 2, 3, 17	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
11	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

avaserveredit (Change scan server information)

Synopsis

```
avaserveredit --server new-scan-server-name
    --port new-port-number scan-server-name
avaserveredit {--server new-scan-server-name|
    --port new-port-number} scan-server-name
avaserveredit -h
```

Description

Changes the scan server information.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Options and arguments

--port *new-port-number*
    Specify the new port number.

--server *new-scan-server-name*
    Specify the new host name, IP address, or domain name of the scan server.

scan-server-name
    Specify the host name, IP address, or domain name of the scan server that will be changed.

Return values

Table 2-82 Return values of the avaserveredit command

Return value	Description
0	Normal termination
1, 2, 3, 17	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.

Return value	Description
21	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To change the scan server information under the following conditions:

- ○ Change the scan server name from `scanserver` to `192.168.4.12`.
- ○ Change the port number used for the scan server to `1344`.

```
$ sudo avaserveredit --server 192.168.4.12 --port 1344 scanserver
```

avaservicestart (Enable the real-time scan service)

Synopsis

```
avaservicestart [-h]
```

Description

Enables the real-time scan service.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

The following conditions must be met before you can use this command:

- The scan software that will be used has been set by using the `avascanengineset` command.
- The scan server has been registered by using the `avaserveradd` command.

Note that after you enable the real-time scan service, restart the CIFS service.

Return values

Table 2-83 Return values of the avaservicestart command

Return value	Description
0	Normal termination
1, 14	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
13, 20, 65[#], 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
18	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
65[#], 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

avaservicestatus (Display the status of the real-time scan service)

Synopsis

```
avaservicestatus [-h]
```

Description

Displays the status of the real-time scan service.

Displayed information

The following table lists the information displayed by this command.

Table 2-84 Information displayed when executing the avaservicestatus command

Item	Description
ScanEngine	Displays the name of the scan software being used.

Item	Description
	If no scan software has been set, – is displayed.
	`SPE` Symantec scan software is being used.
	`TMSP` Trend Micro ServerProtect is being used.
	`TMIWSVA` Trend Micro InterScan Web Security Virtual Appliance is being used.
	`MAVSE` McAfee scan software is being used.

`RealTimeScan`	Displays the status of the real-time scan service.
	
	`Running`
	
	The real-time scan service is enabled.
	
	`Stopped`
	
	The real-time scan service is disabled.

`List of Scanner Servers`	Displays the scan server information in the following format:
	
	scan-server-name port-number scan-server-status
	
	The status of the scan server is displayed as described below. If the real-time scan is disabled, – is displayed.
	
	`Normal`
	
	The scan server is running normally.
	
	`Blocked (Server not found)`
	
	The connection to the scan server has been blocked because the scan server was not found.
	
	Make sure that the IP address, domain name, or host name of the scan server is correct.
	
	`Blocked (Access is impossible)`
	
	The connection to the scan server has been blocked for the following reason: the port number set for the HDI system differs from the port number set for the scan server, the real-time scan service is not available, or the scan software specified for the HDI system differs from the scan software installed on the scan server.
	
	Make sure that the IP address, domain name or host name, 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, and that the scan software of the HDI system is correctly set.
	
	`Blocked (Time-out)`
	
	The connection to the scan server has been blocked because the scan server timed out.
	
	Make sure that an error has not occurred in the network.
	
	`Blocked (Version conflict)`
	
	The connection to the scan server has been blocked because the protocol version of the HDI system is not compatible with the protocol version of the scan server.
	
	Obtain all the log files, and then contact maintenance personnel.

Item	Description

	`Blocked (License expired)`
	
	The connection to the scan server has been blocked because the license of the scan software installed on the scan server is no longer valid.
	
	Make sure that the scan software license is current.
	
	`Blocked (Scanner server error)`
	
	The connection to the scan server has been blocked because an error occurred on the scan server.
	
	Correct the error.
	
	`Blocked (Under registration)`
	
	Information for the registered scan server is being applied to the HDI system.
	
	Wait several minutes, and then re-execute the command to check the status of the server.
	
	`Blocked (Invalid protocol)`
	
	The communication protocol is inconsistent with that of Hitachi Server Protect Agent installed on the scan server.
	
	Check the version of the installed Hitachi Server Protect Agent, and then install the correct version of Hitachi Server Protect Agent.
	
	`Blocked (Scanning software is not installed)`
	
	Scan software is not installed on the scan server.
	
	Install scan software.
	
	`Blocked (Scanning software service has stopped)`
	
	The software service installed on the scan server has stopped. Start the service.
	
	`Blocked (Access user info. is not registered)`
	
	No user information for accessing the CIFS share is registered on the scan server. Register the necessary information.
	
	`Blocked (Access user info. is invalid)`
	
	Invalid user information for accessing the CIFS share is registered on the scan server. Correct the user information.
	
	`Deleting`
	
	An attempt was made to delete the scan server while the CIFS client was being used. The scan server will be deleted when the use of the CIFS client has finished processing.
	
	`Error (System failure)`
	
	An error might have occurred, or an attempt to update the status failed in HDI system.
	
	Wait for the time that was specified in `PollingInterval` by using the `avaconfedit` command to pass, and then check the status again. If the status still cannot be updated, obtain all the log files, and then inform maintenance personnel.

Return values

Table 2-85 Return values of the avaservicestatus command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

avaservicestop (Disable the real-time scan service)

Synopsis

```
avaservicestop [-h]
```

Description

Disables the real-time scan service.

After you disable the real-time scan service, restart the CIFS service.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Return values

Table 2-86 Return values of the avaservicestop command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
19	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

bbuschlget (Display the diagnostics schedule for an internal RAID battery or a super capacitor)

Synopsis

```
bbuschlget [-h]
```

Description

This command can be used in single-node configurations where a user disk has been created from an internal hard disk (excluding HDI Remote Server).

This command displays the diagnostics schedule for an internal RAID battery or a super capacitor installed as an external power supply to safeguard RAID card caching.

Displayed information

The following table lists the information displayed when this command is executed.

Table 2-87 Information displayed when the bbuschlget command is executed

Item	Description
Schedule settings for BBU relearn	Displays information about the diagnostics schedule for the internal RAID battery or the super capacitor.
Day of the month	Displays the date on which diagnostics of the internal RAID battery or the super capacitor are scheduled to take place, as a value from 1 to 31.
Time	Displays the time at which diagnostics of the internal RAID battery or the super capacitor are scheduled to take place, in the format hh:mm.

Return values

Table 2-88 Return values of the bbuschlget command

Return value	Description
0	Normal termination

Return value	Description
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

bbuschlset (Set the diagnostics schedule of the internal RAID battery or the super capacitor)

Synopsis

```
bbuschlset -S diagnostics-schedule
bbuschlset -h
```

Description

This command can be used in single-node configurations where a user disk has been created from an internal hard disk (excluding HDI Remote Server).

Set the diagnostics schedule for an internal RAID battery or a super capacitor provided to safeguard RAID card caching capabilities.

The diagnostics process involves discharging the internal RAID battery or the super capacitor completely, and then charging it again to determine the condition of the device. This process takes between 1 and 5 minutes for a super capacitor. For an internal RAID battery, diagnostics can take a full day, during which time write-through caching is set for disk write operations to OS disks and shared LUs. Schedule diagnostics for a time when the resulting drop in performance will have the least impact on system operation.

Options and arguments

-S *diagnostics-schedule*

Specify the diagnostics schedule for the internal RAID battery or the super capacitor in the following format:

date-time

For *date*, specify a value in the range from 1 to 31. If you specify a value from 29 to 31, diagnostics will only take place in months that contain the specified date.

Specify an integer in the range of 0 to 23 for the *time*.

The default is `1-0` (diagnostics take place at 0:00 on the first day of every month).

Return values

Table 2-89 Return values of the bbuschlset command

Return value	Description
0	Normal termination
1, 2	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To schedule diagnostics at 1:00 on the 15th of every month for an internal RAID battery or a super capacitor:

```
$ sudo bbuschlset -S 15-01
```

bmcctl (Manage BMC port interfaces)

Synopsis (for cluster configurations)

```
bmcctl -a {fixed-IP-address1[:[fixed-IP-address2]]|
    [fixed-IP-address1]:fixed-IP-address2} -n netmask [-g gateway]
bmcctl --account
bmcctl
```

Synopsis (for single node configurations excluding HDI Remote Server)

```
bmcctl -a IP-address [-g gateway]
bmcctl --account
bmcctl
```

Synopsis (to reference the command syntax)

```
bmcctl -h
```

Description

Sets up an interface for a BMC port. You can also use this command to view the current settings.

This command cannot set IP addresses in IPv6 format.

To change the network address in a configuration in which BMC ports are connected to IP switches, after changing the management port settings, you have to change the BMC port settings so that the BMC ports use the same network address as the management port.

Options and arguments

-a { *fixed-IP-address1* [:[*fixed-IP-address2*]]|[*fixed-IP-address1*]: *fixed-IP-address2* }

> The above syntax is for cluster configurations.
>
> Specify the fixed IP addresses of the BMC port. Specify the IP address of the node on which the command is executed for *fixed-IP-address1*, and specify the fixed IP address of the other node for *fixed-IP-address2*. Note that if you are only changing one of the fixed IP addresses, you can omit the specification of the other IP address.

-a *IP-address*

> The above syntax is for single-node configurations.
>
> Specify the IP address of the BMC port.

--account

> Specify this option to set the BMC account of the node that you are logged in. This option can be used when the node is Compute Rack. Note that you can use the `hwstatus` command to check the product name of the node.

-g *gateway*

> Specify the IP address of the default gateway. If you specify two double quotation marks ("") or two single quotation marks (''), the current default gateway setting is canceled.

-n *netmask*

> Specify a netmask. The value you specify is used as the netmask of the fixed IP addresses.
>
> If you omit all the options, the current settings are displayed.

Displayed information

The following table lists the information displayed when this command is executed in a cluster configuration. Note that if you have not set an interface for the BMC port, only the port name is displayed.

Table 2-90 Information displayed when the bmcctl command is executed in a cluster configuration

Item	Description
`Interface`	Displays the port name.
node-number(host-name)	Displays information about the cluster node you are logged in to. This information is displayed in the following format: *node-number(host-name)*
`Fixed IP addr` [1]	Displays the fixed IP address of the node you are logged in to.
`Netmask` [1]	Displays the netmask of the node you are logged in to.
`Gateway` [1]	Displays the IP address of the gateway. If a default gateway is not set, `0.0.0.0` is displayed.
node-number(host-name)	Displays information about the other node in the cluster. This information is displayed in the following format: *node-number(host-name)*
`Fixed IP addr` [1] [2]	Displays the fixed IP address of the other node in the cluster.
`Netmask` [1] [2]	Displays the netmask of the other node in the cluster.
`Gateway` [1] [2]	Displays the IP address of the gateway. If a default gateway is not set, `0.0.0.0` is displayed.

#1:
   If the fixed IP address, netmask, or gateway IP address cannot be obtained, `Invalid(None)` is displayed instead.

#2:
   If the information obtained from the other node contains an error, `Invalid(`*invalid-value*`)` is displayed. If information cannot be obtained from the other node, `Unknown` is displayed.

Note:
   When the node model is D51B-2U, `0.0.0.0` might be displayed instead of the set IP address if you set up the BMC port interface and then try to view the current setting immediately.
   When this symptom occurs, wait a while, and then try again.

The following table lists the information displayed when this command is executed in a single-node configuration. Note that if you have not set an interface for the BMC port, only the port name is displayed.

Table 2-91 Information displayed when the bmcctl command is executed in a single-node configuration

Item	Description
Interface	Displays the port name.
IP address #	Displays the IP address.
Netmask #	Displays the netmask.
Gateway #	Displays the IP address of the gateway. If a default gateway is not set, 0.0.0.0 is displayed.

\#

   If the IP address, netmask, or gateway IP address cannot be obtained, Invalid(None) is displayed instead.

Return values

Table 2-92 Return values of the bmcctl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 71#	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71#	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
98, 99	An error, such as a temporary hardware error, might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Example

To specify the interface for the BMC port according to the following conditions:

- ○ The static IP addresses are `172.19.23.31` and `172.19.23.32`.
- ○ The netmask is `255.255.255.0`.

```
$ sudo bmcctl -a 172.19.23.31:172.19.23.32 -n 255.255.255.0
```

cachedbadbbuget (Display information about RAID card cache operations)

Synopsis

```
cachedbadbbuget [-h]
```

Description

This command can be used in single-node configurations that are not connected to any storage systems (excluding HDI Remote Server).

This command displays information about RAID card cache operations.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-93 Information displayed when executing the cachedbadbbuget command

Item	Description		
`Default Cache Policy`	The values set for RAID card cache operations are displayed in the following format: *setting-for-disk-write-cache-operations*, *setting-for-disk-read-cache-operations*, Direct, *setting-for-disk-write-cache-operations-when-the-internal-RAID-battery-or-the-super-capacitor-is-low*		
	setting-for-disk-write-cache-operations	The value set for disk-write cache operations is displayed. `WriteBack` Displayed when write-back caching is set. `WriteThrough` Displayed when write-through caching is set.	
	setting-for-disk-read-cache-operations	The value set for disk-read cache operations is displayed. `ReadAdaptive`	

Item	Description
	Displayed when adaptive readahead caching is set. `ReadAheadNone` Displayed when readahead caching is not set.

setting-for-disk-write-cache-operations-when-the-internal-RAID-battery-or-the-super-capacitor-is-low	The value set for disk-write cache operations to a user disk when the internal RAID battery or the super capacitor is low is displayed.
	
	`Write Cache OK if Bad BBU`
	
	Displayed when write-back caching is set.
	
	`No Write Cache if Bad BBU`
	
	Displayed when write-through caching is set.
	
	Note that write-through caching is always set for disk-write cache operations to OS disks and cluster management LUs when the internal RAID battery or the super capacitor is low.

`Current Cache Policy`	The values set for RAID card cache operations in the current cache policy are displayed in the following format: *setting-for-disk-write-cache-operations*, *setting-for-disk-read-cache-operations*, Direct, *setting-for-disk-write-cache-operations-when-the-internal-RAID-battery-or-the-super-capacitor-is-low*

setting-for-disk-write-cache-operations	The value set for disk-write cache operations is displayed.
	
	`WriteBack`
	
	Displayed when write-back caching is set for the current cache policy.
	
	`WriteThrough`
	
	Displayed when write-through caching is set for the current cache policy.

setting-for-disk-read-cache-operations	The value set for disk-read cache operations is displayed.
	
	`ReadAdaptive`
	
	Displayed when adaptive readahead caching is set for the current cache policy.
	
	`ReadAheadNone`
	
	Displayed when readahead caching is not set for the current cache policy.

setting-for-disk-write-cache-operations-when-the-internal-RAID-battery-or-the-	The value set for disk-write cache operations to a user disk when the internal RAID battery or the super capacitor is low is displayed. `Write Cache OK if Bad BBU`

Item	Description	
	super-capacitor-is-low	Displayed when write-back caching is set.
		`No Write Cache if Bad BBU`
		Displayed when write-through caching is set.
		Note that write-through caching is always set for disk-write cache operations to OS disks and cluster management LUs when the internal RAID battery or the super capacitor is low.

Return values

Table 2-94 Return values of the cachedbadbbuget command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

cachedbadbbuset (Configure the setting for RAID card cache operations)

Synopsis

```
cachedbadbbuset {--wb|--wt}
cachedbadbbuset -h
```

Description

This command can be used in single-node configurations that are not connected to any storage systems (excluding HDI Remote Server).

This command configures the setting for RAID card cache operations to a user disk when the internal RAID battery or the super capacitor is low.

Note that write-through caching is always set for disk-write cache operations to OS disks and cluster management LUs when the internal RAID battery or the super capacitor is low.

Options and arguments

`--wb`

Specify this to use write-back caching for disk-write cache operations to a user disk when the internal RAID battery or the super capacitor is low. When write-back caching is set, system performance is improved but any data not written to the internal HDDs might be lost if an error occurs.

When you specify this option and execute a command, the following message is displayed if the command executed is the `cachedbadbbuget` command.

```
Default Cache Policy: currently-specified-cache-write-mode,
currently-specified-cache-read-mode, Direct, Write Cache OK if
Bad BBU
```

`--wt`

Specify this to use write-through caching for disk-write cache operations to a user disk when the internal RAID battery or the super capacitor is low. The default value is `--wt`.

When you specify this option and execute a command, the following message is displayed if the command executed is the `cachedbadbbuget` command.

```
Default Cache Policy: currently-specified-cache-write-mode,
currently-specified-cache-read-mode, Direct, No Write Cache if
Bad BBU
```

Return values

Table 2-95 Return values of the cachedbadbbuset command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To use write-back caching for disk-write cache operations to a user disk when the internal RAID battery or the super capacitor is low:

```
$ sudo cachedbadbbuset --wb
```

certctl (Public key certificate-related settings)

Synopsis

To create a certificate signing request (CSR) file 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]
```

To create the keystore

```
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
```

To set a public key certificate in the node

```
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]
```

To initialize a public key certificate that is set in a node

```
certctl --reset [-y]
```

To reference the command syntax

```
certctl -h
```

Description

Creates a certificate signing certificate (CSR) and private key to be sent to the certificate authority, or sets a public key certificate obtained from a certificate authority in a node. You can also initialize the settings.

The file created by using this command will be output to the SSH account home directory (/home/nasroot). The file cannot have the same name as an existing file in the /home/nasroot directory.

When specifying options and arguments for this command, follow the instructions from the certificate authority (CA) to which the certificate signing request (CSR) is sent.

For details about setting up a public key certificate, see the *Administrator's Guide*.

Notes:

- If setting up a public key certificate in a node, or if initializing a public key certificate, performing GUI or API operations is temporarily impossible.

- If creating a private key or certificate signing request (CSR), the total number of characters specified in the following options must not exceed 160 : `--common-name`, `--locality`, `--organization`, `--state-province`, `--unit`

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

Options and arguments

`--cert` *public-key-certificate-file-name*

Specify the name of the public key certificate file obtained from the certificate authority (CA).

`--common-name` *host-name-of-node*

Specify the host name of the node (FQDN). If you omit this option, an empty character string is specified.

`--country` *country-name*

Specify a two-letter country code from the country codes defined by ISO3166-1. If you omit this option, an empty character string is specified.

`--create-cert`

Specify this option if you want to create a private key and certificate signing request (CSR).

This option must be specified together with one or more of the following optional options : `--common-name`, `--country`, `--email`, `--locality`, `--organization`, `--state-province`, `--unit`

`--create-pkcs`

Specify this option if you want to create a keystore file (in PKCS# 12 format).

`--dest-csr` *CSR-file-name*

Specify the name of the certificate signing request (CSR) that you want to create, by using 1-256 characters.

You can use alphanumeric characters, exclamation marks (`!`), hash marks (`#`), dollar signs (`$`), percent signs (`%`), ampersands (`&`), single quotation marks (`'`), left parentheses (`(`), right parentheses (`)`), plus signs (`+`), commas (`,`), hyphens (`-`), periods (`.`), semicolons (`;`), equal signs (`=`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), carets (`^`),

underscores (_), grave accent marks (`), left curly brackets ({), right curly brackets (}), tildes (~), and spaces. Note that `.rand`, and `.rnd` cannot be specified for a file name.

`--dest-key` *private-key-file-name*

Specify the name of the private key file that you want to create, by using 1-256 characters.

You can use alphanumeric characters, exclamation marks (!), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), plus signs (+), commas (,), hyphens (-), periods (.), semicolons (;), equal signs (=), at marks (@), left square brackets ([), right square brackets (]), carets (^), underscores (_), grave accent marks (`), left curly brackets ({), right curly brackets (}), tildes (~), and spaces. Note that `.rand`, and `.rnd` cannot be specified for a file name.

`--dest-keystore` *keystore-file-name*

Specify the name of the keystore file (in PKCS# 12 format) that you want to create, by using 1-256 characters.

You can use alphanumeric characters, exclamation marks (!), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), plus signs (+), commas (,), hyphens (-), periods (.), semicolons (;), equal signs (=), at marks (@), left square brackets ([), right square brackets (]), carets (^), underscores (_), grave accent marks (`), left curly brackets ({), right curly brackets (}), tildes (~), and spaces. Note that `.rand`, and `.rnd` cannot be specified for a file name.

`--email` *E-mail-address*

Specify the email address of no more than 40 characters. If you omit this option, an empty character string is specified.

`--intermediate-cert` *intermediate-certificate-authority-certificate-file-name*

Specify the name of the intermediate certificate authority certificate file if you obtain the file together with a public key certificate from the certificate authority (CA).

`--key` *private-key-file-name*

Specify the name of the private key file.

`--key-passwd` *private-key-password*

Specify a password for the private key file to be created. The password must be 4 to 64 characters long.

You can use alphanumeric characters.

When specifying this option together with the `--create-pkcs` or `--set-cert` option, specify the same password as that used when specifying this option together with the `--create-cert` option.

`--keystore` *keystore-file-name*

Specify the name of the keystore file (JKS format) imported on a machine with Oracle JDK 6 or later installed.

`--locality` *locality-name*

Specify the name of the city, town, or other locality. If you omit this option, an empty character string is specified.

You can use alphanumeric characters, single quotation marks (`'`), left parentheses (`(`), right parentheses (`)`), plus signs (`+`), commas (`,`), hyphens (`-`), periods (`.`), forward slashes (`/`), colons (`:`), equal signs (`=`), question marks (`?`), and spaces.

`--organization` *company-or-organization-name*

Specify the name of the company or organization. If you omit this option, an empty character string is specified.

You can use alphanumeric characters, single quotation marks (`'`), left parentheses (`(`), right parentheses (`)`), plus signs (`+`), commas (`,`), hyphens (`-`), periods (`.`), forward slashes (`/`), colons (`:`), equal signs (`=`), question marks (`?`), and spaces.

`--passwd` *keystore-password*

Specify a password for the keystore file (in PKCS# 12 format) to be created. The password must be 1 to 50 characters long.

You can use alphanumeric characters, single quotation marks (`'`), left parentheses (`(`), right parentheses (`)`), plus signs (`+`), commas (`,`), hyphens (`-`), periods (`.`), forward slashes (`/`), colons (`:`), equal signs (`=`), question marks (`?`), and spaces.

`--reset`

Specify this option if you want to initialize the public key certificate that is set in the node.

This option is applied to the node on which the command is executed. In a cluster configuration, you must specify this option on both nodes before executing the command.

`--set-cert`

Specify this option if you want to set up the public key certificate in the node.

This option is applied to the node on which the command is executed. This command must be executed by specifying this option on both nodes in cluster configurations.

`--state-province` *state-or-province-name*

Specify the name of the state or province. If you omit this option, an empty character string is specified.

You can use alphanumeric characters, single quotation marks (`'`), left parentheses (`(`), right parentheses (`)`), plus signs (`+`), commas (`,`), hyphens (`-`), periods (`.`), forward slashes (`/`), colons (`:`), equal signs (`=`), question marks (`?`), and spaces.

`--unit` *organization-or-department-unit-name*

Specify the name of the organizational unit or department unit. If you omit this option, an empty character string is specified.

You can use alphanumeric characters, single quotation marks ('), left parentheses ((), right parentheses ()), plus signs (+), commas (,), hyphens (-), periods (.), forward slashes (/), colons (:), equal signs (=), question marks (?), and spaces.

Return values

Table 2-96 Return values of the certctl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Examples

Creating a certificate signing request (CSR) file and private key with the following conditions:

- The name of the private key file is `httpsdkey.pem`.
- The name of the certificate signing request (CSR) file is `httpsd.csr`.
- The password of the private key is `password`.
- The name of the country is `US`.
- The name of the state is `Washington`.
- The name of the municipality is `Seattle`.
- The name of the company is `example`.
- The name of the department is `WebSite`.
- The host name of the node is `www.example.com`.

```
$ sudo certctl --create-cert --dest-key httpsdkey.pem --dest-csr
httpsd.csr --key-passwd password --country US --state-province Washington
--locality Seattle --organization example --unit WebSite --common-name
www.example.com
```

Creating a keystore with the following conditions:

- The name of the private key file is `httpsdkey.pem`.
- The name of the public key certificate file is `httpsd.pem`.
- The name of the intermediate certificate authority certificate file is `cacert.cer`.
- The name of the keystore file is `keystore.pkcs12`.
- The password of the keystore is `password`.
- The password of the private key is `password`.

```
$ sudo certctl --create-pkcs --key httpsdkey.pem --cert httpsd.pem --
intermediate-cert cacert.cer --dest-keystore keystore.pkcs12 --passwd
password --key-passwd password
```

Setting the public key certificate to the node with the following conditions:

- The name of the private key file is `httpsdkey.pem`.
- The name of the public key certificate file is `httpsd.pem`.
- The name of the intermediate certificate authority certificate file is `cacert.cer`.
- The name of the keystore file is `keystore`.
- The password of the private key is `password`.

```
$ sudo certctl --set-cert --key httpsdkey.pem --cert httpsd.pem --
intermediate-cert cacert.cer --keystore keystore --key-passwd password
```

cifsbackup (Back up CIFS share information)

Synopsis

```
cifsbackup file-system-name information-definition-file-name
cifsbackup -h
```

Description

Backs up information about the CIFS shares for the specified file system.

The backed-up information about the CIFS shares can be restored by using the `cifsrestore` command. If multiple CIFS shares are created for the same shared directory when a backup is performed, the backup cannot be restored in an HDI system earlier than system version 3.2.1-03.

The resource group to which the specified file system belongs must be properly running on the node for which the command is executed. CIFS share information can be backed up even if the resource group is in the failover status. However, the information definition file will be created on the failover-destination node, where the command is executed.

Options and arguments

file-system-name

Specify the name of the file system whose CIFS share information you want to back up.

information-definition-file-name

Specify the name of the information definition file to which the CIFS share information is backed up.

Specify the name of the information definition file using no more than 255 characters. You can use alphanumeric characters, hyphens (-), and underscores (_). Note that hyphens cannot be used as the first character of the file name. You can also use periods (.), except at the beginning or end of the character string.

The information definition file will be output immediately under the SSH account home directory (/home/nasroot). The file cannot have the same name as an existing file in the /home/nasroot directory.

Notes:

- Do not edit the contents of the information definition file. If the information definition file is edited, restoration of the backup information about the CIFS shares might not be possible.

- You can use the scp command or some other secure transfer tools to send and save the information definition file onto a remote host.

Return values

Table 2-97 Return values of the cifsbackup command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 66#, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66#	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

Example

To back up information about CIFS shares according to the following conditions:

- ○ The name of the file system is FS1.
- ○ The name of the information definition file is FS1_cifsshares.xml.

```
$ sudo cifsbackup FS1 FS1_cifsshares.xml
```

cifscreate (Create a CIFS share)

Synopsis

Advanced ACL type
```
cifscreate -x share-name -d shared-directory [-a use]
   [-s {make_public|do_not_make_public|allow|deny}
   :hostname[,hostname...]]
   [-c comment] [-b {permit|do_not_permit}] [-p {ro|rw}]
   [-g {allow|disallow|default}]
   {[-f {ro|rw|none},{ro|rw|none},{ro|rw|none}]
    [-F {ro|rw|none},{ro|rw|none},{ro|rw|none}]|
    [--owner-only]}
   [-S {write_and_close|close|none|default}]
   [-C {use|do_not_use|default}]
   [-D add:user[,user...]] [-A add:user[,user...]]
   [-o extended-options] [-q]
```

extended-options:
```
   homedir={use|do_not_use}
   acsucc={log-event[,log-event...]|none|default}
   acfail={log-event[,log-event...]|none|default}
   acpol={parallel|serial|default}
   vss={default|do_not_use}
   vssmc={use|do_not_use|default}
   roc={use|do_not_use|default}
   abe={use|do_not_use|default}
   ola={use|do_not_use}
   enc={auto|mandatory|disable|default}
   rfmhdr={use|do_not_use}
```

Classic ACL type
```
cifscreate -x share-name -d shared-directory [-a {use|not_use}]
   [-s {make_public|do_not_make_public|allow|deny}
   :hostname[,hostname...]]
   [-c comment] [-b {permit|do_not_permit}] [-p {ro|rw}]
   [-f {ro|rw|none},{ro|rw|none},{ro|rw|none}]
   [-F {ro|rw|none},{ro|rw|none},{ro|rw|none}]
   [-g {allow|disallow|default}]
   [-S {write_and_close|close|none|default}]
   [-C {use|do_not_use|default}]
   [-t {write_permitted_users|owner_only|default}]
   [-D add:user[,user...]] [-A add:user[,user...]]
   [-o extended-options] [-q]
```

extended-options:
```
homedir={use|do_not_use}
acsucc={log-event[,log-event...]|none|default}
acfail={log-event[,log-event...]|none|default}
acpol={parallel|serial|default}
vss={default|do_not_use}
vssmc={use|do_not_use|default}
roc={use|do_not_use|default}
abe={use|do_not_use|default}
ola={use|do_not_use}
enc={auto|mandatory|disable|default}
rfmhdr={use|do_not_use}
```

To reference the command syntax
```
cifscreate -h
```

Description

Creates a CIFS share using the specified attributes.

Multiple CIFS share names can be assigned to the same share directory by creating multiple CIFS shares for the same share directory. Note the following in regards to share operations:

- We recommend using commands to create and edit CIFS shares.
- In the GUI, information about only the first CIFS share created for each share directory is displayed.

Note:

For a file system linked to the HCP system at the share level, a CIFS share cannot be created at the mount point.

Options and arguments

-a {use|not_use}

Specify whether to allow CIFS clients to view or set ACLs. If you omit this option, it defaults to use.

use

Specify this option to allow CIFS clients to view or set ACLs.

Once you have created a CIFS share, you cannot change this option to not_use, which does not allow CIFS clients to view or set ACLs.

not_use

Specify this option to prohibit CIFS clients from viewing or setting ACLs.

You can specify not instead of not_use.

-A add: *user* [, *user* ...]

Use this option to specify the names of users or groups who are allowed to write to the CIFS share. To specify a group, prefix the name with an at mark (@). When specifying multiple user names or group names, use a

comma (,) to separate them. Note that, you cannot specify both users that have a name starting with an at mark (@), and users who belong to a domain that has a name starting with an at mark (@). You cannot specify a Windows domain built-in user or group.

If the file system is mounted as read-only, the user and group settings specified in this option will be invalid. Also, if the same user or group is specified in the -A option and the -D option, the content specified for the -A option will take effect.

-b {permit|do_not_permit}

In the CIFS client environment, specify whether to display a CIFS share name in the CIFS share name list. If you omit this option, it defaults to permit.

permit

Specify this if you want to display a share name in the CIFS share name list.

do_not_permit

Specify this if you do not want to display a share name in the CIFS share name list. You can specify not instead of do_not_permit.

-c comment

Specify a comment no longer than 256 characters for the CIFS share. If you omit this option, no comment is specified.

You can use alphanumeric characters, exclamation marks (!), hash marks (#), dollar signs ($), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), asterisks (*), plus signs (+), commas (,), hyphens (-), periods (.), forward slashes (/), colons (:), left angle brackets (<), right angle brackets (>), question marks (?), at marks (@), left square brackets ([), back slashes (\), right square brackets (]), carets (^), underscores (_), grave accent marks (`), left curly brackets ({), vertical bars (|), right curly brackets (}), and tildes (~). You cannot specify a space at the beginning or the end of a character string. You cannot specify a backslash (\) at the end of a character string. You can also specify multibyte characters.

-C {use|do_not_use|default}

Specify whether the updated data in the CIFS share file is to be cached on the client. If you omit this option, it defaults to default.

Specify do_not_use for read-write-content-sharing file systems. If the updated data in the file of the CIFS share is cached on the client, the update date might not be reflected properly on other sites.

Note that, if you enable SMB encryption for a CIFS share, the updated data will not be cached, irrespective of the specification of this option.

use

Specify this if the updated data in the CIFS share file is to be cached on the client. If the -C option is specified as use, performance enhances when the updated data in the CIFS share file is cached on

Hitachi Data Ingestor CLI Administrator's Guide

the client. However, data reliability might deteriorate when an error occurs in the network or the CIFS client.

`do_not_use`

Specify this if the updated data in the CIFS share file is not to be cached on the client. You can specify `not` instead of `do_not_use`.

`default`

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box.

`-d` *shared-directory*

Specify the absolute path of the directory where you want to create a CIFS share, using 6 to 256 characters beginning with `/mnt/`.

For a home-directory-roaming file system and read-write-content-sharing file system, you must specify the mount point as a shared directory.

You can use alphanumeric characters, exclamation marks (`!`), hash marks (`#`), dollar signs (`$`), percent signs (`%`), ampersands (`&`), single quotation marks (`'`), left parentheses (`(`), right parentheses (`)`), plus signs (`+`), commas (`,`), hyphens (`-`), periods (`.`), forward slashes (`/`), semicolons (`;`), equal signs (`=`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), carets (`^`), underscores (`_`), grave accent marks (`` ` ``), left curly brackets (`{`), right curly brackets (`}`), tildes (`~`), and spaces. You can also specify multibyte characters. However, you cannot specify a path that includes a symbolic link. Note
that `.conflict`, `.conflict_longpath`, `.snaps`, `.history`, and `.lost +found` cannot be specified for a directory name.
Also, `.arc`, `.system_gi`, `.system_reorganize`, or `lost+found` cannot be specified for the name of a directory immediately under the file system. Forward slashes and spaces specified at the end are deleted.

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:

`%D, %G, %H, %I, %L, %M, %N, %P, %R, %S, %T, %U, %V, %a, %d, %g, %h, %i, %m, %p, %u, %v, %w, %$`

`-D add:` *user* `[,` *user* `...]`

Use this option to specify the names of users or groups who are not allowed to write to the CIFS share. Specify the names of the users or groups not permitted to write to the CIFS share. To specify a group, prefix the name with an at mark (`@`). When specifying multiple user names or group names, use a comma (`,`) to separate them. Note that, you cannot specify both users that have a name starting with an at mark (`@`), and users who belong to a domain that has a name starting with an at mark (`@`). You cannot specify a Windows domain built-in user or group.

Also, if the same user or group is specified in the `-A` option and the `-D` option, the content specified for the `-A` option will take effect.

`-f {ro|rw|none},{ro|rw|none},{ro|rw|none}`

Specify access permissions for files to be created in the writable CIFS share, in the following order: the owner, the owner group, and others (for Advanced-ACL-type file systems, this means all users and groups).

You cannot specify this option when the `--owner-only` option is specified.

You can specify the following values:

`ro`

    Specify this to grant read-only permission to the files. The permissions `r--` are set.

`rw`

    Specify this to grant both read and write permissions to the files. The permissions `rw-` are set.

`none`

    Specify this to grant neither read nor write permission to the files. The permissions `---` are set.

If this option is omitted, the access permissions are set as follows according to the ACL type of the file system to which the CIFS share belongs:

- Advanced ACL type

    If both the `-F` option and this option are omitted, full permissions are set only for the owner, the same as when the `--owner-only` option is specified. In this case, the permissions `rwx------` are set.

    If the `-F` option is specified and this option is omitted, `rw,ro,ro` is set. In this case, the permissions `rw-r--r--` are set.

- Classic ACL type

    If this option is omitted, the `rw,ro,ro` is set. In this case, the permissions `rw-r--r--` are set.

Notes:

- If `ro` or `none` is specified for the owner, none of users, including the owner, can write to new files.

- In an Advanced-ACL-type file system, the following access permissions must be specified for all users and groups depending on the owner group specification:

    - If you specify `ro` for the owner group, specify `ro` or `none` for all users and groups. If you specify `rw`, users belonging to the owner group (including the owner) will no longer be able to write to new files.

    - If you specify `none` for the owner group, specify `none` for all users and groups. If you specify `rw`, users belonging to the owner group (including the owner) will no longer be able to read or write to new files, and if you specify `ro`, they will no longer be able to read new files.

`-F {ro|rw|none},{ro|rw|none},{ro|rw|none}`

Specify access permissions for directories to be created in the writable CIFS share, in the following order: the owner, the owner group, and then the others (for Advanced-ACL-type file systems, this means all users and groups).

You cannot specify this option when the `--owner-only` option is specified.

You can specify the following values:

`ro`

> Specify this to grant read-only permission to directories. The permissions `r-x` are set.

`rw`

> Specify this to grant both read and write permissions to directories. The permissions `rwx` are set.

`none`

> Specify this to grant neither read nor write permission to directories. The permissions `--x` are set.

If this option is omitted, the access permissions are set as follows according to the ACL type of the file system to which the CIFS share belongs:

- Advanced ACL type

  If both the `-f` option and this option are omitted, full permissions are set only for the owner, the same as when the `--owner-only` option is specified. In this case, the permissions `rwx------` are set.

  If the `-f` option is specified and this option is omitted, `rw,ro,ro` is set. In this case, the permissions `rwxr-xr-x` are set.

- Classic ACL type

  If this option is omitted, the `rw,ro,ro` is set. In this case, the permissions `rwxr-xr-x` are set.

Notes:

- If `ro` or `none` is specified for the owner, no users, including the owner, can write to new directories.

- In an Advanced-ACL-type file system, the following access permissions must be specified for all users and groups depending on the owner group specification:

  - If you specify `ro` for the owner group, specify `ro` or `none` for all users and groups. If you specify `rw`, users belonging to the owner group (including the owner) will no longer be able to write to new directories.

  - If you specify `none` for the owner group, specify `none` for all users and groups. If you specify `rw`, users belonging to the owner group (including the owner) will no longer be able to read or write to new directories, and if you specify `ro`, they will no longer be able to read new directories.

`-g {allow|disallow|default}`

Specify access permissions for a guest account. The guest account is regarded as `nobody` (user ID: `65534`) regardless of the CIFS service authentication mode. Therefore, allow access permissions in the CIFS share that guest account users can access as `nobody`. An ACL cannot be set for the guest account (`nobody`).

The value set when this option is omitted depends on whether the file system supports the home-directory-roaming functionality.

- For file systems that support home-directory-roaming: `disallow`

- For file systems that do not support home-directory-roaming: `default`

Specify `disallow` for file systems that support home-directory-roaming.

`allow`

Specify this to allow guest account users access to CIFS share.

`disallow`

Specify this to disallow guest account users access to CIFS share.

`default`

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

`-o` *extended-options*

Specify extended options for the CIFS share, in the following format:
option-ID=value ...

Each unit of *option-ID=value* represents an extended option. You can specify more than one extended option. When specifying multiple extended options, use a space to separate them.

You can specify the following extended options:

`homedir={use|do_not_use}`

Specify whether to use the automatic home directory creation function in the CIFS share.

The value set when this option is omitted depends on whether the file system supports the home-directory-roaming functionality.

- For file systems that support home-directory-roaming: `use`

- For file systems that do not support home-directory-roaming: `do_not_use`

`use`

Specify this if you want to use the automatic home directory creation function. If you specify `use`, when a user accesses the CIFS share through a CIFS client, a directory to serve as the user's home directory is created under the shared directory specified by the `-d` option. This directory has the same name (but all lower case) as the user who created it.

`do_not_use`

Specify this to disable the automatic home directory creation function. You can specify `not` instead of `do_not_use`.

`acsucc={ log-event [, log-event ...]|none|default}`

Specify whether to log successful access to the CIFS share by CIFS clients. If you omit this extended option, it defaults to `default`.

These settings take effect when the CIFS access log functionality is enabled in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

log-event

The following table describes the values you can specify as events for logging successful access to the CIFS share. When specifying multiple events, use a comma (`,`) to separate them.

Value	Description
lfld	Records a log entry when the client successfully displays a folder list.
rdat	Records a log entry when the client successfully reads data.
wdat	Records a log entry when the client successfully creates a file or writes data.
cfld	Records a log entry when the client successfully creates a folder.
del	Records a log entry when the client successfully deletes a file or folder.
rper	Records a log entry when the client successfully reads the access permissions for a file or folder.
cper	Records a log entry when the client successfully changes the access permissions for a file or folder.
cown	Records a log entry when the client successfully changes the owner of a file or folder.
rename	Records a log entry when the client successfully renames a file or folder.
con	Records a log entry when the client successfully establishes or terminates a connection to the CIFS share.

`none`

Specify this if you do not want to log successful access.

`default`

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

`acfail={ log-event [, log-event ...]|none|default}`

Specify whether to log failed access attempts to the CIFS share by CIFS clients. If you omit this extended option, it defaults to `default`.

These settings take effect when the CIFS access log functionality is enabled in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

log-event

The following table describes the values you can specify as events for logging failed access attempts. When specifying multiple events, use a comma (`,`) to separate them.

Value	Description
`lfld`	Records a log entry when a client fails to display a folder list.
`rdat`	Records a log entry when a client fails to read data.
`wdat`	Records a log entry when a client fails to create a file or write data.
`cfld`	Records a log entry when a client fails to create a folder.
`del`	Records a log entry when a client fails to delete a file or folder.
`rper`	Records a log entry when a client fails to read the access permissions for a file or folder.
`cper`	Records a log entry when a client fails to change the access permissions for a file or folder.
`cown`	Records a log entry when a client fails to change the owner of a file or folder.
`rename`	Records a log entry when a client fails to rename a file or folder.
`con`	Records a log entry when a client fails to establish or terminate a connection to the CIFS share.

`none`

Specify this if you do not want to log failed access attempts.

`default`

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

`acpol={parallel|serial|default}`

Specify how to handle access from CIFS clients. If you omit this option, it defaults to `default`.

`parallel`

Specify this to handle access in parallel.

`serial`

Specify this to handle access serially.

`default`

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box.

Hitachi Data Ingestor CLI Administrator's Guide

```
vss={default|do_not_use}
```
This item is not supported.

```
vssmc={use|do_not_use|default}
```
This item is not supported.

```
roc={use|do_not_use|default}
```
Specify whether to use a read-only client cache when multiple CIFS clients simultaneously attempt to access a file. If you omit this option, it defaults to `default`. Note that we recommend that you do not use this if you also want to use the NFS protocol to access the file shares because changes might not be applied.

`use`

Specify this if you want to use a read-only client cache. You can specify `use` when specifying any argument other than `do_not_use` for the `-C` option.

`do_not_use`

Specify this if you do not want to use a read-only client cache. Instead of specifying `do_not_use`, you can also specify `not`.

`default`

Specify this to use the default settings of the CIFS service configuration definitions set from the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box.

```
abe={use|do_not_use|default}
```
Specify whether to use access-based enumeration.

The value set when this option is omitted depends on whether the file system supports the home-directory-roaming functionality.

- For file systems that support home-directory-roaming: `use`

- For file systems that do not support home-directory-roaming: `default`

`use`

Specify this if you want to use access-based enumeration.

`do_not_use`

Specify this if you do not want to use access-based enumeration. Instead of specifying `do_not_use`, you can also specify `not`.

`default`

Specify this to use the default settings of the CIFS service configuration definitions set from the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

```
ola={use|do_not_use}
```
Specify whether to use the offline attribute. If you omit this option, it defaults to `use`.

`use`

Specify this if you want to use the offline attribute.

`do_not_use`

Specify this if you do not want to use the offline attribute. Instead of specifying `do_not_use`, you can also specify `not`. Specify `do_not_use` only if you are using an application does not run normally when using the offline attribute.

`enc={auto|mandatory|disable|default}`

Specify whether to encrypt communication with a CIFS client when using SMB 3.0. If you omit this option, it defaults to `default`.

This option is valid only when **SMB 3.0** is selected as **SMB protocol** on the **CIFS Service Management** page (**Setting Type**: `Basic`) of the Access Protocol Configuration dialog box. If a value other than **SMB 3.0** is selected as the **SMB protocol**, specify `disable`, or disable encryption in the CIFS service configuration definitions and specify `default`.

`auto`

Specify this only if the client supports encryption.

`mandatory`

Specify this if encryption is mandatory.

A client that does not support SMB 3.0 cannot access CIFS sharing.

`disable`

Specify this if you do not want encryption.

`default`

Specify this to use the default settings of the CIFS service configuration definitions set from the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

`rfmhdr={use|do_not_use}`

Specifies whether to use the retry function to improve the status of a client that failed to create or update a file due to the temporary problem of the home directory being read-only. This option is valid for CIFS shares in a home-directory-roaming file system. If you omit this option, it defaults to `do_not_use`.

`use`

Specify this to use the retry function. If this argument is specified, a response indicating the result of file operation will not be sent to the client until the retry is complete (maximum of 15 seconds).

`do_not_use`

Specify this to not perform a retry if an attempt to create or update a file fails.

`--owner-only`

Sets full permissions only for the owner to access files or directories created in the writable CIFS share. The permissions `rwx------` are set. This option can be specified when a file system that belongs to the CIFS

share is of the Advanced ACL type. This option cannot be specified when the `-f` option or `-F` option is specified.

`-p {ro|rw}`

Specify access permissions for the CIFS share. If you omit this option, it defaults to `rw`. If you specify access permissions for users or groups by using the `-A` option or the `-D` option, then those permissions will take priority over permissions set with this option. If the file system is mounted as read-only, specify `ro`. In this case, even if you specify `rw`, `ro` will be set.

`ro`

Specify this to grant read permission only to the CIFS share.

`rw`

Specify this to grant both read and write permissions to the CIFS share.

Specify `rw` for home-directory-roaming file systems.

`-q`

Specify this to suppress the output of messages to the standard output and standard error output.

`-s {make_public|do_not_make_public|allow|deny}`: *hostname* [, *hostname* ...]

Specify the hosts or networks allowed to access the CIFS share. When you specify a network address, use a netmask for IPv4 or a prefix length for IPv6.

If you specify multiple host names or network addresses, use a comma (`,`) to separate them. Specify the host names and network names so that the total number of characters does not exceed 5,631.

You cannot specify the following names as the host name:

o   `ALL`

o   `FAIL`

o   `EXCEPT`

If you omit this option, permission to access the CIFS share is granted to all hosts and network addresses.

`make_public` or `allow`

Specify this to allow the specified hosts or network addresses to access the CIFS share.

`do_not_make_public` or `deny`

Specify this to prohibit the specified hosts or network addresses from accessing the CIFS share. You can specify `not` instead of `do_not_make_public` or `deny`.

Notes:

- If **Host access restrictions** is specified in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

Configuration dialog box, the `-s` option is ignored and the CIFS service configuration definitions set in this page apply to all CIFS shares. When you want to set **Host access restrictions** for each CIFS share separately, use the `-s` option for the `cifscreate` command or the `cifsedit` command rather than specifying **Host access restrictions** in the **CIFS Service Management** page (**Setting Type**: `Security`).

- Even if you specify the `-s` option to permit access to a CIFS share, user authentication for CIFS clients is performed.

- When you specify the host name, edit the `/etc/hosts` file in the **Edit System File** page of the Network & System Configuration dialog box to add the names and IP addresses of all the specified hosts. If the host names are not added to the `/etc/hosts` file, the specified information might be invalid when access to the CIFS share is permitted or denied by using the `-s` option.

`-S {write_and_close|close|none|default}`

Specify the operation to be performed in response to a write request issued from a CIFS client to a CIFS share. If you omit this option, it defaults to `default`. Regardless of the setting for this option, data is written to the disk drive whenever files to be updated are flushed.

`write_and_close`

Specify this to perform writing synchronously with a write request or a close request issued from a client to a CIFS share. If `write_and_close` is specified, data is written to the disk drive when a CIFS client issues a write request or a close request, and then the result is returned to the requestor. This method might cause performance to deteriorate more so than with other methods. However, specifying this option ensures that the returned data has been written to the disk drive even if an error occurs on the CIFS client or network.

`close`

Specify this to perform writing synchronously with a close request issued from a client to a CIFS share. If `close` is specified, the result will be returned to the requestor when the HDI system receives a write request from a CIFS client. Writing to the disk drive is not synchronized with each write request. Instead, writing is processed together with a close request when a close request is issued. By using this method, performance is sometimes better than when data is written synchronously with a write request or a close request. However, specifying this option does not ensure that the returned data has been written to the disk drive if an error occurs.

`none`

Specify this to perform writing at regular intervals. If `none` is specified, data is written to the disk drive at regular intervals, irrespective of the timing at which a client issues a write request or a close request to a CIFS share. This might make it possible to improve

performance over other methods. However, specifying this option does not ensure that the returned data has been written to the disk drive if an error occurs.

default

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box.

-t {write_permitted_users|owner_only|default}

Specify the users for which you want to permit time-stamp updating for files in the CIFS share. If you omit this option, it defaults to `default`. Specify `write_permitted_users` if the file is shared by the CIFS service only.

write_permitted_users

Specify this if you want to permit time-stamp updating for all users who are permitted to write to the file. You can specify `write` instead of `write_permitted_users`.

owner_only

Specify this if you want to limit time-stamp updating to the file owner only. You can specify `owner` instead of `owner_only`.

default

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

-x *share-name*

Specify a name of the CIFS share that can be referred to by the users. A CIFS share name must be a string no longer than 80 characters, and must be unique within the node.

You can use alphanumeric characters, exclamation marks (`!`), hash marks (`#`), dollar signs (`$`), percent signs (`%`), ampersands (`&`), single quotation marks (`'`), left parentheses (`(`), right parentheses (`)`), plus signs (`+`), commas (`,`), hyphens (`-`), periods (`.`), semicolons (`;`), equal signs (`=`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), carets (`^`), underscores (`_`), grave accent marks (`` ` ``), left curly brackets (`{`), right curly brackets (`}`), tildes (`~`), and spaces. You can also specify multibyte characters. However, you cannot specify only a dollar sign or periods (e.g., `$`, `.`, or `..`) in the string, and you cannot specify a period at the end (e.g., `Abc.`). If the string ends with a dollar sign, you cannot specify a period just before the dollar sign (e.g., `Abc.$`). Spaces specified at the end are deleted.

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:

`%D, %G, %H, %I, %L, %M, %N, %P, %R, %S, %T, %U, %V, %a, %d, %g, %h, %i, %m, %p, %u, %v, %w, %$`

In addition, the CIFS share name cannot be `global`, `homes`, `printers`, `admin$`, `c$`, `global$`, `homes$`, `ipc$`, or `printers$`.

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.

Return values

Table 2-98 Return values of the cifscreate command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 66[#], 70, 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 98, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.
99[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Examples

To create a CIFS share according to the following conditions:

o   The name of the CIFS share is `cifs1`.

o   The directory `/mnt/FS1/dir_case1` is made public as a shared directory.

o   Write operations to the CIFS share are not permitted.

```
$ sudo cifscreate -x cifs1 -d /mnt/FS1/dir_case1 -p ro
```

To create a CIFS share according to the following conditions:

- The name of the CIFS share is `cifs2`.
- The directory `/mnt/FS1/dir_case2` is a shared directory.
- The automatic home directory creation function is used.
- Do not display the CIFS share in the share name list.

```
$ sudo cifscreate -x cifs2 -d /mnt/FS1/dir_case2 -b do_not_permit -o
homedir=use
```

To create a CIFS share according to the following conditions:

- Enable the CIFS access log functionality in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.
- The name of the CIFS share is `cifs3`.
- The directory `/mnt/FS1/dir_case3` is made public as a shared directory.
- Record a successful access log entry when a CIFS client successfully creates a file or writes data (`wdat`), or successfully deletes a file or folder (`del`).
- Do not log failed access attempts by CIFS clients (set the event to `none`).
- A read-only client cache is used when multiple CIFS clients simultaneously attempt to access a file.
- Access-based enumeration is used.

```
$ sudo cifscreate -x cifs3 -d /mnt/FS1/dir_case3 -C use -o
"acsucc=wdat,del acfail=none roc=use abe=use"
```

cifsdelete (Delete a CIFS share)

Synopsis (for cluster configurations)
```
cifsdelete -x share-name [-r resource-group-name]
```

Synopsis (for single node configurations)
```
cifsdelete -x share-name
```

Synopsis (to reference the command syntax)
```
cifsdelete -h
```

Description

Deletes a CIFS share.

Options and arguments

-r *resource-group-name*

    Specify the name of the resource group to which the CIFS share belongs.

    If the system is running in a degenerated state after a failover, two CIFS shares with the same name may coexist on the node. For this reason, to delete a CIFS share while the system is running in a degenerated state, you should specify the name of the resource group to which the target CIFS share belongs.

    If you omit this option, the command searches for the CIFS share in the following resource group order, and attempts to delete the share:

    1. The resource group belonging to the node where the command was executed

    2. The resource group belonging to the failover-source node

-x *share-name*

    Specify the name of the CIFS share to be deleted.

Return values

Table 2-99 Return values of the cifsdelete command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 66#, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66#	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

cifsinfogetctl (Specify settings for collecting the CIFS-service performance analysis log)

Synopsis

```
cifsinfogetctl [--dir directory-name] [--count log-collection-count]
    [--interval log-collection-interval] --set log-collection-time
cifsinfogetctl --delete {log-collection-time|--all}
cifsinfogetctl --list
cifsinfogetctl -h
```

Description

Sets or cancels the time to collect log data for analysing performance of the CIFS service. You can also use this command to view the current setting.

The command starts collecting log data at the specified time everyday, and collects log data at the specified intervals for the specified number of times. Log data can be collected a maximum of 72 times per day for a node . You can specify a directory in the file system to receive the log data. If you do not specify a directory, the log data is output to an OS disk. In the Check for Errors dialog box, you can collect this output log data by downloading all the log data from the **List of RAS Information** page. When the capacity of the log output directory is short, the OS may become unstable. If you need to collect log data more than three times, we recommend that the log data be output to a directory. The output directory requires the following amount of free space:

```
Required free space = Log collection count x 100 MB
```

If the directory does not have enough free space, the KAQG52026-W message appears and log data collection stops. Delete old log data from the directory on a regular basis.

Options and arguments

--count *log-collection-count*

Specify the number of times log data is collected, using a value in the range from 1 to 72. This option must be specified with the --set option. If you omit this option, 1 is set.

--delete *log-collection-time*|--all

Specify this option to cancel the setting of the log collection time.

log-collection-time

Specify this to cancel the setting of the specified time. Specify the time in *hhmm* format.

--all

Specify this option to cancel all the settings.

--dir *directory-name*

To output log data to a directory in the file system, specify the absolute path of the directory, using no more than 255 characters beginning with `/mnt/`. Specify this option with the `--set` option. Note that `.conflict`, `.conflict_longpath`, `.snaps`, `.history`, `.arc`, `.system_gi`, `.system_reorganize`, `lost+found`, or `.lost+found` cannot be specified for a directory name. Directories in a home-directory-roaming file system and read-write-content-sharing file system cannot be specified as the log output destination.

`--interval` *log-collection-interval*

Specify the log collection interval (in minutes) in the range from 1 to 60 if the log collection count is specified for the `--count` option. Specify this option with the `--set` option. If you omit this option, `5` is set.

`--list`

Specify this option to display the log collection times.

A log collection time is displayed in the following format:

log-collection-time,*directory-path*#

#

If a directory in the file system is not specified as the log output destination, `default` is displayed.

`--set` *log-collection-time*

Specify the start time of log data collection, using *hhmm* format.

Return values

Table 2-100 Return values of the cifsinfogetctl command

Return value	Description
0	Normal termination
1, 3	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
5, 10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
60	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To specify the following information for the time to collect the CIFS-service performance analysis log:

- ○ The log data is output to `/mnt/cifsshare/log` directory.
- ○ The log data is collected 4 times.
- ○ The log data is collected at 10-minute intervals.
- ○ The first log data is collected at `9:50`.

```
$ sudo cifsinfogetctl --dir /mnt/cifsshare/log --count 4 --interval 10 --
set 0950
$ sudo cifsinfogetctl --list
time,dir,
0950,/mnt/cifsshare/log,
1000,/mnt/cifsshare/log,
1010,/mnt/cifsshare/log,
1020,/mnt/cifsshare/log,
```

To cancel the time to collect the CIFS-service performance analysis log:

```
$ sudo cifsinfogetctl --list
time,dir,
0950,/mnt/cifsshare/log,
1000,/mnt/cifsshare/log,
1010,/mnt/cifsshare/log,
1020,/mnt/cifsshare/log,
$ sudo cifsinfogetctl --delete 1000
$ sudo cifsinfogetctl --list
time,dir,
0950,/mnt/cifsshare/log,
1010,/mnt/cifsshare/log,
1020,/mnt/cifsshare/log,
```

cifsedit (Edit CIFS share information)

Synopsis (for cluster configurations)

Advanced ACL type

```
cifsedit -x share-name [-X new-share-name]
   [-r resource-group-name] [-a use]
   [-s {default|{make_public|do_not_make_public|allow|deny}
   :[{add|del}:]hostname[,hostname...]
   [:[{add|del}:]hostname[,hostname...]]}]
   [-c comment] [-b {permit|do_not_permit}] [-p {ro|rw}]
   {[-f {ro|rw|none},{ro|rw|none},{ro|rw|none}]
    [-F {ro|rw|none},{ro|rw|none},{ro|rw|none}]|
    [--owner-only]}
   [-g {allow|disallow|default}]
   [-S {write_and_close|close|none|default}]
   [-C {use|do_not_use|default}]
   [-D {add|del}:user[,user...][:{add|del}:user[,user...]]]
   [-A {add|del}:user[,user...][:{add|del}:user[,user...]]]
   [-o extended-options] [-q]
```

extended-options:

```
homedir={use|do_not_use}
acsucc={log-event[,log-event...]|none|default}
acfail={log-event[,log-event...]|none|default}
acpol={parallel|serial|default}
vss={default|do_not_use}
vssmc={use|do_not_use|default}
roc={use|do_not_use|default}
abe={use|do_not_use|default}
ola={use|do_not_use}
enc={auto|mandatory|disable|default}
rfmhdr={use|do_not_use}
```

Classic ACL type

```
cifsedit -x share-name [-X new-share-name]
    [-r resource-group-name] [-a use]
    [-s {default|{make_public|do_not_make_public|allow|deny}
    :[{add|del}:]hostname[,hostname...]
    [:[{add|del}:]hostname[,hostname...]]}]
    [-c comment] [-b {permit|do_not_permit}] [-p {ro|rw}]
    [-f {ro|rw|none},{ro|rw|none},{ro|rw|none}]
    [-F {ro|rw|none},{ro|rw|none},{ro|rw|none}]
    [-g {allow|disallow|default}]
    [-S {write_and_close|close|none|default}]
    [-C {use|do_not_use|default}]
    [-t {write_permitted_users|owner_only|default}]
    [-D {add|del}:user[,user...][:{add|del}:user[,user...]]]
    [-A {add|del}:user[,user...][:{add|del}:user[,user...]]]
    [-o extended-options] [-q]
```

extended-options:

```
homedir={use|do_not_use}
acsucc={log-event[,log-event...]|none|default}
acfail={log-event[,log-event...]|none|default}
acpol={parallel|serial|default}
vss={default|do_not_use}
vssmc={use|do_not_use|default}
roc={use|do_not_use|default}
abe={use|do_not_use|default}
ola={use|do_not_use}
enc={auto|mandatory|disable|default}
rfmhdr={use|do_not_use}
```

Synopsis (for single node configurations)

Advanced ACL type

```
cifsedit -x share-name [-X new-share-name] [-a use]
    [-s {default|{make_public|do_not_make_public|allow|deny}
    :[{add|del}:]hostname[,hostname...]
    [:[{add|del}:]hostname[,hostname...]]}]
    [-c comment] [-b {permit|do_not_permit}] [-p {ro|rw}]
    {[-f {ro|rw|none},{ro|rw|none},{ro|rw|none}]
     [-F {ro|rw|none},{ro|rw|none},{ro|rw|none}]|
     [--owner-only]}
    [-g {allow|disallow|default}]
    [-S {write_and_close|close|none|default}]
    [-C {use|do_not_use|default}]
    [-D {add|del}:user[,user...][:{add|del}:user[,user...]]]
```

```
          [-A {add|del}:user[,user...][:{add|del}:user[,user...]]]
          [-o extended-options] [-q]
```

extended-options:

```
    homedir={use|do_not_use}
    acsucc={log-event[,log-event...]|none|default}
    acfail={log-event[,log-event...]|none|default}
    acpol={parallel|serial|default}
    vss={default|do_not_use}
    vssmc={use|do_not_use|default}
    roc={use|do_not_use|default}
    abe={use|do_not_use|default}
    ola={use|do_not_use}
    enc={auto|mandatory|disable|default}
    rfmhdr={use|do_not_use}
```

Classic ACL type

```
cifsedit -x share-name [-X new-share-name] [-a use]
    [-s {default|{make_public|do_not_make_public|allow|deny}
    :[{add|del}:]hostname[,hostname...]
    [:[{add|del}:]hostname[,hostname...]]}]
    [-c comment] [-b {permit|do_not_permit}] [-p {ro|rw}]
    [-f {ro|rw|none},{ro|rw|none},{ro|rw|none}]
    [-F {ro|rw|none},{ro|rw|none},{ro|rw|none}]
    [-g {allow|disallow|default}] [-S {write_and_close|close|none|
default}]
    [-C {use|do_not_use|default}]
    [-t {write_permitted_users|owner_only|default}]
    [-D {add|del}:user[,user...][:{add|del}:user[,user...]]]
    [-A {add|del}:user[,user...][:{add|del}:user[,user...]]]
    [-o extended-options] [-q]
```

extended-options:

```
    homedir={use|do_not_use}
    acsucc={log-event[,log-event...]|none|default}
    acfail={log-event[,log-event...]|none|default}
    acpol={parallel|serial|default}
    vss={default|do_not_use}
    vssmc={use|do_not_use|default}
    roc={use|do_not_use|default}
    abe={use|do_not_use|default}
    ola={use|do_not_use}
    enc={auto|mandatory|disable|default}
    rfmhdr={use|do_not_use}
```

Synopsis (to reference the command syntax)

```
cifsedit -h
```

Description

Updates CIFS share information using the specified attributes.

If you omit any of the following options, the current setting information applies.

Options and arguments

`-a use`

    Specify `use` when viewing or setting ACLs from the CIFS client. Note that you cannot specify `not_use` (not viewing or setting ACLs from the CIFS client).

`-A {add|del}:` *user* `[,` *user* `...][:{add|del}:` *user* `[,` *user* `...]]`

    Use this option to specify the names of users or groups who are allowed to write to the CIFS share. To specify a group, prefix the name with an at mark (`@`). When specifying multiple user names or group names, use a comma (`,`) to separate them. Note that, you cannot specify both users that have a name starting with an at mark (`@`), and users who belong to a domain that has a name starting with an at mark (`@`). You cannot specify a Windows domain built-in user or group.

    To add users or groups to those with write permission, specify `add:` followed by the user or group names. To delete users or groups from those with write permission, specify `del:` followed by the user or group names.

    If the file system is mounted as read-only, the user and group settings specified in this option will be invalid. Also, if the same user or group is specified in the `-A` option and the `-D` option, the content specified for the `-A` option will take effect.

`-b {permit|do_not_permit}`

    In the CIFS client environment, specify whether to display a CIFS share name in the CIFS share name list.

    `permit`

        Specify this if you want to display a share name in the CIFS share name list.

    `do_not_permit`

        Specify this if you do not want to display a share name in the CIFS share name list. You can specify `not` instead of `do_not_permit`.

`-c` *comment*

    Specify a comment no longer than 256 characters for the CIFS share that can be referred to by the users.

    You can use alphanumeric characters, exclamation marks (`!`), hash marks (`#`), dollar signs (`$`), ampersands (`&`), single quotation marks (`'`), left parentheses (`(`), right parentheses (`)`), asterisks (`*`), plus signs (`+`), commas (`,`), hyphens (`-`), periods (`.`), forward slashes (`/`), colons (`:`), left angle brackets (`<`), right angle brackets (`>`), question marks (`?`), at marks (`@`), left square brackets (`[`), back slashes (`\`), right square brackets (`]`), carets (`^`), underscores (`_`), grave accent marks (`` ` ``), left curly brackets (`{`), vertical bars (`|`), right curly brackets (`}`), and tildes (`~`). You cannot specify a space at the beginning or the end of a character string. You cannot specify a backslash (`\`) at the end of a character string. You can also specify multibyte characters.

`-C {use|do_not_use|default}`

Specify whether the updated data in the CIFS share file is to be cached on the client.

Specify `do_not_use` for read-write-content-sharing file systems. If the updated data in the file of the CIFS share is cached on the client, the update date might not be reflected properly on other sites.

Note that, if you enable SMB encryption for a CIFS share, the updated data will not be cached, irrespective of the specification of this option.

`use`

Specify this for the updated data in the CIFS share file to be cached on the client. If the `-C` option is specified as `use`, performance enhances if the updated data in the CIFS share file is cached on the client. However, data reliability might deteriorate when an error occurs in the network or the CIFS client.

`do_not_use`

Specify this for the updated data in the CIFS share file not to be cached on the client. You can specify `not` instead of `do_not_use`.

`default`

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box.

`-D {add|del}:` *user* `[,` *user* `...][:{add|del}:` *user* `[,` *user* `...]]`

Use this option to specify the names of users or groups who are not allowed to write to the CIFS share. To specify a group, prefix the name with an at mark (@). When specifying multiple user names or group names, use a comma (,) to separate them. Note that, you cannot specify both users that have a name starting with an at mark (@), and users who belong to a domain that has a name starting with an at mark (@). You cannot specify a Windows domain built-in user or group.

To add users or groups to those not permitted to write to the CIFS share, specify `add:` followed by the user or group names. To delete users or groups from those without write permission, specify `del:` followed by the user or group names.

Also, if the same user or group is specified in the `-A` option and the `-D` option, the content specified for the `-A` option will take effect.

`-f {ro|rw|none},{ro|rw|none},{ro|rw|none}`

Specify access permissions for files to be created in the writable CIFS share, in the following order: the owner, the owner group, and others (for Advanced-ACL-type file systems, this means all users and groups).

You cannot specify this option when the `--owner-only` option is specified.

You can specify the following values:

`ro`

Specify this to grant read-only permission to the files. The permissions `r--` are set.

rw

> Specify this to grant both read and write permissions to the files. The permissions `rw-` are set.

> Specify this to grant neither read nor write permission to the files. The permissions `---` are set.

When all the conditions below are met, `rw,ro,ro` is set. In this case, the permissions `rw-r--r--` are set.

- ○ The file system to which the CIFS share belongs is the Advanced ACL type.
- ○ Full permissions are set only for the owner (`rwx------`)
- ○ The `-F` option is specified and this option is omitted.

Notes:

- ○ If `ro` or `none` is specified for the owner, none of users, including the owner, can write to new files.
- ○ In an Advanced-ACL-type file system, the following access permissions must be specified for all users and groups depending on the owner group specification:

  - If you specify `ro` for the owner group, specify `ro` or `none` for all users and groups. If you specify `rw`, users belonging to the owner group (including the owner) will no longer be able to write to new files.

  - If you specify `none` for the owner group, specify `none` for all users and groups. If you specify `rw`, users belonging to the owner group (including the owner) will no longer be able to read or write to new files, and if you specify `ro`, they will no longer be able to read new files.

`-F {ro|rw|none},{ro|rw|none},{ro|rw|none}`

> Specify access permissions for creating a directory in the writable CIFS share, in the following order: the owner, the owner group, and then the other users.

> You cannot specify this option when the `--owner-only` option is specified.

> You can specify the following values:

ro

> Specify this to grant read-only permission to directories. The permissions `r-x` are set.

rw

> Specify this to grant both read and write permissions to directories. The permissions `rwx` are set.

> Specify this to grant neither read nor write permission to directories. The permissions `--x` are set.

Hitachi Data Ingestor CLI Administrator's Guide

When all the conditions below are met, `rw,ro,ro` is set. In this case, the permissions `rwxr-xr-x` are set.

- The file system to which the CIFS share belongs is the Advanced ACL type.
- Full permissions are set only for the owner (`rwx------`)
- The `-f` option is specified and this option is omitted.

Notes:

- If `ro` or `none` is specified for the owner, no users, including the owner, can write to new directories.
- In an Advanced-ACL-type file system, the following access permissions must be specified for all users and groups depending on the owner group specification:

    - If you specify `ro` for the owner group, specify `ro` or `none` for all users and groups. If you specify `rw`, users belonging to the owner group (including the owner) will no longer be able to write to new directories.

    - If you specify `none` for the owner group, specify `none` for all users and groups. If you specify `rw`, users belonging to the owner group (including the owner) will no longer be able to read or write to new directories, and if you specify `ro`, they will no longer be able to read new directories.

`-g {allow|disallow|default}`

Specify access permissions for guest accounts. The guest account is regarded as `nobody` (user ID: `65534`) regardless of the CIFS service authentication mode. Therefore, allow access permissions in the CIFS share that guest account users can access as `nobody`. An ACL cannot be set for the guest account (`nobody`).

allow

Specify this to allow guest account users access to CIFS share.

disallow

Specify this to disallow guest account users access to CIFS share.

default

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

You cannot specify `allow` or `default` for home-directory-roaming file systems.

`-o` *extended-options*

Specify extended options for the CIFS share, in the following format:

option-ID=value `...`

Each unit of *option-ID=value* represents an extended option. You can specify more than one extended option. If you specify multiple extended options, use a space to separate them.

You can specify the following extended options:

`homedir={use|do_not_use}`

Specify whether to use the automatic home directory creation function in the CIFS share.

`use`

Specify this if you want to use the automatic home directory creation function. If you specify `use`, when a user accesses the CIFS share through a CIFS client, a directory to serve as the user's home directory is created under the shared directory specified by the `-d` option. This directory has the same name (but all lower case) as the user who created it.

`do_not_use`

Specify this to disable the automatic home directory creation function. You can specify `not` instead of `do_not_use`.

`acsucc={` *log-event* `[,` *log-event* `...]|none|default}`

Specify whether to log successful access to the CIFS share by CIFS clients.

These settings take effect when the CIFS access log functionality is enabled in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

log-event

The following table describes the values you can specify as events for logging successful access to the CIFS share. When specifying multiple events, use a comma (`,`) to separate them

Value	Description
`lfld`	Records a log entry when the client successfully displays a folder list.
`rdat`	Records a log entry when the client successfully reads data.
`wdat`	Records a log entry when the client successfully creates a file or writes data.
`cfld`	Records a log entry when the client successfully creates a folder.
`del`	Records a log entry when the client successfully deletes a file or folder.
`rper`	Records a log entry when the client successfully reads the access permissions for a file or folder.
`cper`	Records a log entry when the client successfully changes the access permissions for a file or folder.
`cown`	Records a log entry when the client successfully changes the owner of a file or folder.
`rename`	Records a log entry when the client successfully renames a file or folder.

Value	Description
con	Records a log entry when the client successfully establishes or terminates a connection to the CIFS share.

Specify this if you do not want to log successful access.

default

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: Security) of the Access Protocol Configuration dialog box.

acfail={ *log-event* [, *log-event* ...]|none|default}

Specify whether to log failed access attempts to the CIFS share by CIFS clients.

These settings take effect when the CIFS access log functionality is enabled in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: Security) of the Access Protocol Configuration dialog box.

log-event

The following table describes the values you can specify as events for logging failed access attempts. When specifying multiple events, use a comma (,) to separate them.

Value	Description
lfld	Records a log entry when a client fails to display a folder list.
rdat	Records a log entry when a client fails to read data.
wdat	Records a log entry when a client fails to create a file or write data.
cfld	Records a log entry when a client fails to create a folder.
del	Records a log entry when a client fails to delete a file or folder.
rper	Records a log entry when a client fails to read the access permissions for a file or folder.
cper	Records a log entry when a client fails to change the access permissions for a file or folder.
cown	Records a log entry when a client fails to change the owner of a file or folder.
rename	Records a log entry when a client fails to rename a file or folder.
con	Records a log entry when a client fails to establish or terminate a connection to the CIFS share.

Specify this if you do not want to log failed access attempts.

default

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box.

`acpol={parallel|serial|default}`

Specify how to handle access from CIFS clients.

`parallel`

Specify this to handle access in parallel.

`serial`

Specify this to handle access serially.

`default`

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box.

`vss={default|do_not_use}`

This item is not supported.

`vssmc={use|do_not_use|default}`

This item is not supported.

`roc={use|do_not_use|default}`

Specify whether to use a read-only client cache when multiple CIFS clients simultaneously attempt to access a file. Note that we recommend that you do not use this if you also want to use the NFS protocol to access the file shares because changes might not be applied.

`use`

Specify this if you want to use a read-only client cache. You can specify `use` when specifying any argument other than `do_not_use` for the -C option.

`do_not_use`

Specify this if you do not want to use a read-only client cache. Instead of specifying `do_not_use`, you can also specify `not`.

`default`

Specify this to use the default settings of the CIFS service configuration definitions set in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box.

`abe={use|do_not_use|default}`

Specify whether to use access-based enumeration.

`use`

Specify this if you want to use access-based enumeration.

`do_not_use`

Specify this if you do not want to use access-based enumeration. Instead of specifying `do_not_use`, you can also specify `not`.

`default`

Hitachi Data Ingestor CLI Administrator's Guide

Specify this to use the default settings of the CIFS service configuration definitions set in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

`ola={use|do_not_use}`

Specify whether to use the offline attribute.

`use`

Specify this if you want to use the offline attribute.

`do_not_use`

Specify this if you do not want to use the offline attribute. Instead of specifying `do_not_use`, you can also specify `not`. Specify `do_not_use` only if you are using an application that does not run normally when using the offline attribute.

`enc={auto|mandatory|disable|default}`

Specify whether to encrypt communication with a CIFS client when using SMB 3.0.

This option is valid only when **SMB 3.0** is selected as **SMB protocol** on the **CIFS Service Management** page (**Setting Type**: `Basic`) of the Access Protocol Configuration dialog box. If a value other than **SMB 3.0** is selected as the **SMB protocol**, specify `disable`, or disable encryption in the CIFS service configuration definitions and specify `default`.

`auto`

Specify this only if the client supports encryption.

`mandatory`

Specify this if encryption is mandatory.

A client that does not support SMB 3.0 cannot access CIFS sharing.

`disable`

Specify this if you do not want encryption.

`default`

Specify this to use the default settings of the CIFS service configuration definitions set from the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

`rfmhdr={use|do_not_use}`

Specifies whether to use the retry function to improve the status of a client that failed to create or update a file due to the temporary problem of the home directory being read-only. This option is valid for CIFS shares in a home-directory-roaming file system.

`use`

Specify this to use the retry function. If this argument is specified, a response indicating the result of file operation will not be sent to the client until the retry is complete (maximum of 15 seconds).

`do_not_use`

Command Reference

Specify this to not perform a retry if an attempt to create or update a file fails.

`--owner-only`

Sets full permissions only for the owner to access files or directories created in the writable CIFS share. The permissions `rwx------` are set. This option can be specified when a file system that belongs to the CIFS share is of the Advanced ACL type. This option cannot be specified when the `-f` option or `-F` option is specified.

`-p {ro|rw}`

Specify access permissions for the CIFS share. If you specify access permissions for users or groups by using the `-A` option or the `-D` option, then those permissions will take priority over permissions set with this option. If the file system is mounted as read-only, specify `ro`. In this case, even if you specify `rw`, `ro` will be set.

`ro`

Specify this to grant read-only permission to the CIFS share.

`rw`

Specify this to grant both read and write permissions to the CIFS share.

Specify `rw` for home-directory-roaming file systems.

`-q`

Specify this to suppress the output of messages to the standard output and standard error output.

`-r` *resource-group-name*

Specify the name of the resource group to which the CIFS share belongs.

If the system is running in a degenerated state after a failover, two CIFS shares with the same name may coexist on the node. For this reason, to change the attributes of a CIFS share while the system is running in a degenerated state, you should specify the name of the resource group to which the target CIFS share belongs.

If you omit this option, the command searches for the CIFS share in the following resource group order, and attempts to change the attributes of the share:

1. The resource group belonging to the node where the command was executed

2. The resource group belonging to the failover-source node

`-s {default|{make_public|do_not_make_public|allow|deny}:[{add|del}:]` *hostname* `[,` *hostname* `...][:[{add|del}:]` *hostname* `[,` *hostname* `...]]}`

Specify the hosts or networks allowed to access the CIFS share. When you specify a network address, use a netmask for IPv4 or a prefix length for IPv6.

Hitachi Data Ingestor CLI Administrator's Guide

If you specify multiple host names or network addresses, use a comma (,) to separate them. Specify the host names and network names so that the total number of characters does not exceed 5,631.

default

Specify this to allow all hosts or network addresses to access the CIFS share (default setting).

make_public or allow

Specify this to allow the specified hosts or network addresses to access the CIFS share.

do_not_make_public or deny

Specify this to prohibit the specified hosts or network addresses from accessing the CIFS share. You can specify not instead of do_not_make_public or deny.

add

Specify this to add a host or network to those granted or denied permission to access the CIFS share.

del

Specify this to delete a host or network from those granted or denied permission to access the CIFS share.

Do not register duplicate host names for make_public (or allow), or do_not_make_public (or deny). The processing to be executed differs depending on the combination specified for make_public (or allow), do_not_make_public (or deny), add, and del.

For example, if host1 and host2 are allowed to access the CIFS share (-s make_public:host1,host2), you must enter the permissions as follows:

- To allow host3 and host4 to access the CIFS share:

  -s make_public:add:host3,host4

  Specifying the -s option as above, the command adds host3 and host4 to the hosts permitted to access the CIFS share.

- To replace host2 with host5 among the hosts permitted to access the CIFS share:

  -s make_public:add:host5:del:host2

  Specifying the -s option as above, host5 is allowed to access the CIFS share and host2 is prohibited from accessing the CIFS share.

- To change the settings so that only host6 is allowed to access the CIFS share:

  Specify the -s option in either of the following ways:

  - -s make_public:host6

  If you specify make_public (or allow) or do_not_make_public (or deny) and you do not specify add or del, all current information about which hosts and networks are granted or denied access to the CIFS share is deleted and the new information is set.

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

Specifying the `-s` option as above, the information about the hosts or networks permitted access (`host1` and `host2`) is deleted and only `host6` is allowed to access the CIFS share.

- `-s make_public:add:host6:del:host1,host2`

Specifying the `-s` option as above, `host6` is allowed to access the CIFS share, and `host1` and `host2` are no longer permitted access.

○ To change the settings so that only `host1` is prohibited from accessing the CIFS share:

`-s do_not_make_public:host1`

Specifying the `-s` option as above, all information about the hosts and networks granted or denied access to the CIFS share is deleted, and only `host1` is allowed to access the CIFS share.

Notes:

- If **Host access restrictions** is specified in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box, the `-s` option is ignored and the information set in this page applies to all CIFS shares. When you want to set up **Host access restrictions** for each CIFS share separately, use the `-s` option for the `cifscreate` command or the `cifsedit` command rather than specifying **Host access restrictions** in the **CIFS Service Management** page (**Setting Type**: `Security`).

- Even if you specify the `-s` option to permit access to a CIFS share, user authentication for CIFS clients is performed.

- When you specify the host name, edit the `/etc/hosts` file in the **Edit System File** page of the Network & System Configuration dialog box to add the names and IP addresses of all the specified hosts. If the host names are not added to the `/etc/hosts` file, the specified information might be invalid when access to the CIFS share is permitted or denied by using the `-s` option.

`-S {write_and_close|close|none|default}`

Specify the operation to be performed in response to a write request issued from a CIFS client to a CIFS share. Regardless of the setting for this option, data is written to the disk drive whenever files to be updated are flushed.

`write_and_close`

Specify this to perform writing synchronously with a write request or a close request issued from a client to a CIFS share. If `write_and_close` is specified, data is written to the disk drive when a CIFS client issues a write request or a close request, and then the result is returned to the requestor. This method might cause performance to deteriorate more so than with other methods. However, specifying this option ensures that the returned data has been written to the disk drive even if an error occurs on the CIFS client or network.

`close`

Specify this to perform writing synchronously with a close request issued from a client to a CIFS share. If `close` is specified, the result will be returned to the requestor when the HDI system receives a write request from a CIFS client. Writing to the disk drive is not synchronized with each write request. Instead, writing is processed together with a close request when a close request is issued. By using this method, performance is sometimes better than when data is written synchronously with a write request or a close request. However, specifying this option does not ensure that the returned data has been written to the disk drive if an error occurs.

Specify this to perform writing at regular intervals. If `none` is specified, data is written to the disk drive at regular intervals, irrespective of the timing at which a client issues a write request or a close request to a CIFS share. This might make it possible to improve performance over other methods. However, specifying this option does not ensure that the returned data has been written to the disk drive if an error occurs.

default

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box.

-t {write_permitted_users|owner_only|default}

Specify the user for whom you want to permit time-stamp updating for files in the CIFS share. Specify `write_permitted_users` if the file is shared by the CIFS service only.

write_permitted_users

Specify this if you want to permit time-stamp updating for all users who are permitted to write to the file. You can specify `write` instead of `write_permitted_users`.

owner_only

Specify this if you want to limit time-stamp file updating to the file owner only. You can specify `owner` instead of `owner_only`.

default

Specify this to use the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

-x *share-name*

Specify the name of the CIFS share whose attributes are to be changed.

-X *new-share-name*

Specify this if you want to change the name of the CIFS share. A CIFS share name must be a string no longer than 80 characters, and must be unique within the node.

You can use alphanumeric characters, exclamation marks (`!`), hash marks (`#`), dollar signs (`$`), percent signs (`%`), ampersands (`&`), single quotation marks (`'`), left parentheses (`(`), right parentheses (`)`), plus signs (`+`), commas (`,`), hyphens (`-`), periods (`.`), semicolons (`;`), equal signs (`=`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), carets (`^`), underscores (`_`), grave accent marks (`` ` ``), left curly brackets (`{`), right curly brackets (`}`), tildes (`~`), and spaces. You can also specify multibyte characters. However, you cannot specify only a dollar sign or periods (e.g., `$`, `.`, or `..`) in the string, and you cannot specify a period at the end (e.g., `Abc.`). If the string ends with a dollar sign, you cannot specify a period just before the dollar sign (e.g., `Abc.$`). Spaces specified at the end are deleted.

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:

`%D, %G, %H, %I, %L, %M, %N, %P, %R, %S, %T, %U, %V, %a, %d, %g, %h, %i, %m, %p, %u, %v, %w, %$`

In addition, the CIFS share name cannot be `global`, `homes`, `printers`, `admin$`, `c$`, `global$`, `homes$`, `ipc$`, or `printers$`.

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.

Return values

Table 2-101 Return values of the cifsedit command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70, 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 98, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.
99[#]	The system might be temporarily disabled for communication. After checking the communication status,

Return value	Description
	wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Examples

To edit the CIFS share information according to the following conditions:

- ○ The name of the CIFS share is `cifs1`.
- ○ Change the settings to allow writing to the CIFS share.
- ○ Deny write operations to the user registered in the user mapping (`DOMAIN01\user100`).

```
$ sudo cifsedit -x cifs1 -p rw -D add:"DOMAIN01\user100"
```

To edit the CIFS share information according to the following conditions:

- ○ The name of the CIFS share is `cifs2`.
- ○ Change the settings to disable the automatic home directory creation function.
- ○ Change the settings to display the CIFS share in the share name list.

```
$ sudo cifsedit -x cifs2 -b permit -o homedir=do_not_use
```

To edit the CIFS share information according to the following conditions:

- ○ The name of the CIFS share is `cifs3`.
- ○ Updates to the files in the CIFS share are cached on the client.
- ○ Change the setting for recording a successful access log entry when a client successfully establishes or terminates a connection to the CIFS share (`con`).
- ○ Change the setting for logging failed access attempts to `default` (apply the default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box).
- ○ A read-only client cache is not used when multiple CIFS clients simultaneously attempt to access a file.
- ○ Access-based enumeration is used.

```
$ sudo cifsedit -x cifs3 -C use -o "acsucc=con acfail=default
roc=do_not_use abe=use"
```

cifslist (List CIFS share information)

Synopsis (for cluster configurations)

```
cifslist [-x CIFS-share-name [-r resource-group-name]]
    [{-c|--del delimiter}] [-v] [-O extended-options]
```

extended-options:
```
    value[,value...]
```

Synopsis (for single node configurations)

```
cifslist [-x CIFS-share-name]
    [{-c|--del delimiter}] [-v] [-O extended-options]
```

extended-options:
```
    value[,value...]
```

Synopsis (to reference the command syntax)

```
cifslist -h
```

Description

Lists information about the CIFS shares on the node you are logged in to. Information is listed for each CIFS share in ascending order of the share names.

Options and arguments

`-c`

Specify this to display CIFS share information separated with colons (:).

`--del` *delimiter*

Specify this to display CIFS share information separated with an alphanumeric character, symbol, or space, whichever is specified.

`-O` *extended-options*

Specify which optional information to be displayed. If this option is omitted, optional information is not displayed.

When you want to display more than one optional information item, use a comma (,) to separate them.

You can specify the following values:

`g`

Specify this to view information about the `Guest account access`.

`s`

Specify this to view information about the `Disk synchronization policy`.

`c`

Specify this to view information about the `CIFS client cache`.

f

　　Specify this to view information about the `File timestamp changeable.`

h

　　Specify this to view information about the `Home directory.`

ls

　　Specify this to view information about the `CIFS access log (success).`

lf

　　Specify this to view information about the `CIFS access log (failure).`

A

　　Specify this to view information about the `ACL type.`

ap

　　Specify this to view information about the `Client access policy.`

vss

　　This item is not supported.

vssmc

　　This item is not supported.

roc

　　Specify this to view information about `Read-only cache for conflicts.`

abe

　　Specify this to view information about `Access Based Enumeration.`

ola

　　Specify this to view information about `Offline attribute.`

hdr

　　Specify this to view information about `Home directory roaming.`

rfmhdr

　　Specify this to view information about `Retry file modify (HDR).`

enc

　　Specify this to view information about `SMB encryption.`

1

　　Specify this to view information about the `Guest account access,` `Disk synchronization policy,` and `CIFS client cache.`

2

　　Specify this to view information about `File timestamp changeable.`

3

Specify this to view information about the `Home directory`, `CIFS access log (success)` and `CIFS access log (failure)`.

all

Specify this to view all optional information.

-r *resource-group-name*

Specify this to view information about a CIFS share in a specific resource group. Specify this option together with the `-x` option.

When the system is running in a degenerated state after a failover, two resource groups will be running on one node. If you omit this option, and both resource groups contain a CIFS share that have the same name, the command displays information about both CIFS shares.

-v

Specify this to view information about whether the users and the groups are permitted to write to CIFS shares.

-x *share-name*

Specify the share name to view information about a specific CIFS share. If you omit this option, information is listed about all the CIFS shares open on the node you are logged in to.

Displayed information

The following table lists the information displayed when you execute the command. Note that the information items are displayed in the following order, irrespective of the order in which the options and extended options are specified.

Table 2-102 Information displayed when executing the cifslist command

Item	Description
Name of file share	Displays the name of the CIFS share.
Shared directory	Displays the absolute path for the directory where the CIFS share was created.
Use ACL	Displays whether CIFS clients are allowed to view and set ACLs. use CIFS clients are allowed to view and set ACLs. not_use CIFS clients are not allowed to view and set ACLs.
Server specification	When specific hosts or networks are allowed to access the CIFS share, `make_public` appears in this item, followed by the specific host names or network addresses.

Item	Description
	When specific hosts or networks are not allowed to access the CIFS share, `do_not_make_public` appears in this item, followed by the specific host names or network addresses.
Comment for file share	Displays a comment about the CIFS share. The colon (:) in the comment is displayed even when you specify the `-c` option.

Permission mode	Displays access permission for the CIFS share.
	
	`ro`
	    Only read permission is granted.
	
	`rw`
	    Read and write permissions are granted.

Browse permission	Displays whether viewing the CIFS share name is permitted.
	
	`permit`
	    Viewing the CIFS share name is permitted.
	
	`do_not_permit`
	    Viewing the CIFS share name is not permitted.

File access permissions	Displays the access permissions when a file has been created in the writable CIFS share. The permissions are listed in the order owner, owner group, and others (for Advanced-ACL-type file systems, this means all users and groups). The permissions are separated by commas (,).
	
	When the file system to which the CIFS share belongs is of the Advanced ACL type and full permissions are set only for the owner (`rwx------`), `--` is displayed for this item. When the ACL type cannot be acquired, `Unknown` appears for this item.
	
	`ro`
	    The file is read-only.
	
	`rw`
	    Both read and write permissions are granted for the file.
	
	`none`
	    No access permissions are granted for the file.

Directory access permissions	Displays the access permissions when a directory has been created in a writable CIFS share. The permissions are listed in the order owner, owner group, and others (for Advanced-ACL-type file systems, this means all users and groups). The permissions are separated by commas (,).
	
	When the file system to which the CIFS share belongs is of the Advanced ACL type and full permissions are set only for the owner (`rwx------`), `--` is displayed for this item. When the ACL type cannot be acquired, `Unknown` appears for this item.
	
	`ro`
	    The directory is read-only.
	
	`rw`

Item	Description
	Both read and write permissions are granted for the directory.
	`none`
	No access permissions are granted for the directory.
`Write disallowed users`	Displays users who do not have write permission for the CIFS share.
	If no users are prohibited from writing to the CIFS share, `--` appears for this item.
`Write disallowed groups`	Displays groups that do not have write permission for the CIFS share.
	Each group name is prefixed with an at mark (`@`). If no groups are prohibited from writing to the CIFS share, `--` appears for this item.
`Write allowed users`	Displays users who have write permission for the CIFS share.
	If no users are allowed to write to the CIFS share, `--` appears for this item.
`Write allowed groups`	Displays groups that have write permission for the CIFS share.
	Each group name is prefixed with an at mark (`@`).
	If no groups are allowed to write to the CIFS share, `--` appears for this item.
`Guest account access`	Displays whether access to the CIFS share is permitted for guest accounts.
	`allow`
	Access is permitted for guest accounts.
	`disallow`
	Access is not permitted for guest accounts.
	`default`
	The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box applies.
`Disk synchronization policy`	Displays the operation to be performed for a write request issued from a CIFS client to a CIFS share.
	`write_and_close`
	Data is written synchronously with a write request or a close request.
	`close`
	Data is written synchronously with a close request.
	`none`
	Data is written at regular intervals, irrespective of the timing at which a write request or a close request is issued.
	`default`

Item	Description
	The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box applies.

`CIFS client cache`	Displays whether the updated data in the CIFS share file is cached on the client.
	
	`use`
	
	    Updated data is cached on the client.
	
	`do_not_use`
	
	    Updated data is not cached on the client.
	
	`default`
	
	    The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box applies.

`File timestamp changeable`	Displays users who can update the time-stamp of files in the CIFS share.
	
	When the ACL type of the file system in which the CIFS shares have been created is the Advanced ACL type, `--` appears for this item. When the ACL type cannot be acquired, `Unknown` appears for this item.
	
	`write_permitted_users`
	
	    All users with file write permission are allowed to update a file time-stamp.
	
	`owner_only`
	
	    Only the file owner is allowed to update a file time-stamp.
	
	`default`
	
	    The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box applies.

`Home directory`	Displays whether the automatic home directory creation function is enabled in the CIFS share.
	
	`use`
	
	    The automatic home directory creation function is enabled.
	
	`do_not_use`
	
	    The automatic home directory creation function is disabled.

`CIFS access log (success)`	Displays the setting information for recording a log entry when a CIFS client operation successfully accesses the CIFS share. The events are represented by the following character strings. When more than one event is specified, they are separated with commas (`,`). `lfld`

Item	Description
	An access log entry is recorded when a client successfully displays a folder list.
	`rdat`
	An access log entry is recorded when a client successfully reads data.
	`wdat`
	An access log entry is recorded when a client successfully creates or writes to a file.
	`cfld`
	An access log entry is recorded when a client successfully creates a folder.
	`del`
	An access log entry is recorded when a client successfully deletes a file or folder.
	`rper`
	An access log entry is recorded when a client successfully reads the access permissions for a file or folder.
	`cper`
	An access log entry is recorded when a client successfully changes the access permissions for a file or folder.
	`cown`
	An access log entry is recorded when a client successfully changes the owner of a file or folder.
	`rename`
	An access log entry is recorded when a client successfully renames a file or folder.
	`con`
	An access log entry is recorded when a client successfully establishes or terminates a connection to the CIFS share.
	`none`
	Successful access to the CIFS share is not logged.
	`default`
	The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box applies.
`CIFS access log (failure)`	Displays the setting information for recording a log entry when a CIFS client operation fails to access the CIFS share. The events are represented by the following character strings. When more than one event is specified, they are separated with commas (,).
	`lfld`
	An access log entry is recorded when a client fails to display a folder list.
	`rdat`

Item	Description
	An access log entry is recorded when a client fails to read data.
	`wdat`
	An access log entry is recorded when a client fails to create a file or write data.
	`cfld`
	An access log entry is recorded when a client fails to create a folder.
	`del`
	An access log entry is recorded when a client fails to delete a file or folder.
	`rper`
	An access log entry is recorded when a client fails to read the access permissions for a file or folder.
	`cper`
	An access log entry is recorded when a client fails to modify the access permissions for a file or folder.
	`cown`
	An access log entry is recorded when a client fails to change the owner of a file or folder.
	`rename`
	An access log entry is recorded when a client fails to rename a file or folder.
	`con`
	An access log entry is recorded when a client fails to establish or terminate a connection to the CIFS share.
	`none`
	Failed access to the CIFS share is not logged.
	`default`
	The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box applies.
`ACL type`	Displays the ACL type of the file system in which the CIFS shares have been created.
	`Advanced ACL`
	Advanced ACL type
	`Classic ACL`
	Classic ACL type
	`Unknown`
	The ACL type could not be acquired.
`Client access policy`	Displays how to process accesses from CIFS clients.
	`parallel`
	Displayed when accesses are processed in parallel.
	`serial`

Item	Description
	Displayed when accesses are processed serially. `default` The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box applies.
`Volume Shadow Copy Service`	`default` is displayed.
`Modified files check (VSS)`	This item is not supported.

`Read-only cache for conflicts`	Displays whether a read-only client cache is used when multiple CIFS clients simultaneously attempt to access a file.
	
	`use`
	
	Displayed when a read-only client cache is used.
	
	`do_not_use`
	
	Displayed when a read-only client cache is not used.
	
	`default`
	
	The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box is applied.

`Access Based Enumeration`	Displays whether access-based enumeration is used.
	
	`use`
	
	Displayed when access-based enumeration is used.
	
	`do_not_use`
	
	Displayed when access-based enumeration is not used.
	
	`default`
	
	The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box is applied.

`Offline attribute`	Displays whether the offline attribute is used.
	
	`use`
	
	Displayed when the offline attribute is used.
	
	`do_not_use`
	
	Displayed when the offline attribute is not used.

`Home directory roaming`	Displays whether roaming among HDI systems is possible for the data from the home directory created for each end-user.
	
	`use`
	
	Displayed when roaming is possible for the data.
	
	`do_not_use`
	
	Displayed when roaming is not possible for the data.

Hitachi Data Ingestor CLI Administrator's Guide

Item	Description

Retry file modify (HDR)	Displays whether the retry function is used to improve the status of the client that failed to create or update a file due to the temporary problem of the home directory being read-only.
	
	use
	
	    Displayed if the retry function is used.
	
	do_not_use
	
	    Displayed if the retry function is not used.

SMB encryption	Displays whether communication with the CIFS client is encrypted when using SMB 3.0.
	
	auto
	
	    Displayed only when the client supports encryption.
	
	mandatory
	
	    Displayed when encryption is mandatory.
	
	disable
	
	    Displayed when encryption is disabled.
	
	default
	
	    The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: Security) of the Access Protocol Configuration dialog box is applied.
	
	You can confirm whether SMB 3.0 is being used by checking the **CIFS Service Maintenance** page of the Access Protocol Configuration dialog box.

Return values

Table 2-103 Return values of the cifslist command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

cifslogctl (Manage CIFS access log information)

Synopsis

```
cifslogctl {--setdir directory-name|--display|--save}
cifslogctl --unsetdir [-f]
cifslogctl -h
```

Description

Sets, displays, or cancels the directory for saving CIFS access log information. If the directory used for saving CIFS access log information has already been set, you can save all the latest CIFS access log information at the same time.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Options and arguments

`--display`

> Specify this to view the current directory used for saving CIFS access log information.

`-f`

> Specify this to prevent the confirmation message from appearing.

`--save`

> Specify this to save the latest CIFS access log information.
>
> Before executing the command by specifying this option, check whether the directory for saving the CIFS access log information has been set.

`--setdir` *directory-name*

> Specify the absolute path of a directory in the file system where you want to save the CIFS access log information, using no more than 255 characters beginning with `/mnt/` . Note that `.snaps`, `.history`, `.arc`, `.system_gi`, `.system_reorganize`, `lost +found`, or `.lost+found` cannot be specified for a directory name. In addition, for a read-write-content-sharing file system, `.conflict` and `.conflict_longpath` also cannot be specified as a directory name.
>
> Note that a directory in the home-directory-roaming file system or read-write-content-sharing file system cannot be specified for the directory used for saving CIFS access log information.
>
> For physical nodes in a cluster configuration, you need to execute the command with this option on every physical node. Specify a file system on the node where you will execute the command.

`--unsetdir`

> Specify this to cancel the setting for the directory used for saving the CIFS access log information.
>
> Note:

Before deleting the transfer directory, cancel the setting for the directory.

Displayed information

The following table lists the information displayed by this command when the `--display` option is specified.

Table 2-104 Information displayed when executing the cifslogctl command with the --display option specified

Item	Description
Directory for saving	Displays the absolute path of the directory used for saving CIFS access log information.
	When no directory is set, Unsetting appears in this item.

Return values

Table 2-105 Return values of the cifslogctl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To set the directory used for saving CIFS access log information:

```
$ sudo cifslogctl --setdir /mnt/filesystem02/cifslog
```

To save the latest CIFS access log information:

```
$ sudo cifslogctl --save
```

cifsoptlist (Display the configuration definition for the CIFS service)

Synopsis

```
cifsoptlist [-s|-x CIFS-share-name]
cifsoptlist -h
```

Description

Displays information set for the configuration definition for the CIFS service and the CIFS share.

Options and arguments

-s

Specify this to view information specified for the configuration definition for the CIFS service.

-x *CIFS-share-name*

Specify this to view the information set for a specific CIFS share.

Note that if you omit all options, the information set for the configuration definition for the CIFS service and for all CIFS shares of the node to which you are logged in is displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-106 Information displayed when executing the cifsoptlist command

Item	Description
information-to-be-displayed	Displays the applicable information. If the information is the configuration information of the CIFS service, `CIFS service` is displayed. If the information is CIFS share information, the CIFS share name is displayed.

`case_sensitive`	Displays whether to distinguish between upper-case and lower-case characters contained in the file name.
	
	`on`
	
	The file name is case sensitive.
	
	`off`
	
	The file name is not case sensitive.
	
	`inherit`
	
	The CIFS share settings follow the settings for the configuration definition of the CIFS service.

`max_cifs_processes`	Displays the maximum number of CIFS connections.

Item	Description
dfree_cache_time	Displays the number of seconds for which information about the unused capacity of the disk is cached.

use_gidnumber	Displays whether to use the gidNumber of the user, or the gidNumber of the group that the user belongs to, as a group ID of the primary group for the UNIX attribute of Active Directory. This item is enabled when the method of user mapping is the schema method of Active Directory, and **Using LDAP as a network information service (RFC2307)** is specified to **Name service switch** at **User mapping setup** on the **CIFS Service Management** page (**Setting Type**: User mapping). When **Using LDAP as a network information service (RFC2307)** is not specified to **Name service switch**, CIFS service is not affected even if yes is displayed.
	
	yes
	
	    This is displayed when the user's gidNumber is used.
	
	no
	
	    This is displayed when the gidNumber of the group that the user belongs to is used.

pending_delete_dir	Displays whether to wait until a folder in a CIFS share is closed to delete it when another user currently has the folder open.
	
	yes
	
	    This is displayed when the folder is not deleted until it is closed.
	
	no
	
	    This is displayed when the folder is deleted immediately, without waiting until it is closed.

change_notify	This indicates whether the client is notified when the monitoring targets are changed in response to a request from the client to monitor the folders and files in a folder.
	
	yes
	
	    This is displayed if the client is to be notified.
	
	no
	
	    This is displayed if the client is not to be notified.
	
	inherit
	
	    This is displayed when the CIFS share inherits the corresponding setting in the CIFS service configuration definition.

unix_extensions	Displays whether the UNIX client extended functionality is used when a client accesses the CIFS service.
	
	yes
	
	    This is displayed if the UNIX client extended functionality is used whenever a client accesses the CIFS service.
	
	no
	
	    This is displayed if the UNIX client extended functionality is not used whenever a client accesses the CIFS service.

client_ldap_sasl_wrapping	Displays whether LDAP communication with a domain controller is signed.

Item	Description
	`plain`
	This is displayed if LDAP communication with the domain controller is not signed.
	`sign`
	This is displayed if LDAP communication with the domain controller is signed.
`enable_watch_subtree`	This indicates whether the client is notified when the monitoring targets are changed in response to a request from the client to monitor all the folders and files in the specified folder.
	`yes`
	This is displayed if the client is to be notified.
	`no`
	This is displayed if the client is not to be notified.
`notify_delay_time`	This indicates the amount of time (units: milliseconds) by which notification to the client is delayed after the monitoring targets are changed in response to a request from the client to monitor the files in a folder.
	If the settings common to CIFS are subject to the settings of the configuration definition for the CIFS service, `inherit` is displayed.
`performance_monitor`	Displays whether to collect performance statistics of a CIFS service.
	`yes`
	Collect performance statistics of the CIFS service.
	`no`
	Do not collect performance statistics of the CIFS service.
`hide_system_files`	Displays whether files and folders used by the system are excluded from an object list when replying to a request from the client to obtain the object list.
	`yes`
	Files and folders used by the system are excluded from the list.
	`no`
	Files and folders used by the system are included in the list.
	`inherit`
	This is displayed when the CIFS share inherits the corresponding setting in the CIFS service configuration definition.
`hd_upperlower_mixed`	Displays whether a mixture of uppercase and lowercase letters is allowed in the home directory name on the home-directory-roaming file system.
	`yes`
	A mixture of uppercase and lowercase letters is allowed in the home directory name.
	`no`

Item	Description
	A mixture of uppercase and lowercase letters is not allowed in the home directory name.
	`inherit` This is displayed when the CIFS share inherits the corresponding setting in the CIFS service configuration definition.

`enable_additional_builtin_sid`	Displays whether ACL is enabled for the default Windows-domain user groups `Authenticated Users` and `Network`.
	
	`yes`
	
	Displays when enable ACL for `Authenticated Users` and `Network`.
	
	`no`
	
	Displays when disable ACL for `Authenticated Users` and `Network`.

`server_signing`	Displays whether SMB signing is used during communication with a SMB 1.0 CIFS client that requires SMB signing.
	
	`auto`
	
	Displayed when SMB signing is used.
	
	`disabled`
	
	Displayed when SMB signing is not used.

`logging_unsupported_access`	This command shows whether records are output to the CIFS access log and SNMP trap notifications are sent for unsupported settings requested by a CIFS client for an ACL or file attribute.
	
	`yes`
	
	This is displayed if unsupported settings are recorded in the CIFS access log and the corresponding SNMP trap notifications are sent.
	
	`no`
	
	This is displayed if unsupported settings are not recorded in the CIFS access log and SNMP trap notifications are not sent.
	
	`inherit`
	
	This is displayed when the CIFS share inherits the corresponding setting in the CIFS service configuration definition.

`check_strict_allocate`	Displays whether to check the amount of free space in the file system before data is written to a file to be created or overwritten.
	
	`yes`
	
	The amount of free space is checked before data is written.
	
	`no`
	
	The amount of free space is not checked before data is written.
	
	`inherit`

Item	Description
	This is displayed when the CIFS share inherits the corresponding setting in the CIFS service configuration definition.
opt_deny_server	Displays the IP address specified for suppressing communication during CIFS client authentication to a domain controller that cannot establish a connection with HDI system. If more than one IP address is specified, they are separated with commas (,). If communication to the domain controller is not suppressed, disabled is displayed.
client_max_protocol	Displays the newest version of the SMB protocol to be used to communicate with another file server when using the CIFS protocol to import data from the file server. SMB1.0 This is displayed if the newest version of the protocol is SMB 1.0. SMB2.0 This is displayed if the newest version of the protocol is SMB 2.0. SMB2.1 This is displayed if the newest version of the protocol is SMB 2.1. SMB3.0 This is displayed if the newest version of the protocol is SMB 3.0.
client_min_protocol	Displays the oldest version of the SMB protocol to be used to communicate with another file server when using the CIFS protocol to import data from the file server. SMB1.0 This is displayed if the oldest version of the protocol is SMB 1.0. SMB2.0 This is displayed if the oldest version of the protocol is SMB 2.0. SMB2.1 This is displayed if the oldest version of the protocol is SMB 2.1. SMB3.0 This is displayed if the oldest version of the protocol is SMB 3.0.
client_signing	Displays whether SMB signing is to be requested for communication with another file server when using the CIFS protocol to import data from the file server. auto This is displayed if SMB signing is used but does not request SMB signing to the import-source file server. mandatory

Item	Description
	This is displayed if SMB signing is to be requested to the import-source file server.

client_ipc_max_prot ocol	Displays the newest version of the SMB protocol to be used to communicate with the domain controller when joining domains or authenticating users.
	
	SMB1.0
	
	    This is displayed if the newest version of the protocol is SMB 1.0.
	
	SMB2.0
	
	    This is displayed if the newest version of the protocol is SMB 2.0.
	
	SMB2.1
	
	    This is displayed if the newest version of the protocol is SMB 2.1.
	
	SMB3.0
	
	    This is displayed if the newest version of the protocol is SMB 3.0.

client_ipc_min_prot ocol	Displays the oldest version of the SMB protocol to be used to communicate with the domain controller when joining domains or authenticating users.
	
	SMB1.0
	
	    This is displayed if the oldest version of the protocol is SMB 1.0.
	
	SMB2.0
	
	    This is displayed if the oldest version of the protocol is SMB 2.0.
	
	SMB2.1
	
	    This is displayed if the oldest version of the protocol is SMB 2.1.
	
	SMB3.0
	
	    This is displayed if the oldest version of the protocol is SMB 3.0.

client_ipc_signing	Displays whether SMB signing is to be requested for communication with the domain controller when joining domains or authenticating users.
	
	auto
	
	    This is displayed if SMB signing is used but does not request SMB signing to the domain controller.
	
	mandatory
	
	    This is displayed if SMB signing is to be requested to the domain controller.

Table 2-107 Return values of the cifsoptlist command

Return value	Description
0	Normal termination
1	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
4	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

cifsoptset (Change the configuration definition of the CIFS service)

Synopsis

```
cifsoptset extended-option {-s|-x CIFS-share-name}
cifsoptset -h
```

Expansion option:

```
case_sensitive {on|off|default}
max_cifs_processes
dfree_cache_time number-of-seconds-for-which-caching-is-performed
use_gidnumber {yes|no}
pending_delete_dir {yes|no}
change_notify {yes|no|default}
unix_extensions {yes|no}
client_ldap_sasl_wrapping {plain|sign}
enable_watch_subtree {yes|no}
notify_delay_time {delay-time|default}
hide_system_files {yes|no|default}
hd_upperlower_mixed {yes|no|default}
enable_additional_builtin_sid {yes|no}
server_signing {auto|disabled}
logging_unsupported_access {yes|no|default}
check_strict_allocate {yes|no|default}
opt_deny_server {domain-controller-IP-address
    [,domain-controller-IP-address...]|disabled}
client_max_protocol {SMB1.0|SMB2.0|SMB2.1|SMB3.0|default}
client_min_protocol {SMB1.0|SMB2.0|SMB2.1|SMB3.0|default}
client_signing {auto|mandatory}
```

```
client_ipc_max_protocol {SMB1.0|SMB2.0|SMB2.1|SMB3.0|default}
client_ipc_min_protocol {SMB1.0|SMB2.0|SMB2.1|SMB3.0|default}
client_ipc_signing {auto|mandatory}
```

Description

Changes the configuration definition for the CIFS service and the settings for the CIFS share of the node you are logged in to.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Execute this command for each node so that the settings in the configuration definition for the CIFS service will be the same across the cluster.

Options and arguments

`-s`

Specify this to change the configuration definition settings of the CIFS service.

`-x` *CIFS-share-name*

Specify this to change the settings for a specific CIFS share.

extended-option

Specify the extended option to be set for the configuration definition for the CIFS service and the CIFS share. Use the following format to specify the extended option:

option-identifier value...

The extended option you can specify is as follows:

`case_sensitive {on|off|default}`

Specify whether to distinguish between upper-case and lower-case characters in a file name.

If automatic reloading of CIFS share settings is enabled in the CIFS service configuration, to apply settings changes to a CIFS client that is currently connected to the CIFS service, log off of the CIFS client and then log on again. Alternatively, restart the CIFS service.

`on`

Specify this to make file names case sensitive.

`off`

Specify this to not make file names case sensitive. The initial setting in the configuration definition for the CIFS service is `off`.

`default`

Specify this to apply the default setting. If you specify this with the `-s` option, `off` is set in the configuration definition of the CIFS service. If you specify this with the `-x` option, the setting in the configuration definition of the CIFS service is applied to the CIFS share. In addition, the setting in the configuration definition for the CIFS service is inherited as the initial setting for the CIFS share. If you execute a

command by specifying `-s` option while the CIFS service is running, restart the CIFS service after completing the command execution.

Note:

In CIFS clients (Windows), upper-case and lower-case characters are usually not distinguished. Accordingly, if the configuration definition information of the CIFS service or CIFS share is set to distinguish between upper-case and lower-case characters in file names, a CIFS client might perform operations on an unintended file.

Note:

If the CIFS service configuration definition settings have been specified to allow the CIFS share settings to be automatically reloaded and the following condition is met, restart the CIFS service after completing the command execution.

- This option is specified with `default` specified when the `-s` option is also specified.

If the CIFS service configuration definition settings have been specified to allow the CIFS share settings to be automatically reloaded and either of the following conditions is met, in order to apply the changes made to the connected CIFS client, log out from the CIFS client and then log in again, or restart the CIFS service.

- This option is specified with `on` or `off` specified when the `-s` option is also specified.

- This option is specified with `default` specified when the `-x` option is also specified.

`max_cifs_processes`

This option is not supported.

`dfree_cache_time` *number-of-seconds-for-which-caching-is-performed*

Specify this to specify the number of seconds for which the HDI system caches information about unused capacity of the disk in the range from 0 to 300 (units: seconds). Note that if you specify 0, the latest information is always displayed, and caching is not performed. Specify this together with the `-s` option. The default is `1`.

`use_gidnumber {yes|no}`

Specify whether to use the gidNumber of the user, or that of a group that the user belongs to, as a group ID of the primary group for the UNIX attribute of Active Directory. Specify this together with the `-s` option. This option is enabled when the method of user mapping is a schema method of Active Directory, and **Using LDAP as a network information service (RFC2307)** is specified to **Name service switch** at **User mapping setup** on **CIFS Service Management** page (**Setting Type**: `User mapping`). If you execute a command by specifying this option while the CIFS service is running, restart the CIFS service after completing the command execution.

`yes`

Specify this to use the user's gidNumber.

no

Specify this to use the gidNumber of the group that the user belongs to. The default is `no`.

`pending_delete_dir {yes|no}`

Specify this option to determine whether to wait until a folder in a CIFS share is closed to delete it when another user currently has the folder open. Specify this together with the `-s` option.

yes

Specify this to wait until the folder is closed to delete it.

no

Specify this to delete the folder immediately, without waiting until it is closed. The default is `no`.

`change_notify {yes|no|default}`

Specify whether to notify the client when the monitoring targets are changed in response to a request from the client to monitor the folders and files in a folder.

If automatic reloading of CIFS share settings is enabled in the CIFS service configuration, to apply settings changes to a CIFS client that is currently connected to the CIFS service, log off of the CIFS client and then log on again. Alternatively, restart the CIFS service.

yes

Specify this to notify the client. The initial setting in the configuration definition for the CIFS service is `yes`.

no

This is displayed if the client is not to be notified. After you execute the command, you must manually refresh the folder and file information displayed on the CIFS client. If the most recent information is not displayed after you manually refresh the information, wait a while and then refresh the information again.

default

Specify this to apply the default setting. If you specify this with the `-s` option, `yes` is set in the configuration definition of the CIFS service. If you specify this with the `-x` option, the setting in the configuration definition of the CIFS service is applied to the CIFS share. In addition, the setting in the configuration definition for the CIFS service is inherited as the initial setting for the CIFS share. If you execute a command by specifying `-s` option while the CIFS service is running, restart the CIFS service after completing the command execution.

`unix_extensions {yes|no}`

Specify this to determine whether to use the UNIX client extended functionality when a client accesses the CIFS service. Specify this together with the `-s` option.

If automatic reloading of CIFS share settings is enabled in the CIFS service configuration, to apply settings changes to a CIFS client that is

currently connected to the CIFS service, log off of the CIFS client and then log on again. Alternatively, restart the CIFS service.

yes

Specify this to use the UNIX client extended functionality whenever a client accesses the CIFS service.

no

Specify this to not use the UNIX client extended functionality whenever a client accesses the CIFS service. The default is no.

client_ldap_sasl_wrapping {plain|sign}

Specify this to determine whether to sign the LDAP communication with domain controllers. Specify this together with the -s option. If you execute a command by specifying this option while the CIFS service is running, restart the CIFS service after completing the command execution.

plain

Specify this to connect to domain controllers that do not use signed LDAP communication.

sign

Specify this to connect to domain controllers that use signed LDAP communication. The default is sign.

enable_watch_subtree {yes|no}

Specify whether to notify the client when the monitoring targets are changed in response to a request from a client to monitor all the folders and files in the specified folder. Specify this together with the -s option.

yes

Specify this to notify the client.

no

Specify this to not notify the client. The default is no.

Note:

When yes is set for this option, if a large number of CIFS clients connect to HDI, the load on HDI increases, which might cause a delayed response to one or more clients. In such cases, setting no for this option might alleviate the problem.

notify_delay_time {*delay-time*|default}

Specify how long to delay notification to the client after the monitoring targets are changed in response to a request from the client to monitor the files in a folder.

If automatic reloading of CIFS share settings is enabled in the CIFS service configuration, to apply settings changes to a CIFS client that is currently connected to the CIFS service, log off of the CIFS client and then log on again. Alternatively, restart the CIFS service.

delay-time

Specify the length of time to delay notification. The specifiable range is 0 to 60,000 (units: milliseconds). The initial setting in the configuration definition for the CIFS service is `3,000`.

`default`

Specify this to apply the default setting. If you specify this with the `-s` option, `3,000` is set in the configuration definition of the CIFS service. If you specify this with the `-x` option, the setting in the configuration definition of the CIFS service is applied to the CIFS share. In addition, the setting in the configuration definition for the CIFS service is inherited as the initial setting for the CIFS share.

`hide_system_files {yes|no|default}`

Specifies whether to exclude files and folders used by the system from an object list when replying to a request from the client to obtain the object list. If files and folders used by the system are excluded from the list, if the client then sets the ACL to multiple objects in a folder at once, the processing will not be interrupted by a possible failure to set the ACL to files and folders used by the system. For details on files and folders used by the system, see the *File System Protocols (CIFS/ NFS) Administrator's Guide*.

If automatic reloading of CIFS share settings is enabled in the CIFS service configuration, to apply settings changes to a CIFS client that is currently connected to the CIFS service, log off of the CIFS client and then log on again. Alternatively, restart the CIFS service.

`yes`

Excludes files and folders used by the system from the list.

`no`

Includes files and folders used by the system in the list.

`default`

Specify this to apply the default setting. If you specify this with the `-s` option, `no` is set in the configuration definition of the CIFS service. If you specify this with the `-x` option, the setting in the configuration definition of the CIFS service is applied to the CIFS share. In addition, the setting in the configuration definition for the CIFS service is inherited as the initial setting for the CIFS share. If you execute a command by specifying `-s` option while the CIFS service is running, restart the CIFS service after completing the command execution.

Note:

If `yes` is specified, if one file or folder is created and has the same name as another file or folder used by the system, the created file or folder is excluded from the list.

Note:

If the CIFS service configuration definition settings have been specified to allow the CIFS share settings to be automatically reloaded and the following condition is met, restart the CIFS service after completing the command execution.

- This option is specified with `default` specified when the `-s` option is also specified.

If the CIFS service configuration definition settings have been specified to allow the CIFS share settings to be automatically reloaded and either of the following conditions is met, in order to apply the changes made to the connected CIFS client, log out from the CIFS client and then log in again, or restart the CIFS service.

- This option is specified with `yes` or `no` specified when the `-s` option is also specified.

- This option is specified with `default` specified when the `-x` option is also specified.

hd_upperlower_mixed {yes|no|default}

Specifies whether to allow a mixture of uppercase and lowercase letters in the home directory name in the home-directory-roaming file system.

yes

Allows a mixture of uppercase and lowercase letters in the home directory name. The initial setting in the configuration definition for the CIFS service is `yes`.

no

Does not allow a mixture of uppercase and lowercase letters in the home directory name.

default

Specify this to apply the default setting. If you specify this with the `-s` option, `yes` is set in the configuration definition of the CIFS service. If you specify this with the `-x` option, the setting in the configuration definition of the CIFS service is applied to the CIFS share. In addition, the setting in the configuration definition for the CIFS service is inherited as the initial setting for the CIFS share. If you execute a command by specifying `-s` option while the CIFS service is running, restart the CIFS service after completing the command execution.

enable_additional_builtin_sid {yes|no}

This specifies whether to enable ACL for the default Windows-domain user groups `Authenticated Users` and `Network`. Specify this together with the `-s` option.

When using this option, note the following points:

○ Before executing the command, ask either the CIFS administrator or the end user to terminate all connections from CIFS clients.

○ If you executed the command while the CIFS service was running, restart the CIFS service after the command has been executed.

yes

Specify this if you want to enable ACL for `Authenticated Users` and `Network`.

Tip: When you import data from another file server, the ACL settings for `Authenticated Users` and `Network` are not imported. In addition, the

Hitachi Data Ingestor CLI Administrator's Guide

dirsetacl command cannot specify `Authenticated Users` and `Network` as the group names. Specify the following group IDs:

- `Authenticated Users: 4294900000`

- `Network: 4294900001`

`no`

Specify this if you want to disable ACL for `Authenticated Users` and `Network`. The default is `no`.

`server_signing {auto|disabled}`

Specifies whether to use SMB signing during communication with an SMB 1.0 CIFS client that requires SMB signing. Even if you specify the setting to not use SMB signing, the system operates with the setting to use SMB signing during communication with SMB 2.0, 2.1 and 3.0. Specify this together with the `-s` option. If you execute a command by specifying this option while the CIFS service is running, restart the CIFS service after completing the command execution.

`auto`

Specify this to use SMB signing.

`disabled`

Specify this to not use SMB signing. The default is `disabled`.

`logging_unsupported_access {yes|no|default}`

Use this command to specify whether to record unsupported settings in the CIFS access log and send the corresponding SNMP notifications when a CIFS client requests an unsupported setting for an ACL or a file attribute. Note that this option's settings only take effect if the CIFS access log function is enabled in the CIFS service configuration definitions on the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box.

`yes`

Specify this option to record unsupported settings in the CIFS access log and send the corresponding SNMP trap notifications. Note, however, that if the file system to be accessed uses classic ACLs, even if `yes` is specified, records will not be made to the CIFS access log and SNMP trap notifications will not be sent.

`no`

Specify this option if unsupported settings are not to be recorded in the CIFS access log and SNMP trap notifications are not to be sent. The initial setting in the configuration definition for the CIFS service is `no`.

`default`

Specify this to apply the default setting. If you specify this with the `-s` option, `no` is set in the configuration definition of the CIFS service. If you specify this with the `-x` option, the setting in the configuration definition of the CIFS service is applied to the CIFS share.

Note:

If the CIFS service configuration definition settings have been specified to allow the CIFS share settings to be automatically reloaded and either of

the following conditions is met, in order to apply the changes made to the connected CIFS client, log out from the CIFS client and then log in again.

- This option is specified when the `-s` option is also specified.

- This option is specified with `default` specified when the `-x` option is also specified.

check_strict_allocate {yes|no|default}

Specify whether to check the amount of free space in the file system before data is written to a file to be created or overwritten.

yes

The amount of free space in the file system is checked before data is written.

If you specify this argument, the usage for the quota, excluding the namespace quota, and the usage for the file system will be calculated before data is written to a file to be created or overwritten. The amount of free space in the file system for writing data will be checked in units of 1 megabyte. If the file system does not have sufficient free space, an error occurs on the CIFS client side due to insufficient free space.

no

The amount of free space in the file system is not checked before data is written. The initial setting in the configuration definition for the CIFS service is `no`.

default

Specify this to apply the default setting. If you specify this with the `-s` option, `no` is set in the configuration definition of the CIFS service. If you specify this with the `-x` option, the setting in the configuration definition of the CIFS service is applied to the CIFS share.

Note:

Regardless of whether the amount of free space in the file system is checked before data is written, an error occurs on the CIFS client side if the amount of free space becomes insufficient while the data is being written. At this time, some clients might not be able to determine that the error is caused by insufficient free space.

Note:

If an error occurs due to insufficient free space, delete unnecessary files or save those files in another file system to increase the amount of free space, and then retry the operation. Alternatively, create the file in another file system or folder.

Note:

Even if the disk space viewed from the CIFS client indicates that there is sufficient free space to write data, an error might occur due to insufficient disk space. In this case, use the `fslist` command to check the available space in the file system block. In addition, use the `quotaget` and `stquota` commands to check the block usage and the inode usage for the user or affiliated group.

Note:

If the CIFS service configuration definition settings have been specified to allow the CIFS share settings to be automatically reloaded and either of

Hitachi Data Ingestor CLI Administrator's Guide

the following conditions is met, in order to apply the changes made to the connected CIFS client, log out from the CIFS client and then log in again, or restart the CIFS service.

- This option is specified when the `-s` option is also specified.

- This option is specified with default specified when the `-x` option is also specified.

`opt_deny_server {`*`domain-controller-IP-address`*`[,`*`domain-controller-IP-address`*`...]|disabled}`

Specify this option to set the IP address of the domain controller, in order to suppress communication during CIFS client authentication to a domain controller that cannot establish a connection with HDI system, or to cancel the suppression of communication to the domain controller.

This option can be used to reduce delays in the processing for CIFS client authentication, by suppressing communication to the target domain controller if the processing of connecting HDI system with the domain controller during CIFS client authentication times out frequently.

Specify this together with the `-s` option. If you execute a command by specifying this option while the CIFS service is running, restart the CIFS service after completing the command execution.

`domain-controller-IP-address``[,`*`domain-controller-IP-address`*`...]`

Specify the IP address in IPv4 or IPv6 format. If there are multiple IP addresses, separate them by inserting a commas (,) between each one, and specify the IP addresses by using 1,095 characters or less. If the IP address is already specified, all the settings are canceled and the new IP address is specified. Note that the argument specified for this option is valid only if the authentication mode of the CIFS service is set for Active Directory authentication.

`disabled`

Specify this option to cancel the suppression of communication to the domain controller. The default is `disabled`.

`client_max_protocol {SMB1.0|SMB2.0|SMB2.1|SMB3.0|default}`

To use the CIFS protocol to import data from another file server, specify the newest version of the SMB protocol to be used to communicate with the file server. Specify this together with the `-s` option. Note that, set `client_max_protocol`, `client_min_protocol`, and `client_signing`, then restart the node.

`SMB1.0`

Specify this to use SMB 1.0 as the newest version of the SMB protocol.

`SMB2.0`

Specify this to use SMB 2.0 as the newest version of the SMB protocol.

`SMB2.1`

Specify this to use SMB 2.1 as the newest version of the SMB protocol.

`SMB3.0`

Specify this to use SMB 3.0 as the newest version of the SMB protocol. The default is `SMB3.0`.

`default`

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

Specify this to apply the default setting. If you specify this argument, `SMB3.0` is set.

Note:

The protocol version set for `client_max_protocol` must be the same as, or later than, the protocol version set for `client_min_protocol`.

Note:

The setting specified for this option might cause communication with the import-source file server to fail. Before changing this option, check which versions of the SMB protocol the import-source file server supports.

`client_min_protocol {SMB1.0|SMB2.0|SMB2.1|SMB3.0|default}`

To use the CIFS protocol to import data from another file server, specify the oldest version of the SMB protocol to be used to communicate with the file server. Specify this together with the `-s` option. Note that, set `client_max_protocol`, `client_min_protocol`, and `client_signing`, then restart the node.

`SMB1.0`

Specify this to use SMB 1.0 as the oldest version of the SMB protocol.

`SMB2.0`

Specify this to use SMB 2.0 as the oldest version of the SMB protocol. The default is `SMB2.0`.

`SMB2.1`

Specify this to use SMB 2.1 as the oldest version of the SMB protocol.

`SMB3.0`

Specify this to use SMB 3.0 as the oldest version of the SMB protocol.

`default`

Specify this to apply the default setting. If you specify this argument, `SMB2.0` is set.

Note:

The protocol version set for `client_max_protocol` must be the same as, or later than, the protocol version set for `client_min_protocol`.

Note:

The setting specified for this option might cause communication with the import-source file server to fail. Before changing this option, check which versions of the SMB protocol the import-source file server supports.

`client_signing {auto|mandatory}`

Specify whether to request SMB signing for communication with another file server when using the CIFS protocol to import data from the file server. Specify this together with the `-s` option. Note that, set `client_max_protocol`, `client_min_protocol`, and `client_signing`, then restart the node.

`auto`

Specify this if you want to use the SMB signing but does not request SMB signing to the import-source file server. The default is `auto`.

`mandatory`

Specify this if you want to request SMB signing.

`client_ipc_max_protocol {SMB1.0|SMB2.0|SMB2.1|SMB3.0|default}`

Specify the newest version of the SMB protocol to be used to communicate with the domain controller when joining domains or authenticating users. Specify this together with the `-s` option. If you execute a command by specifying this option while the CIFS service is running, set `client_ipc_max_protocol`, `client_ipc_min_protocol`, and `client_ipc_signing`, then restart the CIFS service.

`SMB1.0`

Specify this to use SMB 1.0 as the newest version of the SMB protocol.

`SMB2.0`

Specify this to use SMB 2.0 as the newest version of the SMB protocol.

`SMB2.1`

Specify this to use SMB 2.1 as the newest version of the SMB protocol.

`SMB3.0`

Specify this to use SMB 3.0 as the newest version of the SMB protocol. The default is `SMB3.0`.

`default`

Specify this to apply the default setting. If you specify this argument, `SMB3.0` is set.

Note:

The protocol version set for `client_ipc_max_protocol` must be the same as, or later than, the protocol version set for `client_ipc_min_protocol`.

Note:

The setting specified for this option might cause communication with the domain controller to fail. Before setting this option, check which versions of the SMB protocol the domain controller supports.

`client_ipc_min_protocol {SMB1.0|SMB2.0|SMB2.1|SMB3.0|default}`

Specify the oldest version of the SMB protocol to be used to communicate with the domain controller when joining domains or authenticating users. Specify this together with the `-s` option. If you execute a command by specifying this option while the CIFS service is running, set `client_ipc_max_protocol`, `client_ipc_min_protocol`, and `client_ipc_signing`, and then restart the CIFS service.

`SMB1.0`

Specify this to use SMB 1.0 as the oldest version of the SMB protocol.

`SMB2.0`

Specify this to use SMB 2.0 as the oldest version of the SMB protocol. The default is `SMB2.0`.

`SMB2.1`

Specify this to use SMB 2.1 as the oldest version of the SMB protocol.

`SMB3.0`

Specify this to use SMB 3.0 as the oldest version of the SMB protocol.

`default`

Specify this to apply the default setting. If you specify this argument, `SMB2.0` is set.

Note:

The protocol version set for `client_ipc_max_protocol` must be the same as, or later than, the protocol version set for `client_ipc_min_protocol`.

Note:

The setting specified for this option might cause communication with the domain controller to fail. Before setting this option, check which versions of the SMB protocol the domain controller supports.

`client_ipc_signing {auto|mandatory}`

Specify whether SMB signing is to be requested for communication with the domain controller when joining domains or authenticating users. Specify this together with the `-s` option. If you execute a command by specifying this option while the CIFS service is running, set `client_ipc_max_protocol`, `client_ipc_min_protocol`, and `client_ipc_signing`, then restart the CIFS service.

`auto`

Specify this if you want to use the SMB signing but does not request SMB signing to the domain controller. The default is `auto`.

`mandatory`

Specify this if you want to request SMB signing.

Return values

Table 2-108 Return values of the cifsoptset command

Return value	Description
0	Normal termination
1, 2	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
3, 4, 5	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To change the CIFS share (`cifs1`) setting so that the upper-case and lower-case characters in file names are not distinguished:

```
$ sudo cifsoptset case_sensitive off -x cifs1
```

cifsrestore (Restore CIFS share information)

Synopsis

```
cifsrestore information-definition-file-name
cifsrestore --list information-definition-file-name
cifsrestore --template template-file-name
    information-definition-file-name
cifsrestore -h
```

Description

Restores information about CIFS shares based on the CIFS share information that has been backed up to an information definition file by using the `cifsbackup` command. You can also display the CIFS share information without restoring it, or create a template file of scripts for performing restoration.

Note that depending on the number of CIFS shares that will be restored and the number of CIFS shares that have already been created, the restoration process might take a while. For example, it takes about two minutes to restore 20 CIFS shares.

You can restore CIFS share information if the following conditions are met:

- The name of the target file system has not been changed since the CIFS share information was backed up.
- The target file system has been mounted.
- The directory in which the CIFS shares were created still exist in the target file system.
- A CIFS share has not been created in the target file system.
- If a cluster configuration is used, the same CIFS share name does not exist in the target resource group.
- If a single node configuration, the same CIFS share name does not exist in a node.
- The names of all users and groups that have been granted or denied write permission for the backed-up CIFS share can be resolved.
- A CIFS share in a home-directory-roaming file system must be restored in a home-directory-roaming file system. If a CIFS share in a home-directory-roaming file system is restored to a non-home-directory-roaming file system, the home-directory-roaming functionality is disabled.

Options and arguments

`--list`

Specify this option to display the contents of an information definition file.

`--template` *template-file-name*

Specify this option to create a template file of scripts for restoring based on the contents of the information definition file.

Specify a template file name using no more than 255 characters. You can use alphanumeric characters, hyphens (-), and underscores (_). However, hyphens cannot be used as the first character of the file name. You can also use periods (.), except at the beginning or end of the character string.

The template file will be output immediately under the SSH account home directory (/home/nasroot). The file cannot have the same name as an existing file in the /home/nasroot directory.

The template file can be transferred, and then edited or executed on a remote host. If you want to restore CIFS share information that is different from the backed-up information, edit the template file according to your purpose, and then execute the template file. To transfer the template file, use the scp command or some other secure transfer tools.

The following shows an example of a template file.

```
#!/bin/sh
##############################################################################
#####
# This template is for scripts used to restore CIFS share settings.
# Note:
#   You must edit this template to create a script that can handle
#   command execution errors, and execute commands from remote hosts.
##############################################################################
#####

PRECMD=""

/bin/echo Executing\ the\ command\ cifscreate\(cifsshare01\)\.\.\.\.\.\.
$PRECMD sudo cifscreate -x cifsshare01 -d \/mnt\/FS01\/dir01 -c "cifs
comment" -a "use" -p "rw" -b "permit" -g "allow" -t
"write_permitted_users" -C "default" -s "make_public:hostA,hostB" -S
"close" -f "rw,rw,rw" -F "rw,rw,rw" -o "homedir=do_not_use acpol=parallel
vss=default vssmc=default enc=default roc=default abe=default ola=use
rfmhdr=do_not_use acsucc=none acfail=none" -A "add:usr001" -D "add:usr002"

/bin/echo Executing\ the\ command\ cifscreate\(common\)\.\.\.\.\.\.
$PRECMD sudo cifscreate -x common -d \/mnt\/FS01\/common -a "use" -p "rw" -
b "permit" -g "allow" -t "write_permitted_users" -C "default" -s
"make_public:hostA,hostB" -S "close" -f "rw,rw,rw" -F "rw,rw,rw" -o
"homedir=use acpol=parallel vss=default vssmc=default enc=auto roc=default
abe=default ola=do_not_use rfmhdr=do_not_use acsucc=none
acfail=del,lfld,rdat,rper,wdat"

/bin/echo Executing\ the\ command\ cifscreate\(documents\)\.\.\.\.\.\.
$PRECMD sudo cifscreate -x documents -d \/mnt\/FS01\/docs -a "use" -p "rw"
-b "permit" -g "allow" -t "write_permitted_users" -C "default" -s
"make_public:hostA,hostB" -S "close" -f "rw,rw,rw" -F "rw,rw,rw" -o
"homedir=use acpol=serial vss=do_not_use vssmc=do_not_use enc=auto
roc=do_not_use abe=do_not_use ola=use rfmhdr=do_not_use
acsucc=cfld,con,cown,cper acfail=del,lfld,rdat,rper,wdat"

/bin/echo Executing\ the\ command\ cifscreate\(test01\)\.\.\.\.\.\.
$PRECMD sudo cifscreate -x test01 -d \/mnt\/FS01\/test01 -a "use" -p "rw" -
b "permit" -g "allow" -t "write_permitted_users" -C "default" -s
"make_public:hostA,hostB" -S "write_and_close" -f "rw,rw,rw" -F "rw,rw,rw"
-o "homedir=use acpol=parallel vss=default vssmc=do_not_use enc=auto
roc=default abe=default ola=use rfmhdr=do_not_use acsucc=none
acfail=del,lfld,rdat,rper,wdat"

/bin/echo Executing\ the\ command\ cifscreate\(test02\)\.\.\.\.\.\.
$PRECMD sudo cifscreate -x test02 -d \/mnt\/FS01\/test02 -a "use" -p "rw" -
b "permit" -g "allow" -t "write_permitted_users" -C "default" -s
"make_public:[fdf1:afcb:44f9:1000::3:25]" -S "write_and_close" -f
```

```
"rw,rw,rw" -F "rw,rw,rw" -o "homedir=use acpol=parallel vss=default
vssmc=default enc=mandatory roc=default abe=default ola=do_not_use
rfmhdr=do_not_use acsucc=none acfail=del,lfld,rdat,rper,wdat"

exit 0
```

Notes:

> - For the variable `PRECMD`, specify the syntax of the `ssh` command
> used when executing from a remote host.
>
> Example: `ssh -2 nasroot@fshost01`
>
> - When using special characters, use the escape characters
> appropriate for the remote host environment.

Information-definition-file-name

> Specify the name of the information definition file. You can specify only
> the name of an CIFS share information definition file that is immediately
> under the home directory for the SSH account (`/home/nasroot`).

Displayed information

The following table lists the information displayed by this command when the
`--list` option is specified.

**Table 2-109 Information displayed when executing the cifsrestore
command with the --list option specified**

Item	Description
`Backup date and time`	Displays the data and time when information about the CIFS share was last backed up.
`Name of file share`	Displays the name of the CIFS share.
`Shared directory`	Displays the absolute path for the directory of the created CIFS share.

`Use ACL`	Displays whether CIFS clients are allowed to view and set ACLs.
	`use`
	　　CIFS clients are allowed to view and set ACLs.
	`not_use`
	　　CIFS clients are not allowed to view and set ACLs.

`Server specification`	If specific hosts or networks are allowed to access the CIFS share, `make_public` appears in this item, followed by the specific host names or network addresses. If specific hosts or networks are not allowed to access the CIFS share, `do_not_make_public` appears in this item, followed by the specific host names or network addresses.
`Comment for file share`	Displays a comment about the CIFS share.
`Permission mode`	Displays access permission for the CIFS share. `ro`

Item	Description
	Only read permission is granted.
	`rw`
	Read and write permissions are granted.
`Browse permission`	Displays whether viewing the CIFS share name is permitted.
	`permit`
	Viewing the CIFS share name is permitted.
	`do_not_permit`
	Viewing the CIFS share name is not permitted.
`File access permissions`	Displays the access permissions for files created in a writable CIFS share. The permissions are listed in order for the owner, owner group, and other users. The permissions are separated with commas.
	When the ACL type of the file system in which the CIFS share has been created is the Advanced ACL type, -- appears for this item.
	`ro`
	Files are read-only.
	`rw`
	Read and write permissions are granted for files.
	`none`
	No access permissions are granted for files.
`Directory access permissions`	Displays the access permissions for directories created in a writable CIFS share. The permissions are listed in order for the owner, owner group, and other users. The permissions are separated with commas.
	When the ACL type of the file system in which the CIFS share has been created is the Advanced ACL type, -- appears for this item.
	`ro`
	Directories are read-only.
	`rw`
	Read and write permissions are granted for directories.
	`none`
	No access permissions are granted for directories.
`Write disallowed users`	Displays users who do not have write permission for the CIFS share.
	If no users are prohibited from writing to the CIFS share, this item does not appear.
`Write disallowed groups`	Displays groups that do not have write permission for the CIFS share.
	Each group name is prefixed with an at mark (`@`). If no groups are prohibited from writing to the CIFS share, this item does not appear.
`Write allowed users`	Displays users who have write permission for the CIFS share.

Item	Description
	If no users are allowed to write to the CIFS share, this item does not appear.
Write allowed groups	Displays groups that have write permission for the CIFS share. Each group name is prefixed with an at mark (@). If no groups are allowed to write to the CIFS share, this item does not appear.
Guest account access	Displays whether access to the CIFS share is permitted for guest accounts. allow Access is permitted for guest accounts. disallow Access is not permitted for guest accounts. default The default settings of the CIFS service configuration definitions set in the **CIFS Service Management** page (**Setting Type**: Security) of the Access Protocol Configuration dialog box applies.
Disk synchronization policy	Displays the operation to be performed for a write request issued from a CIFS client to a CIFS share. write_and_close Data is written synchronously with a write request or a close request. close Data is written synchronously with a close request. none Data is written at regular intervals, irrespective of the timing at which a write request or a close request is issued. default The default settings of the CIFS service configuration definitions set in the **CIFS Service Management** page (**Setting Type**: Performance) of the Access Protocol Configuration dialog box applies.
CIFS client cache	Displays whether the updated data in the CIFS share file is cached on clients. use Updated data is cached on clients. do_not_use Updated data is not cached on clients. default The default settings of the CIFS service configuration definitions set in the **CIFS Service Management** page (**Setting Type**: Performance) of the Access Protocol Configuration dialog box applies.

Item	Description
File timestamp changeable	Displays users who can update the time-stamp of files in the CIFS share. When the ACL type of the file system in which the CIFS shares have been created is the Advanced ACL type, -- appears for this item. write_permitted_users All users with file write permission are allowed to update a file's time-stamp. owner_only Only the file owner is allowed to update a file's time-stamp. default The default settings of the CIFS service configuration definitions set in the **CIFS Service Management** page (**Setting Type**: Security) of the Access Protocol Configuration dialog box applies.
Home directory	Displays whether the automatic home directory creation function is enabled in the CIFS share. use The automatic home directory creation function is enabled. do_not_use The automatic home directory creation function is disabled.
CIFS access log (success)	Displays the setting information for recording log entries when a CIFS client operation successfully accesses the CIFS share. The events are represented by the following character strings. If more than one log-event is specified, they are separated with commas (,). lfld An access log entry is recorded when a client successfully displays a folder list. rdat An access log entry is recorded when a client successfully reads data. wdat An access log entry is recorded when a client successfully creates or writes to a file. cfld An access log entry is recorded when a client successfully creates a folder. del An access log entry is recorded when a client successfully deletes a file or folder. rper

Item	Description
	An access log entry is recorded when a client successfully reads the access permissions for a file or folder.
	`cper`
	An access log entry is recorded when a client successfully changes the access permissions for a file or folder.
	`cown`
	An access log entry is recorded when a client successfully changes the owner of a file or folder.
	`rename`
	An access log entry is recorded when a client successfully renames a file or folder.
	`con`
	An access log entry is recorded when a client successfully establishes or terminates a connection to the CIFS share.
	`none`
	Successful access to the CIFS share is not logged.
	`default`
	The default settings of the CIFS service configuration definitions set in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box applies.
`CIFS access log (failure)`	Displays the setting information for recording log entries when a CIFS client operation fails to access the CIFS share. The events are represented by the following character strings. If more than one log-event is specified, they are separated with commas (,).
	`lfld`
	An access log entry is recorded when a client fails to display a folder list.
	`rdat`
	An access log entry is recorded when a client fails to read data.
	`wdat`
	An access log entry is recorded when a client fails to create a file or write data.
	`cfld`
	An access log entry is recorded when a client fails to create a folder.
	`del`
	An access log entry is recorded when a client fails to delete a file or folder.
	`rper`
	An access log entry is recorded when a client fails to read the access permissions for a file or folder.
	`cper`

Item	Description
	An access log entry is recorded when a client fails to change the access permissions for a file or folder.
	`cown` An access log entry is recorded when a client fails to change the owner of a file or folder.
	`rename` An access log entry is recorded when a client fails to rename a file or folder.
	`con` An access log entry is recorded when a client fails to establish or terminate a connection to the CIFS share.
	`none` Failed access to the CIFS share is not logged.
	`default` The default settings of the CIFS service configuration definitions set in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box applies.

`Client access policy`	Displays how to process access from CIFS clients.
	
	`parallel`
	
	Access is processed in parallel.
	
	`serial`
	
	Access is processed serially.
	
	`default`
	
	The default settings of the CIFS service configuration definitions set in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box applies.

`Volume Shadow Copy Service`	`default` is displayed.
`Modified files check (VSS)`	This item is not supported.

`Read-only cache for conflicts`	Displays whether a read-only client cache is used when multiple CIFS clients simultaneously attempt to access a file.
	
	`use`
	
	A read-only client cache is used.
	
	`do_not_use`
	
	A read-only client cache is not used.
	
	`default`
	
	The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Performance`) of the Access Protocol Configuration dialog box is applied.

`Access Based Enumeration`	Displays whether access-based enumeration is used.

Item	Description

	`use`
	    Access-based enumeration is used.
	`do_not_use`
	    Access-based enumeration is not used.
	`default`
	    The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box is applied.

`Offline attribute`	Displays whether the offline attribute is used.
	`use`
	    Displayed when the offline attribute is used.
	`do_not_use`
	    Displayed when the offline attribute is not used.

`SMB encryption`	Displays whether communication with the CIFS client is encrypted when using SMB 3.0.
	`auto`
	    Displayed only when the client supports encryption.
	`mandatory`
	    Displayed when encryption is mandatory.
	`disable`
	    Displayed when encryption is disabled.
	`default`
	    The default set in the CIFS service configuration definitions in the **CIFS Service Management** page (**Setting Type**: `Security`) of the Access Protocol Configuration dialog box is applied.
	You can confirm whether SMB 3.0 is being used by checking the **CIFS Service Maintenance** page of the Access Protocol Configuration dialog box.

`Retry file modify (HDR)`	Displays whether the retry function is used to improve the status of the client that failed to create or update a file due to the temporary problem of the home directory being read-only.
	`use`
	    Displayed if the retry function is used.
	`do_not_use`
	    Displayed if the retry function is not used.

Return values

Table 2-110 Return values of the cifsrestore command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 66[#], 70, 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 98, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.
99[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

\#
   The command ended abnormally due to multiple causes.

Examples

To restore information about CIFS shares according to the following conditions:

- The file system name is FS1.
- The information definition file name is FS1_cifsshares.xml.

```
$ sudo cifsrestore FS1_cifsshares.xml
```

To create a template file of scripts for performing restoration according to the following conditions:

- The template file name is FS1_cifsrestore.sh.
- The information definition file name is FS1_cifsshares.xml.

```
$ sudo cifsrestore --template FS1_cifsrestore.sh FS1_cifsshares.xml
```

clctl (Set cluster processing values)

Synopsis

```
clctl [-s timeout-value] [-e timeout-value] [-b timeout-value]
    [-l timeout-value] [-p {normal|ignore_resource_error}]
clctl -h
```

Description

Sets timeout values related to failing over or failing back. You can set timeout values for the following operations:

- Resource group start processing

  If a timeout error occurs during the start processing on the destination node, the destination node is reset, and then the start processing on the original node begins. If the start processing on the original node terminates abnormally, the resource groups and services for users stop as well.

- Resource group stop processing

  If a timeout occurs during the stop processing on a node, the node is reset, and then the start processing on the other node begins. If the start processing on the other node terminates abnormally, the resource groups and services for users stop as well.

- Heartbeat monitoring

  If a timeout occurs during heartbeat monitoring, an error is assumed to have occurred on the other node. The other node is reset, and then the resource group begins processing on the local node.

- Link-down monitoring

  If a timeout occurs during link-down monitoring, an error is assumed to have occurred on the local node. The resource group begins processing on the other node. Note that if the resource group is excluded from being monitored, the resource group cannot be failed over.

The following conditions must be met before you can use this command:[#]

- A cluster is set up.
- The OSs on both nodes have been started and are in a state in which they can be logged into.

[#]

  Any settings changed by this command are also applied to the other node. After changing a setting, execute the clctl command (without any arguments) on both nodes to confirm that the changed settings have been applied.

Options and arguments

-b *timeout-value*

Specify the timeout value for a failover to start after a heartbeat LAN failure is detected (in seconds). Enter an integer from 15 to 600. The default value is 60.

-e *timeout-value*

Specify the stop processing timeout value (in minutes). Enter `0` (zero) or an integer from 3 to 180. If you enter `0` (zero) here, the stop processing will not time out. The default value is 60.

-l *timeout-value*

Specify the timeout value for a failover to start after a link-down failure is detected (in seconds). Enter an integer from 15 to 600. The default value is 60.

-p {normal|ignore_resource_error}

Specify the resource group start policy when a failure occurs on a resource that is part of the resource group. The default is **ignore_resource_error**.

normal

If a failure occurs on a resource that is part of a resource group, the resource group is not started. If the resource group is not started, the status of the resource group changes to `Online/srmd executable error` and either no services are provided, or the services are provided by the other node.

ignore_resource_error

Even if a failure occurs on a resource that is part of a resource group, the resource group still starts. However, if the error might affect the system or multiple services, the resource group is not started.

-s *timeout-value*

Specify the start processing timeout value (in minutes). Enter `0` (zero) or an integer from 3 to 180. If you enter `0` (zero) here, the start processing will not time out. The default value is 0.

Note that if you do not specify any options, the currently set values will be displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-111 Information displayed when executing the clctl command

Item	Description
Timeout value for the processing to start the resource group during failover	Displays the timeout value for starting a resource group during a failover (unit: minutes).
Timeout value for the processing to stop the resource group during failover	Displays the timeout value for stopping a resource group during a failover (unit: minutes).

Item	Description
`Time until a failover starts after a failure is detected on the heartbeat LAN`	Displays the timeout value for a failover to start after a heartbeat LAN failure is detected (unit: seconds).
`Time until a failover starts after a link-down error is detected`	Displays the timeout value for a failover to start after a link-down is detected (unit: seconds).

`Resource group start policy if an error occurs with a resource`	Displays the resource group start policy when a failure occurs on a resource that is part of a resource group.
	
	`normal`
	
	If a failure occurs on a resource that is part of a resource group, the resource group is not started. If the resource group is not started, the status of the resource group changes to `Online/srmd executable error` and either no services are provided, or the services are provided by the other node.
	
	`ignore_resource_error`
	
	Even if a failure occurs on a resource that is part of a resource group, the resource group still starts. However, if the error might affect the system or multiple services, the resource group is not started.

Return values

Table 2-112 Return values of the clctl command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`98`	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To change timeout values under the following conditions:

- Change the start processing timeout value to `45` minutes.
- Change the stop processing timeout value to `45` minutes.

```
$ sudo clctl -s 45 -e 45
```

clstart (Start a cluster)

Synopsis

```
clstart [-h]
```

Description

Starts the cluster that contains the node to which you are logged in.

Before executing this command, check the information in *Before starting cluster operation:* in <u>Cluster management on page 3-4</u>. This command can be executed when the cluster is in the `INACTIVE` state.

If you start the cluster with the resource group status in the `Online Ready/No error` state, the resource group also starts automatically. After the `clstart` command processing has been completed, it might take a while until resource group-related operations can be performed (the resource group status has changed to `Online/No error`).

Return values

Table 2-113 Return values of the clstart command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 25, 66, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80, 81	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

clstatus (Display cluster status)

Synopsis

```
clstatus [-c] {-v|[--] [cluster-name]}
clstatus -h
```

Description

Displays the status of the cluster that contains the node you are logged in to.

Options and arguments

`-c`

Specify this to display cluster status information separated with colons (:). When the `-c` option is specified, any colon (:) contained in the cluster, node, and resource group names is replaced with a hash mark (#).

`-v`

Specify this to view the maintenance information, such as information about the cluster management LU and the IP address of a heartbeat port.

cluster-name

Specify this option to view the status of only the cluster containing the node you are logged in to.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-114 Information displayed when executing the clstatus command

Item	Description
`--Cluster Status--`	Information about the cluster is displayed.
`Cluster name`	The name of the cluster is displayed.

`Cluster status`	The status of the cluster is displayed.[1]
	
	`ACTIVE`
	    The cluster is running normally.
	`INACTIVE`
	    The cluster is stopped.
	`UNKNOWN` [2][3]
	    The status cannot be determined.
	`DISABLE`
	    The failover function is disabled due to an error.

Item	Description
`--Node Status--`	If you do not specify a cluster name, the command displays the status of the node to which you are logged in and the status of the other node in the cluster, in that order.
node-number , *host-name*	Information about the node is displayed in the following format: `node-number(host-name)`
`Node name`	The name of the node is displayed.

`Node status`	The status of the node is displayed.[#1]
	`UP`
	    The node is running normally.
	`INACTIVE`
	    The node is stopped.
	`DOWN`
	    The node ended abnormally and has shut down.
	`UNKNOWN` [#2][#3]
	    The status cannot be determined.

`--Resource Group Status--`	If you do not specify a cluster name, the command displays the status of the resource group that belongs to the node to which you are logged in and the status of the resource group that belongs to the other node in the cluster, in that order.
`Resource group name`	The name of a resource group is displayed.
`Resource group status`	The status and error information about a resource group, displayed in the following format: `resource-group-status/error-information`

	resource-group-status	`Online Ready` [#4]
		    The resource group cannot start because the cluster is inactive, or an error was detected when the cluster was stopping.
		`Initializing`
		    The resource group is initializing.
		`Discovery (exclusivity)`
		    Online processing is being performed for the resource group, before operations begin.
		`Online Pending`
		    The resource group is starting.
		`Online`
		    The resource group is active.
		`Online Maintenance`
		    Monitoring is disabled. If a failure occurs, automatic failover will not be performed.
		`Offline Pending`
		    The resource group is stopping.

Hitachi Data Ingestor CLI Administrator's Guide

Item		Description
		`Offline` [#4] The resource group is stopped. `Internal Error` An internal error was detected. Contact the maintenance personnel.

	error-information [#5]	`No error`
		
		No errors occurred.
		
		`Internal error - not recoverable`
		
		An unrecoverable internal error occurred. Contact the maintenance personnel.
		
		`Monitor activity unknown`
		
		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.
		
		`No available nodes` or `No available nodes in failure domain after monitor failure`
		
		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 the first failover.
		
		`Node not available (exclusivity)`
		
		Failover is impossible because the `Node status` of the alternate node is not `ACTIVE`. Perform a forced stop and start the alternate node. If you cannot start the alternate node, perform a forced stop for the alternate node and fix the problem.
		
		`Node unknown`
		
		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.
		
		`Split resource group (exclusivity)`
		
		A duplicate resource group is active in the cluster. Perform a forced stop for the cluster, and

Command Reference

Item	Description
	then ask maintenance personnel to stop and restart the OS on the nodes in the cluster. `srmd executable error` An error occurred during start or stop processing. Perform a forced stop and fix the problem.
`Running node`	The name of the node on which the resource group is running is displayed.
`--Cluster Management LU Information--`	Displays information about the cluster management LU.
`Model`	Displays the model of the storage system where the cluster management LU exists.
`Serial number`	Displays the serial number of the storage system to which the cluster management LU belongs.
`LDEV number`	Displays the LDEV number of the LU assigned to the cluster management LU in decimal (base-10) format. The value in the parentheses is in hexadecimal format.
`--Heartbeat Port IP Address--`	Displays the IP addresses of the heartbeat ports on both nodes. The IP addresses of the heartbeat port of the node you are logged in to and then the IP addresses of the heartbeat port of the other node in the cluster are displayed.
node-number , *host-name*	Displays information about the node you are logged in to and about the other node. This information is displayed in the following format in that order: *node-number(host-name)*
`Heartbeat port`	Displays the IP address of the heartbeat port on the node you are logged in to and on the other node, in that order.

Note:

   If you execute the `clstatus` command immediately after executing the `clstart` command or the `ndstart` command, the command might remain in the processing status for some time.

#1:

   If an error occurs in the system, the status of clusters and nodes might not be displayed. In this case, collect the error information and contact the maintenance personnel. For details on how to collect error information, see the Troubleshooting.

#2:

   If you execute the `clstatus` command while you are logged in to a stopped node, the cluster and the other node are shown as having `UNKNOWN` status, regardless of their actual status. To check the cluster status, the status of the other node, and the resource group status, log in to the active node (the other node), and then re-execute the `clstatus` command.

#3:

> UNKNOWN is also displayed when a cluster starts up. Note that, when a cluster starts up, UNKNOWN is displayed until both OSs on the nodes making up the cluster complete startup (for up to 10 minutes).

#4:

> This information also appears when the cluster status is DISABLE.

#5:

> For details on how to correct each type of error, see the *Troubleshooting Guide*.

Return values

Table 2-115 Return values of the clstatus command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 26, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

clstop (Stop a cluster)

Synopsis

```
clstop [-f] [-y]
clstop -h
```

Description

Stops the cluster that contains the node to which you are logged in.

You can execute this command when the cluster and resource group have the following statuses:

- The cluster status is ACTIVE.

- The resource group status is `Online/No error`, `Offline/No error`, or `Online Maintenance/No error`.

Options and arguments

`-f`

Specify this option if you want to forcibly stop the cluster. If an error occurs during a cluster startup or stop operation and prevents processing from continuing, you can forcibly stop the cluster by executing this command with the `-f` option specified.

Return values

Table 2-116 Return values of the clstop command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 24, 66, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

datamigrateaccessctl (Setting the operation mode for imports)

Synopsis

```
datamigrateaccessctl [--specialmode {on|off}]
datamigrateaccessctl -h
```

Description

Sets the operation mode to import data from a file share on another file server. You can also use the command to view the current setting.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Note:
> When executing this command, make sure to follow the instructions given by the vendor or support service.

Options and arguments

`--specialmode {on|off}`

This option specifies the operation mode to import data from a file share on another file server.

`on`

Specify this option to set the operation mode as a special mode.

`off`

Specify this option to not set the operation mode as a special mode. The initial setting is `off`.

Note that if you do not specify any options, the currently set values will be displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-117 Information displayed when executing the datamigrateaccessctl command

Item	Description

Special mode	Displays the operation mode used to import data from a file share on another server.
	
	On
	
	    This is displayed if the operation mode is a special mode.
	
	Off
	
	    This is displayed if the operation mode is not a special mode.

Return values

Table 2-118 Return values of the datamigrateaccessctl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation.

Return value	Description
	If this error occurs repeatedly, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

datamigrateaccesstest (Check accessibility of import-source file servers)

Synopsis

When the import source is a CIFS share

```
datamigrateaccesstest --name import-definition-name
datamigrateaccesstest --source host\CIFS-share-name
    --user user-name --password password
```

When the import source is an NFS share

```
datamigrateaccesstest --name import-definition-name
datamigrateaccesstest --source host:NFS-shared-directory
```

To reference the command syntax

```
datamigrateaccesstest -h
```

Description

Check whether file shares are accessible on an import-source file server.

Options and arguments

`--name` *import-definition-name*

Specify the name of the import definition information. You cannot specify this option when the `--source` option is specified.

`--password` *password*

Specify the password used for connecting to the CIFS shares of the source file server.

`--source` *host\CIFS-share-name*

If the file share is a CIFS share, specify the host name or IP address of the import-source file server, and the name of the CIFS share. You cannot specify this option when the `--name` option is specified.

`--source` *host:NFS-shared-directory*

If the file share is an NFS share, specify the host name or IP address of the import-source file server, and the absolute path of the shared directory. You cannot specify this option when the `--name` option is specified.

`--user` *user-name*

Specify the user name used for connecting to CIFS shares on the source file server.

If the HDI system is in a different domain from the user or belongs to multiple domains, specify the domain name and user name in the following format:

```
domain-name \ user-name
```

Return values

Table 2-119 Return values of the datamigrateaccesstest command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70, 72[#], 73	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
69	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
72[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Example

To specify an import definition name and check whether a CIFS share is accessible on the import-source file server:

```
$ sudo datamigrateaccesstest --name importfiles
KAQM37179-I A connection was established to the migration-source file
server.
```

datamigrateconfadd (Add data import definition information)

Synopsis

When the import source is a CIFS share

```
datamigrateconfadd [--mapdef mapping-file-name] [-y]
    --name import-definition-name --source host\CIFS-share-name
    --destination import-target-directory --user user-name
    --password password
    [--account-map-mode {auto|domain|local}]
    [--replaceowner alternate-owner-name|
     --replacegroup alternate-group-name]
```

When the import source is an NFS share

```
datamigrateconfadd [-y] --name import-definition-name
    --source host:NFS-shared-directory
    --destination import-target-directory
```

To reference the command syntax

```
datamigrateconfadd -h
```

Description

Adds the definition information (import definition information) needed to import data from a file share on another file server, or registers local account mapping information.

This command can be executed when the following conditions are satisfied:

- The configuration definition for the CIFS or NFS service has been applied to both nodes, according to the type of file share being imported.
- Another file server is accessible by using the `datamigrateaccesstest` command.
- The share name to be specified as the import source is not set in the data import definition information.
- The import-target file system is not sharing the data with another HDI system via linked HCP systems.
- The directory path to be specified as the import target is not set in the data import definition information.
- The import-target directory is on the node to which you have logged in.

Note that the maximum number of data import definition information entries that can be added by using this command is 20 per cluster.

Options and arguments

`--account-map-mode {auto|domain|local}`

    Specify the mode to use for name resolution of the owner name and ACE account information of files and directories at the import source.

    `auto`

Specify this option to select the name resolution mode automatically.

domain

Specify this option to perform name resolution using the user mapping of the CIFS service.

local

Specify this option to perform name resolution using a mapping file. If this option is omitted, `auto` will be set.

--destination *import-target-directory*

Specify the absolute path beginning with `/mnt/` of a directory in the HDI system.

--mapdef *mapping-file-name*

Specify this option to register local account mapping information. Before registering a mapping file, you must transfer the mapping file to the SSH account home directory (`/home/nasroot`). If you do not specify this option, the command registers no mapping information.

--name *import-definition-name*

Specify the name of the import definition information. You can specify a maximum of 1,280 bytes.

You can use alphanumeric characters, symbols, and multi-byte Unicode (UTF-8) characters.

--password *password*

Specify the password used to connect to the file shares on the import-source file server.

--replacegroup *alternate-group-name*

If the group name of the owner of the data to be imported cannot be resolved, specify a group name that can be assigned as an alternate account. Note that you cannot use any of the following characters in the group name: double quotation marks (`"`), asterisks (`*`), plus signs (`+`), commas (`,`), colons (`:`), semicolons (`;`), left angle brackets (`<`), equal signs (`=`), right angle brackets (`>`), question marks (`?`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), or vertical bars (`|`). Furthermore, you cannot specify a group name consisting of more than 20 characters.

This option can be omitted. Note that the `--replacegroup` option cannot be specified with the `--replaceowner` option.

--replaceowner *alternate-owner-name*

If the user name of the owner of the data to be imported cannot be resolved, specify a user name that can be assigned as an alternate account. Note that you cannot use any of the following characters in the user name: double quotation marks (`"`), asterisks (`*`), plus signs (`+`), commas (`,`), colons (`:`), semicolons (`;`), left angle brackets (`<`), equal signs (`=`), right angle brackets (`>`), question marks (`?`), at marks (`@`), left

square brackets (`[`), right square brackets (`]`), or vertical bars (`|`). Furthermore, you cannot specify a user name consisting of more than 20 characters.

This option can be omitted. Note that the `--replaceowner` option cannot be specified with the `--replacegroup` option.

`--source` *host**CIFS-share-name*

If the import-source file share is a CIFS share, specify the host name or IP address of the import-source file server and the name of the CIFS share. If you specify different host name or IP address values, the command will treat them as different hosts even if they resolve to the same host. If you execute this command more than once for a given host, specify the host information in the same way each time.

`--source` *host*:*NFS-shared-directory*

If the import-source file share is an NFS share, specify the host name or IP address of the import-source file server and the absolute path of the shared directory. If you specify different host name or IP address values, the command will treat them as different hosts even if they resolve to the same host. When executing this command more than once for a given host, specify the host information in the same way each time.

`--user` *user-name*

Specify the user name used to connect to the file shares on the import-source file server.

Note that if the HDI system does not participate in the domain to which the user belongs, or if the HDI system participates in multiple domains, use the following format to specify the domain name and user name:

domain-name \ *user-name*

Note that you cannot use any of the following characters in the user name: double quotation marks (`"`), asterisks (`*`), plus signs (`+`), commas (`,`), colons (`:`), semicolons (`;`), left angle brackets (`<`), equal signs (`=`), right angle brackets (`>`), question marks (`?`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), or vertical bars (`|`). Furthermore, you cannot specify a user name consisting of more than 20 characters.

Return values

Table 2-120 Return values of the datamigrateconfadd command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 4, 5, 7, 8, 10, 12, 15, 16, 17, 18, 19, 22, 32, 70, 71[#], 72[#], 73	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output

Return value	Description
	message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66, 67, 69	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71#, 72#, 80	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
    The command ended abnormally due to multiple causes.

Examples

To add data import definition information from other CIFS shares in the file server, and to register the local account mapping information:

```
$ sudo datamigrateconfadd --name definition_name --source "host\share" --
destination /mnt/fs01/share --user USER01 --password PASS01 --account-map-
mode auto --replaceowner OWNER01
```

To add data import definition information when importing data from NFS shares in other file servers:

```
$ sudo datamigrateconfadd --name definition_name --source "host:/nfs/
share" --destination /mnt/fs01/share
```

datamigrateconfdel (Delete data import definition information)

Synopsis

When the import source is a CIFS share
```
datamigrateconfdel [-f] --source host\CIFS-share-name
datamigrateconfdel [-f] --name import-definition-name
```

When the import source is an NFS share
```
datamigrateconfdel [-f] --source host:NFS-shared-directory
datamigrateconfdel [-f] --name import-definition-name
```

To reference the command syntax
```
datamigrateconfdel -h
```

Description

Deletes the data import definition information and local account mapping information.

Options and arguments

`-f`

Specify this option to forcibly delete the data import definition information and local account mapping information. Note that if this option is specified, import processing is interrupted, and then forcibly stopped.

`--name` *import-definition-name*

Specify the import definition name. You cannot specify this option when the `--source` option is specified.

`--source` *host**CIFS-share-name*

If the import-source file share is a CIFS share, specify the host name or IP address of the import-source file server, and the name of the CIFS share. If you specify a different host name or IP address from the one specified in the `datamigrateconfadd` command, they will be treated as different hosts even if they resolve to the same host. You cannot specify this option when the `--name` option is specified.

`--source` *host*:*NFS-shared-directory*

If the import-source file share is an NFS share, specify the host name or IP address of the import-source file server and the absolute path of the shared directory. If you specify a different host name or IP address from the one specified in the `datamigrateconfadd` command, they will be treated as different hosts even if they resolve to the same host. You cannot specify this option when the `--name` option is specified.

Return values

Table 2-121 Return values of the datamigrateconfdel command

Return value	Description
0	Normal termination
1, 15	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 23#, 41, 68#, 70, 71#	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
23#, 65, 66, 67, 68#, 69	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
71#	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71#, 97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Example

To delete data import definition information:

```
$ sudo datamigrateconfdel --name importfiles
```

datamigrateconfedit (Set data import definition information)

Synopsis

```
datamigrateconfedit [--mapdel|--mapdef mapping-file-name]
    [--user user-name] [--password password]
    [--account-map-mode {auto|domain|local}]
    [--replaceowner alternate-owner-name]
    [--replacegroup alternate-group-name]
    {--name import-definition-name|--source host\CIFS-share-name}
datamigrateconfedit -h
```

Description

Re-registers or deletes local account mapping information.

You can execute this command when the import source is a CIFS share.

Options and arguments

```
--account-map-mode {auto|domain|local}
```
Specify the mode to use for name resolution of the owner name and ACE account information of files and directories at the import source.

```
auto
```
Specify this option to select the name resolution mode automatically.

```
domain
```
Specify this option to perform name resolution using the user mapping of the CIFS service.

```
local
```

Specify this option to perform name resolution using a mapping file. If you omit this option, the current setting value remains in effect.

`--mapdef` *mapping-file-name*

Specify this option to re-register the local account mapping information.

`--mapdel`

Specify this option to delete the local account mapping information. If no mapping information is registered, do not specify this option.

`--name` *import-definition-name*

Specify the name of the import definition information. You cannot specify this option if the `--source` option is specified.

`--password` *password*

Specify the password used to connect to the file shares of the import-source file server.

If you omit this option, the current setting applies.

`--replacegroup` *alternate-group-name*

If the group name of the owner of the data to be imported cannot be resolved, specify a group name that can be assigned as an alternate account. Note that you cannot use any of the following characters in the group name: double quotation marks (`"`), asterisks (`*`), plus signs (`+`), commas (`,`), colons (`:`), semicolons (`;`), left angle brackets (`<`), equal signs (`=`), right angle brackets (`>`), question marks (`?`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), or vertical bars (`|`). Furthermore, you cannot specify a group name consisting of more than 20 characters. You can omit this option.

If you intend to change the alternate account specification from a group name to a user name, specify an empty character string (e.g., "" or '') in this option to delete the existing group name.

`--replaceowner` *alternate-owner-name*

If the user name of the owner of the data to be imported cannot be resolved, specify a user name that can be assigned as an alternate account. Note that you cannot use any of the following characters in the user name: double quotation marks (`"`), asterisks (`*`), plus signs (`+`), commas (`,`), colons (`:`), semicolons (`;`), left angle brackets (`<`), equal signs (`=`), right angle brackets (`>`), question marks (`?`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), or vertical bars (`|`). Furthermore, you cannot specify a user name consisting of more than 20 characters. You can omit this option.

If you intend to change the alternate account specification from a user name to a group name, specify an empty character string (e.g., "" or '') in this option to delete the existing user name.

`--source` *host\CIFS-share-name*

If the import source is a CIFS share, specify the host name or IP address of the import-source file server and the name of the CIFS share. If you

specify a different host name or IP address from the one specified in the
`datamigrateconfadd` command, it will be treated as a different host even
if the IP address or host name resolves to the same host. You cannot
specify this option if the `--name` option is specified.

`--user` *user-name*

Specify the user name used to connect to the file shares at the import-
source file server.

If the HDI system is in a different domain from the user or the HDI
system belongs to multiple domains, specify the domain name and user
name in the following format:

   domain-name \ *user-name*

Note that you cannot use any of the following characters in the user
name: double quotation marks (`"`), asterisks (`*`), plus signs (`+`), commas
(`,`), colons (`:`), semicolons (`;`), left angle brackets (`<`), equal signs (`=`),
right angle brackets (`>`), question marks (`?`), at marks (`@`), left square
brackets (`[`), right square brackets (`]`), or vertical bars (`|`). Furthermore,
you cannot specify a user name consisting of more than 20 characters.

Note:

Be sure to specify at least one optional option.

Return values

Table 2-122 Return values of the datamigrateconfedit command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 4, 5, 6, 7, 8, 15, 32, 41, 70, 71, 73, 78	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 67, 69	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To specify an import definition name and re-register the local account mapping information:

```
$ sudo datamigrateconfedit --mapdef mappingfile --account-map-mode local --
replaceowner user02 --name importfiles
```

datamigrateconflist (Display data import definition information)

Synopsis

When the import source is a CIFS share

```
datamigrateconflist [--source host\CIFS-share-name]
datamigrateconflist [--name import-definition-name]
datamigrateconflist --mapdef --source host\CIFS-share-name
datamigrateconflist --mapdef --name import-definition-name
```

When the import source is an NFS share

```
datamigrateconflist [--source host:NFS-shared-directory]
datamigrateconflist [--name import-definition-name]
```

To reference the command syntax

```
datamigrateconflist -h
```

Description

Display data import definition information for CIFS shares on other file servers. Note that if you omit all the options, all the data import definition information is displayed.

Options and arguments

`--mapdef`

Specify this option to display local account mapping information. If no mapping information is registered, do not specify this option.

`--name` *import-definition-name*

Specify the import definition name. You cannot specify this option when the `--source` option is specified.

`--source` *host\CIFS-share-name*

If the import source is a CIFS share, specify the host name or IP address of the import-source file server and the name of the CIFS share. If you specify a different host name or IP address from the one specified in the `datamigrateconfadd` command, it will be treated as a different host even if the IP address or host name resolves to the same host. You cannot specify this option if the `--name` option is specified.

`--source` *host*:*NFS-shared-directory*

> If the import source is an NFS share, specify the host name or IP address of the import-source file server and the absolute path of the shared directory. If you specify a different host name or IP address from the one specified in the `datamigrateconfadd` command, it will be treated as a different host even if the IP address or host name resolves to the same host. You cannot specify this option if the `--name` option is specified.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-123 Information displayed when executing the datamigrateconflist command (the --mapdef option is not specified)

Item		Description
`CIFS import definition number (number)`		Displays information about each CIFS share.
-	`Import-definition name`	Displays the name of the import definition information.
-	`Import-source host name`	Displays the CIFS share name of the import-source file server.
-	`Import-source share name`	Displays the name of the CIFS share on the import-source file server.
-	`User name`	Displays the user name of the import-source file server.
-	`Import-destination directory`	Displays the absolute path of the CIFS share in the HDI system.
-	`Account mapping mode`	Displays the mode to use for name resolution of the owner name and ACE account information of files and directories at the import source.
-	`Import-replace owner`	Displays the user name assigned as the alternate account.
-	`Import-replace group`	Displays the group name assigned as the alternate account.

-	`File share import status`	Displays the status of the import or verification process.
		
		`success`
		
		    All data has been imported.
		
		`all`
		
		    Data is currently being imported.
		
		`all(temporary on-demand)`
		
		    The data import process has been suspended because data is being migrated to the HCP system, or the amount of disk space available on the target file system has fallen below a threshold. In this state, the HDI system will only import data requested by clients.

Item		Description

		on-demand
		
		    The HDI system is only importing data requested by clients.
		
		not execute
		
		    The import or verification process has not started yet.
		
		failed
		
		    Full data import has failed.
		
		unable
		
		    The import or verification process could not be performed.
		
		retry
		
		    The process of importing all data needs to be performed again.
		
		stop
		
		    The import process has stopped.
		
		scan
		
		    The import definition information is being verified.
		
		scan complete
		
		    Verification of the import definition information has finished.

-	Account mapping	Displays whether local account mapping is used.
		
		Use
		
		    Mapping is used.
		
		Do not use
		
		    Mapping is not used.

-	Mapping file name	Displays the name of the mapping file.
NFS import definition number (number)		Displays information about each NFS share.
-	Import-definition name	Displays the name of the import definition information.
-	Import-source host name	Displays the host name or IP address of the import-source file server.
-	Import-source share path	Displays the shared directory on the import-source file server by absolute path.
-	Import-destination directory	Displays the absolute path of the shared directory on the HDI system.

-	File share import status	Displays the status of the import or verification process.
		
		success
		
		    All data has been imported.
		
		all
		
		    Data is currently being imported.
		
		all(temporary on-demand)

Item	Description

	The data import process has been suspended because data is being migrated to the HCP system, or the amount of disk space available on the target file system has fallen below a threshold. In this state, the HDI system will only import data requested by clients.
	
	`on-demand`
	
	    The HDI system is only importing data requested by clients.
	
	`not execute`
	
	    The import or verification process has not started yet.
	
	`failed`
	
	    The full data import process has failed.
	
	`unable`
	
	    The import or verification process could not be performed.
	
	`retry`
	
	    The full data import process needs to be performed again.
	
	`stop`
	
	    The import process has stopped.
	
	`scan`
	
	    The import definition information is being verified.
	
	`scan complete`
	
	    Verification of the import definition information has finished.

The following table describes the information displayed by this command when the `--mapdef` option is specified.

Table 2-124 Information displayed by the datamigrateconflist command (when the --mapdef option is specified)

Item	Description
`SID`	The SID of the account is displayed.
`SRC_NAME`	The user name or group name of the current account (before migration) is displayed.

`KIND`	Displays the account type.
	
	`u`
	
	    The account is a user.
	
	`g`
	
	    The account is a group.

`DST_NAME`	The user name or group name of the new account (after an import) is displayed.

Return values

Table 2-125 Return values of the datamigrateconflist command

Return value	Description
0	Normal termination
1, 15	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
6, 10, 25, 26, 27, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 69	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To specify the import definition name and to view data import definition information:

```
$ sudo datamigrateconflist --name importfiles
List of CIFS Import Definitions
CIFS import definition number (1)
 Import-definition name : importfiles
 Import-source host name : 192.168.100.10
 Import-source share name : share01
 User name : user01
 Import-destination directory : /mnt/importfiles01
 Account mapping mode : auto
 Import-replace owner : --
 Import-replace group : --
 File share import status : not execute
 Account mapping : Do not use
 Mapping file name :
```

datamigratectl (Change how to import data)

Synopsis

When the import source is a CIFS share
```
datamigratectl [-y] --type {all|on-demand|cancel}
    --name import-definition-name
datamigratectl [-y] --type {all|on-demand|cancel}
    --source host\CIFS-share-name
```

When the import source is an NFS share

```
datamigratectl [-y] --type {all|on-demand|cancel}
    --name import-definition-name
datamigratectl [-y] --type {all|on-demand|cancel}
    --source host:NFS-shared-directory
```

To reference the command syntax
```
datamigratectl -h
```

Description

Change the method for importing data from file shares on another file server to an HDI system. You can also use this command to stop the import process.

This command can be executed when the following conditions are satisfied:

- The configuration definition for the CIFS or NFS service has been applied to both nodes on which the command is being executed according to the type of file share from which data is being imported.
- The import-source file server is accessible by using the `datamigrateaccesstest` command.
- There is 8 MB or more of unused capacity in a file system in the HDI system.
- The import-target file share is on the node to which you have logged in.

Options and arguments

`--name` *import-definition-name*

Specify the name of the import definition information. You cannot specify this option if the `--source` option is specified.

`--source` *host\CIFS-share-name*

If the import-source file share is a CIFS share, specify the host name or IP address of the import-source file server, and the name of the CIFS share. If you specify a different host name or IP address from the one specified in the `datamigrateconfadd` command, it will be treated as a different host even if the IP address or host name resolves to the same host. You cannot specify this option when the `--name` option is specified.

`--source` *host:NFS-shared-directory*

If the import-source file share is an NFS share, specify the host name or IP address of the import-source file server and the absolute path of the shared directory. If you specify a different host name or IP address from the one specified in the `datamigrateconfadd` command, it will be treated as a different host even if the IP address or host name resolves to the same host. You cannot specify this option when the `--name` option is specified.

`--type {all|on-demand|cancel}`

Specify how to import data from another file server to the HDI system.

`all`

Specify this to import all data to the HDI system.

on-demand

> Specify this parameter to only import data requested by clients from the import-target HDI system.

cancel

> Specify this parameter to stop the import process. You can resume the import process by executing this command again.

Return values

Table 2-126 Return values of the datamigratectl command

Return value	Description
0	Normal termination
1, 2	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 11, 14[#], 17, 24, 25, 26, 28, 32, 41, 68[#], 70, 71[#], 72[#], 73	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
14[#], 65, 66, 67, 68[#], 69	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71[#], 72[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71[#], 97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Example

To change the import method so that the import definition name is specified and only the data accessed by a client in the HDI system of the import destination is imported:

```
$ sudo datamigratectl --type on-demand --source "host\share"
KAQM37174-Q An all-data migration is being performed in accordance to data
migration definition information. Do you want to stop the migration? (y/n)
```

datamigratelimitget (Display the threshold at which data importation is suspended or resumed)

Synopsis

```
datamigratelimitget --file-system file-system-name
datamigratelimitget -h
```

Description

Displays the threshold (available disk space) at which the full import process is suspended and the import-target HDI system only imports data requested by clients. If the full import process is already suspended, this command displays the threshold (available disk space) at which the process is resumed.

This command can be executed when the following conditions are met:

- User mapping is set in the configuration definition for the CIFS service on both nodes.
- The import-source file server is accessible by using the `datamigrateaccesstest` command.
- The share name to be specified as the import source is not set in the data import definition information.
- The directory path to be specified as the import target is not set in the data import definition information.
- The import-target directory is on the node to which you have logged in.

Options and arguments

`--file-system` *file-system-name*
    Specify the name of the import-target file system.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-127 Information displayed when executing the datamigratelimitget command

Item	Description
Suspend limit rest size	Displays the threshold (available disk space) at which the full data import process is suspended, as a percentage.
Resume limit rest size	Displays the threshold (available disk space) at which the full data import process is resumed, as a percentage.

Table 2-128 Return values of the datamigratelimitget command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 4, 15, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

datamigratelimitset (Set the threshold at which a data import is suspended or resumed)

Synopsis

```
datamigratelimitset --file-system file-system-name
    {[--suspend-rest-size remaining-capacity-until-suspend-threshold]
     [--resume-rest-size remaining-capacity-until-resume-threshold]}
datamigratelimitset -h
```

Description

Sets the threshold (available disk space) at which the full import process is suspended and the import-target HDI system only imports data accessed by clients. This command also sets the threshold (available disk space) at which the full import process is resumed.

When the amount of available disk space in the file system falls below a certain threshold, the full data import process is suspended. The process resumes when the available disk space rises above the threshold. If linkage with HCP is established and the import processing is interrupted, stub processing is performed on the files after the migration finishes until the remaining capacity of the file system reaches or exceeds the threshold, and then the import processing of all the data is resumed.

If you use this command to change the threshold while data is being imported, the change will not take effect until you suspend or resume the import process.

This command can be executed when the following conditions are met:

- User mapping is set in the configuration definition for the CIFS service on both nodes.

- The import-source file server is accessible by using the `datamigrateaccesstest` command.
- The share name to be specified as the import source is not set in the data import definition information.
- The directory path to be specified as the import target is not set in the data import definition information.
- The import-target directory is on the node to which you have logged in.
- A migration task is set.

Options and arguments

`--file-system` *file-system-name*

Specify the name of the import-target file system.

`--resume-rest-size` *remaining-amount-for-resume-threshold*

Specify the percentage of available file system capacity at which the full import process is resumed, within a range from 1 to 99. The default is 20.

`--suspend-rest-size` *remaining-amount-for-suspend-threshold*

Specify the percentage of available file system capacity at which the full import process is suspended, within a range from 1 to 99. The default is 10.

Return value

Table 2-129 Return values of the datamigratelimitset command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 4, 15, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Hitachi Data Ingestor CLI Administrator's Guide

Example

To set the thresholds for the `FS_1` file system according to the following conditions:

- ○ Set 10% as the threshold at which the full data import process is suspended.
- ○ Set 20% as the threshold at which the full data import process is resumed.

```
$ sudo datamigratelimitset --file-system fs1 --suspend-rest-size 10 --resume-rest-size 20
```

datamigratestart (Start a data import)

Synopsis

When the import source is a CIFS share

```
datamigratestart [-y] [--type {all|on-demand}]
    --name import-definition-name
datamigratestart [-y] [--type {all|on-demand}]
    --source host\CIFS-share-name
```

When the import source is an NFS share

```
datamigratestart [-y] [--type {all|on-demand}]
    --name import-definition-name
datamigratestart [-y] [--type {all|on-demand}]
    --source host:NFS-shared-directory
```

To reference the command syntax

```
datamigratestart -h
```

Description

Starts importing data to an HDI system from a file share on another file server, based on import definition information added by the `datamigrateconfadd` command.

If the available disk space on the import-target file system falls below a set threshold, the HDI system will only import data requested by clients.

This command can be executed when the following conditions are satisfied:

- The configuration definition for the CIFS or NFS service has been applied to both nodes on which the command is being executed.
- The CIFS service configuration definition is set on both nodes.
- The import-source file server is accessible by using the `datamigrateaccesstest` command.
- The import-target file share is on the node to which you have logged in.

Options and arguments

`--name` *import-definition-name*

>Specify the name of the import definition information. You cannot specify this option if the `--source` option is specified.

`--source` *host\CIFS-share-name*

>If the import source is a CIFS share, specify the host name or IP address of the import-source file server and the name of the CIFS share. If you specify a different host name or IP address from the one specified in the `datamigrateconfadd` command, it will be treated as a different host even if the IP address or host name resolves to the same host. You cannot specify this option if the `--name` option is specified.

`--source` *host:NFS-shared-directory*

>If the import source is an NFS share, specify the host name or IP address of the import-source file server and the absolute path of the shared directory. If you specify a different host name or IP address from the one specified in the `datamigrateconfadd` command, it will be treated as a different host even if the IP address or host name resolves to the same host. You cannot specify this option if the `--name` option is specified.

`--type {all|on-demand}`

>Specify how to import data from another file server to the HDI system. If you omit this option, `all` is set.

>`all`

>>Specify this parameter to import all data to the HDI system.

>`on-demand`

>>Specify this parameter to have the HDI system only import data requested by clients.

Return values

Table 2-130 Return values of the datamigratestart command

Return value	Description
`0`	Normal termination
`1, 2`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10, 11, 14`[#]`, 17, 25, 26, 29, 30, 31, 32, 41, 68`[#]`, 69`[#]`, 70, 71`[#]`, 72`[#]`, 73`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`14`[#]`, 65, 66, 67, 68`[#]`, 69`[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation.

Return value	Description
	If this error occurs repeatedly, contact maintenance personnel.
71#, 72#, 74	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Example

To specify the import definition name and to start data import from file shares on another file server to the HDI system:

```
$ sudo datamigratestart --name importfiles
```

datamigratestatus (Display the results of the import process)

Synopsis

When the import source is a CIFS share
```
datamigratestatus --name import-definition-name
    [--incompletionlist|--srcfailedlist|--migfailedlist]
datamigratestatus --source host\CIFS-share-name
    [--incompletionlist|--srcfailedlist|--migfailedlist]
```

When the import source is an NFS share
```
datamigratestatus --name import-definition-name
    [--incompletionlist|--srcfailedlist|--migfailedlist]
datamigratestatus --source host:NFS-shared-directory
    [--incompletionlist|--srcfailedlist|--migfailedlist]
```

To reference the command syntax
```
datamigratestatus -h
```

Description

Display the results of importing all data from another file server to an HDI system, or the results of verifying import definition information.

Options and arguments

```
--incompletionlist
```

Specify this option to display a list of files that were not imported in their entirety. You can use this option only after the HDI system has finished importing all data from the other file server.

`--migfailedlist`

Specify this option to display a list of files that could not be imported.

`--name` *import-definition-name*

Specify the name of the import definition information. You cannot specify this option if the `--source` option is specified.

`--source` *host\CIFS-share-name*

If the import source is a CIFS share, specify the host name or IP address of the import-source file server and the name of the CIFS share. If you specify a different host name or IP address from the one specified in the `datamigrateconfadd` command, they will be treated as different hosts even if they resolve to the same host. You cannot specify this option if the `--name` option is specified.

`--source` *host:NFS-shared-directory*

If the import source is an NFS share, specify the host name or IP address of the import-source file server and the absolute path of the shared directory. If you specify a different host name or IP address from the one specified in the `datamigrateconfadd` command, they will be treated as different hosts even if they resolve to the same host. You cannot specify this option if the `--name` option is specified.

`--srcfailedlist`

Specify this option to display a list of files that were not recognized as import targets.

Displayed information

When you execute the `datamigratestatus` command, messages reporting the status of the import process are displayed together with the following information:

Table 2-131 Information displayed by the datamigratestatus command when importation is in progress or suspended

Item	Description
Number of files in the import source	Displays the number of files or directories to be imported.
Number of files that failed to be read	The number of files or directories that were not recognized as import targets.
Number of successfully imported files	Displays the number of files or directories that were successfully imported, and the number of files or directories that were deleted during the import process.

Item	Description
`Number of files that failed to be imported`	Displays the number of files or directories that could not be imported. If you suspended and then resumed the import process, this field shows the number of files or directories that failed to be imported since the process was resumed.
`Number of files pending import`	Displays the number of files or directories that have not been fully imported. A hyphen (-) is displayed if the number is still being calculated, or if the system failed to calculate the number.

Note:

This information is not displayed if the HDI system is only importing data requested by clients.

Table 2-132 Information displayed by the datamigratestatus command after importation has ended normally or terminated abnormally

Item	Description
`Number of files in the import source`	Displays the number of files or directories that were import targets.
`Number of files that failed to be read`	Displays the number of files or directories that were not recognized as import targets.
`Total number of successfully imported files`	Displays the number of files or directories that were successfully imported, and the number of files or directories that were deleted during the import process.
`Number of files that failed to be imported`	Displays the number of files or directories that could not be imported.
`Number of files pending import`	Displays the number of files or directories that have not been fully imported. A hyphen (-) is displayed if the number is still being calculated, or if the system failed to calculate the number.

Note:

This information is not displayed if the HDI system is only importing data requested by clients.

Table 2-133 Information displayed by the datamigratestatus command while verifying import definition information

Item	Description
`Number of files in the import source`	Displays the number of files or directories to be verified according to the import definition information.
`Number of files that failed to be read`	Displays the number of files or directories referenced in the import definition information that were not recognized as targets for verification.
`Number of successfully scan files`	Displays the number of files or directories referenced in the import definition information that have been

Item	Description
	successfully verified. If you suspended and then resumed the verification process, this field shows the number of files or directories that have been verified since the process was resumed.
`Number of files that failed to be scan`	Displays the number of files or directories that cannot be imported because they failed the verification process. If you suspended and then resumed the verification process, this field shows the number of files or directories that failed verification since the process was resumed.
`Number of files pending scan`	Displays the number of files or directories referenced in the import definition information that have not yet been verified. A hyphen (-) is displayed if the number is still being calculated, or if the system failed to calculate the number.

Table 2-134 Information displayed by the datamigratestatus command after import definition information has been verified

Item	Description
`Number of files in the import source`	Displays the number of files or directories to be verified in the import definition information.
`Number of files that failed to be read`	Displays the number of files or directories referenced in the import definition information that were not recognized as targets for verification.
`Total number of successfully scan files`	Displays the number of files or directories referenced in the import definition information that were successfully verified.
`Total number of files that failed to be scan`	Displays the number of files or directories that cannot be imported because they failed the verification process.
	As a result of verifying the import definition information, the number of files and directories that could not be correctly imported is displayed.
	If error or warning messages are displayed for files when you run this command by specifying the `--migfailedlist` option, you need to resolve those problems. Files for which an error message is displayed cannot be imported. Files for which a warning message is displayed can be imported data, but some ACEs will not be imported.
`Number of files pending scan`	The number of files or directories referenced in the import definition information that are yet to be verified. A hyphen (-) is displayed if the number is still being calculated, or if the system failed to calculate the number.

Return values

Table 2-135 Return values of the datamigratestatus command

Return value	Description
0	Normal termination
1, 15	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 25, 26, 27, 68[#], 70, 71[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66, 67, 68[#], 69	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Examples

To specify an import definition name and display the result of import processing that ended successfully:

```
$ sudo datamigratestatus --name importfiles
Number of files in the import source : 143556
Number of files that failed to be read : 0
Total number of successfully imported files : 143556
Total number of files that failed to be imported : 0
Number of files pending import : 0
KAQM37147-I An all-data migration was successfully performed.
```

To specify an import definition name and display the files that were not completely imported:

```
$ sudo datamigratestatus --name importfiles --incompletionlist
KAQM37249-I Processing might take a while.
file03
file04
```

datamigratetest (Verify import definition information)

Synopsis

When the import source is a CIFS share

```
datamigratetest [--cancel] --name import-definition-name
datamigratetest [-v] --name import-definition-name
    --path import-source-file-or-directory
```

When the import source is an NFS share

```
datamigratetest [--cancel] --name import-definition-name
```

To reference the command syntax

```
datamigratetest -h
```

Description

Verifies import definition information to determine whether the target data can be imported. This command can also test specific files or directories in a CIFS share.

This command can be executed when the following conditions are satisfied:

- The configuration definition for the CIFS or NFS service has been applied to both nodes , according to the type of file share from which data is being imported.
- The import-source file server is accessible by the `datamigrateaccesstest` command.
- The import-target directory is on a node to which you have logged in.

Options and arguments

`--cancel`

Stops the process of verifying import definition information. To resume the verification process, execute this command without the `--cancel` option. In this case, files and directories that were verified the previous time are also verified.

`--name` *import-definition-name*

Specify the name of the import definition information.

`--path` *import-source-file-or-directory*

Specify the path of the CIFS share file or directory.

`-v`

Specify this option to display detailed information about the file or directory being verified. This option must be specified with the `--path` option.

Displayed information and settings

The following table lists the information displayed when the `-v` option is specified.

Table 2-136 Information displayed when the datamigratetest command is executed with the -v option

Item	Description

Data migration	Displays whether the specified file or directory can be imported.
	`Possible`
	    The file or directory can be imported.
	`Impossible`
	    The file or directory cannot be imported.

Size	Displays the size of the file or directory (in bytes).

Owner	Displays the account information for the owner of the file or directory, in the following format:
	SID(*user-ID*)
	For certain account types, the following information might appear instead of the user ID:
	`-`
	    Displayed when the system could not obtain the user ID.
	`*`
	    Displayed for universal well-known SIDs.
	`M`
	    Displayed when the account information is registered in a mapping file.

Group	Displays the account information for the owner group of the file or directory, in the following format:
	SID(*group-ID*)
	For certain account types, the following information might appear instead of the group ID:
	`-`
	    Displayed when the system could not obtain the group ID.
	`*`
	    Displayed for universal well-known SIDs.
	`M`
	    Displayed when the account information is registered in a mapping file.

Access time	Displays the date and time when the import-source file or directory was last accessed.
Modify time	Displays the date and time when the import-source file or directory was last modified.
Create time	Displays the data and time when the import-source file or directory was created.
DOS attribute	Displays the attributes (DOS attributes) of the import-source file or directory, separated by forward slashes (`/`).

Item	Description

	`R`
	
	    The file or directory is read-only.
	
	`A`
	
	    The file or directory is archived.
	
	`S`
	
	    The file is a system file.
	
	`H`
	
	    The file is hidden.
	
	`D`
	
	    The import-source is a directory.

`ACL` or `Skipped ACL`	The `ACL` entry displays information about ACEs that can be imported. The `Skipped ACL` entry displays ACEs that cannot be imported. ACEs are displayed in the following format:
	
	SID(*user-ID-or-group-ID*):*account-type*:*ACE-type*:*access-permissions*
	
	For certain account types, the following information might appear instead of the user ID and group ID:
	
	`-`
	
	    Displayed when the system could not obtain the user ID or group ID.
	
	`*`
	
	    Displayed for universal well-known SIDs.
	
	`M`
	
	    Displayed when the account information is registered in a mapping file.
	
	The account type is represented by one of the following flags:
	
	`u`
	
	    Indicates a user ACE.
	
	`g`
	
	    Indicates a group ACE.
	
	The ACE type is one of the following:
	
	`ALLOW`
	
	    Indicates an allow ACE.
	
	`DENY`
	
	    Indicates a deny ACE.
	
	Access permissions are displayed as follows. Multiple access permissions are separated by two colons (`::`).
	
	`f`
	
	    Full Control
	
	`s`
	
	    Traverse Folder/Execute File
	
	`r`
	
	    List Folder/Read Data
	
	`a`

Item	Description
	Read Attributes
e	
	Read Extended Attributes
w	
	Create Files/Write Data
p	
	Create Folders/Append Data
t	
	Write Attributes
x	
	Write Extended Attributes
l	
	Delete Subfolders and Files
d	
	Delete
c	
	Read Permissions
h	
	Change Permissions
g	
	Take Ownership

Return values

Table 2-137 Return values of the datamigratetest command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review the command format and execute it again.
10, 14[#], 17, 25, 26, 32, 41, 42, 69[#], 70, 71, 72, 75[#], 81	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
14[#], 66, 67, 69[#]	The system might be busy or a temporary error might have occurred. Wait a while and then execute the command again. If the error still occurs, contact maintenance personnel.
74, 75[#], 82	The system might be experiencing temporary communication problems. Check the communication status, wait a while, and then execute the command

Return value	Description
	again. If the error still occurs, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command terminated abnormally due to multiple causes.

Examples

To verify import definition information:

```
$ sudo datamigratetest --name importfiles
```

To verify whether data can be imported into the file10:

```
$ sudo datamigratetest -v --name importfiles --path file10
Data migration : Possible
Size           : 6
Owner          : S-1-5-21-160711927-2234185241-3274099064-500(70500)
Group          : S-1-5-21-160711927-2234185241-3274099064-513(70513)
Access time    : 2017-08-21 12:47:43.648112700
Modify time    : 2017-08-21 12:48:23.912849500
Create time    : 2017-08-21 12:47:43.648112700
DOS attribute  : A
ACL            :
S-1-5-21-160711927-2234185241-3274099064-500(70500):u:ALLOW:f
Skipped ACL    : -
```

dhcpget (Display the status of DHCP settings)

Synopsis

```
dhcpget [interface]
dhcpget -h
```

Description

This command can be used in a single-node configuration.

This command displays the status of DHCP settings.

Options and arguments

interface

Specify the mng0. If an option is omitted, the command is executed as if mng0 were specified.

Displayed information

The current settings information that is displayed when this command is executed is as follows.

Table 2-138 Current settings information that is displayed when the dhcpget command is executed

Item	Description
`Interface`	Displays information about the interface.

`DHCP`	Displays whether DHCP is used.
	
	`On`
	
	    DHCP is used.
	
	`Off`
	
	    DHCP is not used.
	
	If any settings information has not been applied to the system after the `dhcpset` command is executed, a message appears indicating that the information has not been applied.

Return values

Table 2-139 Return values of the dhcpget command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review the command format and execute it again.
`10`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65`	The system might be busy or a temporary error might have occurred. Wait a while and then execute the command again. If the error still occurs, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

dhcpreload (Reconfiguring the interface when using DHCP)

Synopsis

```
dhcpreload [-y] interface
dhcpreload -h
```

Description

This command can be used in a single-node configuration.

This command obtains information from the DHCP server and sets the information to the interface.

After executing this command, use the `dhcpget` command to confirm whether any settings information has not been applied, or use the `iflist` command to confirm whether the correct IP address is specified. Restart the OS if the KAQM05280-I system message is output.

After this command executes, the management console might be disconnected from the node.

Note:

Before executing this command, ask the CIFS administrator or the end user to disconnect all connections from CIFS clients. Also, confirm that `0` is displayed for **Current number of CIFS login clients** on the **CIFS Service Maintenance** page of the Access Protocol Configuration dialog box. If this command is executed without disconnecting all connections from CIFS clients, users might become unable to access the HDI system from CIFS clients. In such a case, restart the CIFS services.

Options and arguments

interface
Specify the `mng0`.

Return values

Table 2-140 Return values of the dhcpreload command

Return value	Description
0	Normal termination
1[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
1[#], 10, 66[#], 70, 75	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

dhcpset (Setting the interface for when using DHCP)

Synopsis

```
dhcpset [-y] --on interface
dhcpset [-y] --off -a IP-address -n netmask
    [-g gateway] interface
dhcpset --cancel interface
dhcpset -h
```

Description

This command can be used in a single-node configuration.

This command uses DHCP to configure the interface. If information is unavailable from the DHCP server, the status of the application of the settings for using DHCP becomes pending, and a static IP address is set temporarily. To apply the settings information that is pending, verify communication with the DHCP and DNS servers and then restart the node OS or execute the `dhcpreload` command. To cancel the pending status of the settings information, specify the `--cancel` option.

After executing this command, use the `dhcpget` command to confirm whether any settings information has not been applied, or use the `iflist` command to confirm whether the correct IP address is specified. Restart the OS if the KAQM05280-I system message is output.

After this command is executed, the management console might be disconnected from the node.

Notes:

If the status of the application of the settings for using DHCP is pending because of the unavailability of information from the DHCP server, the following information is temporarily set to the specified interface:

- IP address : 169.254.1.100
- netmask : 255.255.0.0
- default gateway : No setting

If any settings information has not been applied to the system, the following operations cannot be executed on the target interface.

- Add an interface (`ifadd` command)
- Edit an interface (`ifedit` command)
- Add routing information (`routeadd` command)
- Delete routing information (`routedel` command)

Options and arguments

`-a` *IP-address*

Specify an IP address in IPv4 format. Specify this option together with the `--off` option.

`--cancel`

Specify this option to cancel the pending status of the application of settings information to the system. This option cannot be specified when the `--on` option or `--off` option is specified.

`-g` *gateway*

Specify the IP address of the gateway to be passed through, in IPv4 format. Specify this option together with the `--off` option.

`-n` *netmask*

Specify a netmask. Specify this option together with the `--off` option.

`--off`

Specify this option when disabling the setting to use DHCP. This option cannot be specified when the `--on` option or `--cancel` option is specified.

If you specify this option to disable the use of DHCP, you must manually register the IP address and the host name of HDI in the DNS server.

`--on`

Specify this option when setting an interface by acquiring information from the DHCP server. This option cannot be specified when the `--off` option or `--cancel` option is specified.

interface

Specify the `mng0`.

Return values

Table 2-141 Return values of the dhcpset command

Return value	Description
0	Normal termination
1[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
1[#], 10, 66[#], 70, 73, 75	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Examples

When setting an interface by acquiring information from the DHCP server

```
$ sudo dhcpset --on mng0
KAQM05271-Q Changes to the DHCP settings will be applied to the system. If
you proceed, the node might become disconnected. Are you sure you want to
apply the changes to the DHCP settings? (y/n) y
KAQM05273-I The node might be disconnected because the network settings
were changed. If the node is disconnected, wait a few minutes, and then
log in again.
```

When disabling DHCP and manually setting the interface information

- The IP address is `10.213.89.103`.
- The netmask is `255.255.255.0`.
- Set the gateway IP address to `10.213.89.1`
- The port name of the interface is `mng0`.

```
$ sudo dhcpset --off -a 10.213.89.103 -n 255.255.255.0 -g 10.213.89.1 mng0
KAQM05271-Q Changes to the DHCP settings will be applied to the system. If
you proceed, the node might become disconnected. Are you sure you want to
apply the changes to the DHCP settings? (y/n) y
KAQM05273-I The node might be disconnected because the network settings
were changed. If the node is disconnected, wait a few minutes, and then
log in again.
```

When breaking out of pending status where DHCP settings information has not been applied to the system

```
$ sudo dhcpset --cancel mng0
KAQM05277-I The DHCP settings that were pending application to the system
were canceled.
```

dircreate (Create a directory)

Synopsis

```
dircreate -u {user-name|user-ID} -g {group-name|group-ID}
    [-m {mode|inherit}] path
dircreate -h
```

Description

Creates a directory in a file system.

If you want to create a hierarchy of directories under the mount point, create the top directory first, and then create the lower directories.

For a file system where data from another HDI system is referenced as read-only, when the target directory synchronizes data migrated to the HCP system, will be updated with the attribute settings of HDI system that discloses data.

Notes:
  - This command cannot be used for home-directory-roaming file systems.
  - This command cannot be used for read-write-content-sharing file systems.

Options and arguments

-g { *group-name* | *group-ID* }

Specify the group name or group ID of the owner group for the directory you are creating.

You cannot specify a Windows domain built-in group for the group name.

When you specify the owner group by using its group ID, specify it in the range from 0 to 2147483147. Non-zero IDs cannot start with 0.

-m { *mode* | inherit }

Specify the mode for the owner, owner group, and other users (for Advanced-ACL-type file systems, this means all users and groups).

mode

Specify the 3- or 4-digit number resulting from the logical OR of the owner, owner group, and other users modes. For details about the specifiable modes, see Table 2-142 Directory modes specifiable in the -m option of the dircreate command on page 2-277.

For an Advanced ACL file system, ACEs set in the parent directory are inherited, and then the ACEs corresponding to the mode specified in the command are overwritten. Therefore, the ACEs corresponding to the specified mode are set for the owner, owner group, all users and groups. For other users or groups, the ACEs inherited from the parent directory are set.

inherit

Specify this option to set only the ACEs inherited from the parent directory for an Advanced ACL file system.

If you omit this option, the command is executed assuming that 0755 was specified for the mode of the directory to be created.

Table 2-142 Directory modes specifiable in the -m option of the dircreate command

Octal numbers	Description
2000	Uses the SetGID. The subdirectories and files created under the directory inherit the GID of the directory. When further subdirectories are created under the directory to which the SetGID is applied, those subdirectories inherit the GID of the upper directory.
1000	Sets the sticky bit so that subdirectories and files created under the directory can only be deleted or renamed by the owner.
0400	Sets read permission for the owner.
0200	Sets write permission for the owner.
0100	Sets search permission for the owner.
0040	Sets read permission for the owner group.
0020	Sets write permission for the owner group.
0010	Sets search permission for the owner group.
0004	Sets read permission for other users.
0002	Sets write permission for other users.
0001	Sets search permission for other users.

-u { *user-name* | *user-ID* }

Specify the user name or user ID of the owner of the directory to be created.

You cannot specify a Windows domain built-in user for the user name.

When you specify the owner by using its user ID, specify it in the range from 0 to 2147483147. Non-zero IDs cannot start with 0.

path

Specify the absolute path of the directory to be created, using no more than 256 characters beginning with /mnt/.

You can use alphanumeric characters, exclamation marks (!), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), plus signs (+), commas (,), hyphens (-), periods (.), forward slashes (/), semicolons (;), equal signs (=), at marks (@), left square brackets ([), right square brackets (]), carets (^), underscores (_), grave accent marks (`), left curly brackets ({), right curly brackets (}), tildes (~), and spaces. You can also specify multibyte characters. However, you cannot specify a path that includes a symbolic link. Note that .conflict, .conflict_longpath, .snaps, .history, and .lost+found cannot be specified for a directory name.
Also, .arc, .system_gi, .system_reorganize, or lost+found cannot be

specified for the name of a directory immediately under the file system. Forward slashes and spaces specified at the end are deleted.

Note that if you use the created directory as a CIFS or NFS shared directory, the number and type of specifiable characters differ. For details, see the description for shared directories in cifscreate (Create a CIFS share) on page 2-151 or nfscreate (Create an NFS share) on page 2-502.

Return values

Table 2-143 Return values of the dircreate command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To create a directory according to the following conditions:

- Create the directory `dir_case1` directly under the `/mnt/FS1`.
- Specify `USER1` as the owner.
- Specify `GROUP1` as the owner group.
- Set the mode to `750`.

```
$ sudo dircreate -u USER1 -g GROUP1 -m 750 /mnt/FS1/dir_case1
```

dirdel (Delete a directory)

Synopsis
```
dirdel path
dirdel -h
```

Description

Releases the NFS share or CIFS share in a file system, and then deletes directories that are not in use.

For a file system where data from another HDI system is referenced as read-only, unnecessary directories can be deleted if the target directory does not synchronize the data migrated to the HCP system. To check whether the directory on the HDI system and data migrated to the HCP system are synchronizing, use the `arcurlget` command.

Options and arguments

path

Specify the absolute path beginning with `/mnt/` of the directory to be deleted. You cannot include symbolic links in the path. Note that the following paths cannot be specified as a directory to be deleted:

- A path that includes a symbolic link
- A directory used for saving transferred log files of performance statistics
- A directory used for saving s CIFS access log
- A directory for which a CIFS share or NFS share has been set
- A login directory of the FTP or SFTP service
- TFTP access directory
- A directory with a name that includes `.conflict`, `.conflict_longpath`, `.snaps` , `.history`, and `.lost+found`

Also, `.arc`, `.system_gi`, `.system_reorganize`, or `lost+found` cannot be specified for the name of a directory immediately under the file system.

Return values

Table 2-144 Return values of the dirdel command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 66, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation.

Return value	Description
	If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

diredit (Change directory attributes)

Synopsis

```
diredit [-u {user-name|user-ID}] [-g {group-name|group-ID}]
    [-m mode] path
diredit -h
```

Description

Changes the attributes of a directory in the file system.

If you omit any of the following options, the current setting information applies. If you omit all the options, only the path validation check is performed.

For a file system where data from another HDI system is referenced as read-only, the attributes can be modified if the target directory does not synchronize data migrated to the HCP system. Note that when synchronizing data migrated to the HCP system, will be updated with the attribute settings of HDI system that discloses data. To check whether the directory on the HDI system and data migrated to the HCP system are synchronizing, use the arcurlget command.

Note:

This command cannot be used for home-directory-roaming file systems.

Options and arguments

-g { *group-name* | *group-ID* }

Specify the group name or group ID if you want to change the owner group of the specified directory.

You cannot specify a Windows domain built-in group for the group name.

When you specify the owner group by using its group ID, specify it in the range from 0 to 2147483147. Non-zero IDs cannot start with 0.

-m *mode*

Specify the new mode if you want to change the mode for the owner, owner group, and other users. Specify the mode as a 3-digit or 4-digit number representing the logical OR of the following octal numbers.

Table 2-145 Directory modes specifiable in the -m option of the diredit command

Octal numbers	Description
2000	Uses the SetGID. The subdirectories and files created under the directory inherit the GID of the directory. When further subdirectories are created under the directory to which the SetGID is applied, those subdirectories inherit the GID of the upper directory.
1000	Sets the sticky bit so that subdirectories and files created under the directory can only be deleted or renamed by the owner.
0400	Sets read permission for the owner.
0200	Sets write permission for the owner.
0100	Sets search permission for the owner.
0040	Sets read permission for the owner group.
0020	Sets write permission for the owner group.
0010	Sets search permission for the owner group.
0004	Sets read permission for other users.
0002	Sets write permission for other users.
0001	Sets search permission for other users.

-u { *user-name* | *user-ID* }

Specify the user name or user ID if you want to change the owner of the specified directory.

You cannot specify a Windows domain built-in user for the user name.

When you specify the owner by using its user ID, specify it in the range from 0 to 2147483147. Non-zero IDs cannot start with 0.

path

Specify the absolute path beginning with /mnt/ of the directory whose attributes you want to change. You cannot include symbolic links in the path. Note that .conflict, .conflict_longpath, .snaps , .history, and .lost+found cannot be specified for a directory name.

Also, .arc, .system_gi, .system_reorganize, or lost+found cannot be specified for the name of a directory immediately under the file system.

For read-write-content-sharing file systems, the mount point must be specified.

Return values

Table 2-146 Return values of the diredit command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To change the mode of the `/mnt/FS1/dir_case1` directory to `777`:

```
$ sudo diredit -m 777 /mnt/FS1/dir_case1
```

dirgetacl (Display ACL information)

Synopsis

```
dirgetacl path
dirgetacl -h
```

Description

Displays the ACL information set for a shared directory. The displayed ACL information differs depending on the ACL type of the file system to which the shared directory belongs.

Options and arguments

path

Specify the absolute path beginning with `/mnt/` of the directory where you want to display ACL information. You cannot include symbolic links in the path.

Displayed information (Advanced ACL type)

The following table lists the information displayed when you execute the command.

Table 2-147 Information displayed when executing the dirgetacl command (Advanced ACL type)

Item	Description
path	Displays the specified directory name.
user-or-group	Displays the name of the user or group for which the ACE is set. If a `__groupowner` user (user ID: 4294967292) is specified for ACE, the `__groupowner` user (user ID: 4294967292) is displayed as `groupowner`.

account-type	Displays the account type.
	
	`u`
	    User
	`g`
	    Group

application-destination	Displays the application destination for the ACE.
	
	`o`
	    This folder only
	`a`
	    This folder, subfolders, and files
	`f`
	    This folder and subfolders
	`e`
	    This folder and files
	`s`
	    Subfolders and files only
	`u`
	    Subfolders only
	`i`
	    Files only

inheritance-range	Displays the range for which the ACE is to be inherited.
	
	`o`
	    Only the folders and files immediately under this folder
	`a`
	    All folders and files under this folder

ACE-type	Displays the ACE type.
	`ALLOW`
	    Allowed ACE
	`DENY`
	    Denied ACE

Item	Description
access-permissions	Displays the access permissions. When more than one type of access permission is set, they are separated by two colons (::).
	`f` Full Control
	`s` Traverse Folder / Execute File
	`r` List Folder / Read Data
	`a` Read Attributes
	`e` Read Extended Attributes
	`w` Create Files / Write Data
	`p` Create Folders / Append Data
	`t` Write Attributes
	`x` Write Extended Attributes
	`l` Delete Subfolders and Files
	`d` Delete
	`c` Read Permissions
	`h` Change Permissions
	`g` Take ownership

Displayed information (Classic ACL type)

For an ACL set by a CIFS client, the information displayed by the `dirgetacl` command depends on the information selected in **Apply To**. An ACL set by a CIFS client with **This folder only** selected in **Apply To** will be displayed as an access ACL. An ACL set with **Subfolders and files only** selected in **Apply To** will be displayed as the default ACL.

Note:

You can check the **Apply To** setting from a CIFS client (Windows 7 environment) as follows:

a.   On the CIFS client, display the directory properties.

b. Select the **Security** tab, and then click the **Advanced** button.

c. Select the **Permissions** tab.

The following table lists the information displayed when you execute the command.

Table 2-148 Information displayed when executing the dirgetacl command (Classic ACL type)

Item	Description
# file	Displays the specified directory name.
# owner	Displays the directory owner name.
# group	Displays the directory owner group name.
user	Displays the ACE for the owner or the specific user.
	If the entry is for the owner, information is displayed in the following format:
	user::*access-permissions*
	If the entry is for a specific user, information is displayed in either of the following formats:
	user:*user-name*:*access-permissions* user:*user-ID*:*access-permissions*
group	Displays the ACE for the group.
	If the entry is for the owner group, information is displayed in the following format:
	group::*access-permissions*
	If the entry is for a specific group, information is displayed in either of the following formats:
	group:*group-name*:*access-permissions* group:*group-ID*:*access-permissions*
mask	Displays the permissions (mask) applied to the specific user or group.
	The mask is the ACE that limits the access permissions that are valid for the specific user or group.
other	Displays the ACE for others.
default:user	Displays the ACE of the default ACL for the owner or the specific user.
	If the entry is for the owner, information is displayed in the following format:
	default:user::*access-permissions*
	If the entry is for a specific user, information is displayed in the following format:
	default:user: *user-name*:*access-permissions* default:user: *user-ID*:*access-permissions*
default:group	Displays the ACE of the default ACL for the group.
	If the entry is for the owner group, information is displayed in the following format:
	default:group::*access-permissions*

Item	Description
	If the entry is for a specific group, information is displayed in either of the following formats: `default:group:`*`group-name`*`:`*`access-permissions`* `default:group:`*`group-ID`*`:`*`access-permissions`*
`default:mask`	Displays the default access permissions (mask) applied to the specific user or group.
`default:other`	Displays the ACE of the default ACL for other information.

Note:

When a mask is set or the settings specify the mask is not recalculated, the ACL for the owner group, specific user, or specific group might not be controlled as specified by the specified access permissions. When the setting for the mask is in effect, the ACL for the specific user is followed by the access permissions that are actually in effect.

ACL-for-specific-user `#effective:` *access-permissions-in-effect*

Return values

Table 2-149 Return values of the dirgetacl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

dirlist (List directory attributes)

Synopsis

```
dirlist [-d] [-n] [-c] path
dirlist -h
```

Description

Lists the attributes of the specified directory or subdirectory. When multiple subdirectories reside under the specified directory, the attributes are listed in ascending order of the subdirectory names.

Options and arguments

`-c`

Specify this to display directory information separated with colons (`:`).

`-d`

Specify this to view the attributes of only the specified directory. If you omit this option, the command lists attributes for the subdirectories under the specified directory.

`-n`

Specify this to view the owner's user ID and group ID in place of user name and owner group name. If you omit this option, the user name and the group name are displayed.

path

Specify the absolute path beginning with `/mnt/` for the directory whose attributes you want to view. You cannot include symbolic links in the path.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-150 Information displayed when executing the dirlist command

Item	Description
directory-mode	Displays the directory mode as the logical OR of mode bits (a 4-digit octal number).
	`2000`
	Uses the SetGID.
	`1000`
	Sets the sticky bit.
	`0400`
	Sets read permission for the owner.
	`0200`
	Sets write permission for the owner.
	`0100`
	Sets search permission for the owner.
	`0040`
	Sets read permission for the owner group.
	`0020`

Item	Description
	Sets write permission for the owner group.
	`0010`
	Sets search permission for the owner group.
	`0004`
	Sets read permission for other users.
	`0002`
	Sets write permission for other users.
	`0001`
	Sets search permission for other users.
owner	Displays the user name or user ID of the owner.
	Specify the `-n` option to display the user ID.
	If you omit the `-c` option, and the user name does not include a multibyte character, the first 16 characters of the user name are left-justified and displayed (padded with spaces). The 17th and subsequent characters are truncated. In other cases, all characters will be displayed.
	If the user ID cannot be converted into the user name, the user ID is displayed.
owner-group	Displays the group name or group ID of the owner group.
	Specify the `-n` option to display the group ID.
	If you omit the `-c` option, and the user name does not include a multibyte character, the first 16 characters of the user name are left-justified and displayed (padded with spaces). The 17th and subsequent characters are truncated. In other cases, all characters will be displayed.
	If the group ID cannot be converted into the group name, the group ID is displayed.
directory-path	Displays the absolute path of the specified directory.

Return values

Table 2-151 Return values of the dirlist command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10, 70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

dirsetacl (Set ACLs)

Synopsis

Advanced ACL type

```
dirsetacl -t advanced [-e]
    {{--allow|--replace|--deny} ACE|-x ACE}... path
dirsetacl -t advanced -e -r
     -x ACE[ -x ACE...] path
dirsetacl -t advanced -e -b [-r] path
```

Classic ACL type

```
dirsetacl [-t classic] [-n] [-d] {-s|-m|-x}
    ACE[,ACE...] path
dirsetacl [-t classic] -b path
dirsetacl [-t classic] -k path
```

To reference the command syntax

```
dirsetacl -h
```

Description

Sets an ACL for the shared directory.

Advanced ACL type

For one directory, you can specify a maximum of 700 ACEs.

Classic ACL type

For one directory, you can specify a maximum of 128 ACEs (up to 64 ACEs each for access ACLs and masks, and for the default ACLs and masks).

In the default ACL of the owner group, if you specify 0 or – for access permission, you must also specify 0 or – for access permissions in the default ACL of other users. However, in the default ACL of specific users or specific groups, do not specify 0 or – for access permissions.

The ACLs you can set differ depending on the ACL type of the file system to which the shared directory belongs.

Do not create or rename a folder or file under the directory that was specified when processing this command.

The amount of time required for processing is proportionate to the total number of files and folders in the specified directory. For example, if there is a total number of 1 million files and folders, processing will take about 4 hours and 10 minutes, and if there is a total number of 10 million files and folders, processing will take about 42 hours.

For a file system where data from another HDI system is referenced as read-only, the ACL can be configured if the target directory does not synchronize data migrated to the HCP system. Note that when synchronizing data migrated to the HCP system, will be updated with the attribute settings of HDI system that discloses data. To check whether the directory on the HDI system and data migrated to the HCP system are synchronizing, use the `arcurlget` command.

Note:
    This command cannot be used for home-directory-roaming file systems.

Options and arguments

`{--allow|--replace|--deny}` *ACE*
    Specify this option to add or replace the specified ACE.

    When you want to edit an existing ACL, specify this option together with the `-e` option. If you do not specify the `-e` option, all the existing ACEs for the specified directory are deleted and replaced with the new ACEs you have set.

    Note that a denied ACE overrides an allowed ACE, irrespective of the order in which the ACEs are set.

    `--allow`

        Specify this option to grant access permissions to the specified user or group.

        When you specify this option together with the `-e` option, the specified access permissions are added to the ACE for the same user or group.

    `--replace`

        Specify this option to grant access permissions to the specified user or group.

        When you specify this option together with the `-e` option, the ACEs for the same user or group with the equivalent application destination or inheritance range are discarded and replaced by the specified ACE.

    `--deny`

        Specify this option to deny access permissions to the specified user or group.

        When you specify this option together with the `-e` option, the ACEs for the same user or group with the equivalent application destination or inheritance range are discarded and replaced by the specified ACE.

    ACE

        Specify the ACE to be added or replaced in the following format:

```
user-or-group:account-type:application-
destination:inheritance-range:access-permissions[::access-
permissions...]
```
The following table lists the information specified as ACEs.

Table 2-152 Information specified as ACEs in the dirsetacl command (when the --allow, --replace, or --deny option is specified)

Item	Specification
user-or-group	Specify the name of the user or group to which you want to grant access permissions. You cannot specify a Windows domain built-in user or group other than `Everyone`, `CREATOR GROUP`, and `CREATOR OWNER` for the user name or group name.

account-type [#1] [#2]	Specify the account type.
	
	u
	
	    Specify this to grant access permissions to a user.
	
	g
	
	    Specify this to grant access permissions to a group.

application-destination [#3]	Specify the application destination for the ACE. When the application destination differs between the specified ACE and the existing ACE for the same user or group, the specified ACE will be added.
	
	o
	
	    This folder only
	
	a
	
	    This folder, subfolders, and files
	
	f
	
	    This folder and subfolders
	
	e
	
	    This folder and files
	
	s
	
	    Subfolders and files only
	
	u
	
	    Subfolders only
	
	i
	
	    Files only

inheritance-range [#3]	Specify the range for which the ACE is inherited. When the inheritance range differs between the specified ACE and the existing ACE for the same user or group, the specified ACE will be added. o Only the folders and files immediately under this folder

Hitachi Data Ingestor CLI Administrator's Guide

Item	Specification
	a All folders and files under this folder

access-permissions	Specify the access permissions. When more than one type of access permission is set, they are separated by two colons (::).
	
	f
	
	    Full Control
	
	s
	
	    Traverse Folder / Execute File
	
	r
	
	    List Folder / Read Data
	
	a
	
	    Read Attributes
	
	e
	
	    Read Extended Attributes
	
	w
	
	    Create Files / Write Data
	
	p
	
	    Create Folders / Append Data
	
	t
	
	    Write Attributes
	
	x
	
	    Write Extended Attributes
	
	l
	
	    Delete Subfolders and Files
	
	d
	
	    Delete.
	
	c
	
	    Read Permissions
	
	h
	
	    Change Permissions
	
	g
	
	    Take ownership

#1: If you specify the CREATOR OWNER for the user name, you need to specify u.

#2: If you specify the Everyone or CREATOR GROUP for the group name, you need to specify g.

#3: ACEs are inherited according to application destinations and inheritance ranges. The following table lists inheritance ranges.

Command Reference

Table 2-153 Inheritance ranges of ACEs

Application destination	Inheritance range	
	o	**a**
o	Not inherited	
a	Folders and files immediately under the directory	All folders and files under the directory
f	Folders immediately under the directory	All folders under the directory
e	Files immediately under the directory	All folders and files under the directory
s	Folders and files immediately under the directory	All folders and files under the directory
u	Folders immediately under the directory	All folders under the directory
i	Files immediately under the directory	All folders and files under the directory

-b

Specify this option when you want to delete all existing ACLs.

Advanced ACL type

Specify this option when you want to delete all existing ACLs for the specified directory. Specify this option together with the -e option.

Classic ACL type

Specify this option when you want to delete all access ACLs or default ACLs for the specific user or group.

-d

Specify this option if you want to set a default ACL. If you omit this option, an access ACL is set. If you omit any of the default ACEs for the owner, owner group, or other users, the permissions set for the owner, owner group, or other users of the parent directory apply.

-e

Specify this option when you want to edit an existing ACL.

-k

Specify this option if you want to delete all default ACLs.

-n

Specify this option if you do not want to recalculate the mask. You do not need to specify this option for normal operation. If you set an ACL without specifying this option, the mask will be recalculated to an appropriate value.

-r

For the Advanced ACL type, specify this option to delete all the ACEs for the files and folders under the specified directory. Specify this option whenever inherited ACLs for files or folders under the specified directory will be deleted.

If you specify this option with the -x option, all ACLs for the specified user or group are deleted. If you specify this option with the -b option, all ACLs are deleted that are set for users and groups assigned to files and directories under the specified directory that are the same as the users and groups assigned to the specified directory.

`{-s|-m|-x} ACE[,ACE...]`

For the Classic ACL type, specify this option to add, modify, or delete the specified ACEs.

`-s`

Specify this option to delete all existing ACEs and reset the ACL.

When you set an access ACL, all the ACEs for the access ACL are deleted, and then the new ACEs for the access ACL are added. You must specify ACEs for the owner, owner group, and other users.

When you set a default ACL, all the ACEs for the default ACL are deleted, and then the new ACEs for the default ACL are added.

`-m`

Specify this option in the following cases:
- When you want to add a new ACE to the existing ACL.
- When you want to change the ACEs.

`-x`

Specify this option if you want to delete the specified ACE.

Only the following ACEs can be deleted:
- An access ACL for a specific user or group.
- A default ACL for a specific user or group.

When deleting a default ACL or a mask of the default ACL for the owner, owner group and others, specify the -k option.

ACE [, *ACE* ...]

Specify the ACE to be added, modified, or deleted. Specify the ACE in the following format:

`processing-target:user-or-group:access-permissions`

However, when the -x option is specified to delete the ACL for a specific user or a specific group, the *ACE* argument must be specified in the following format:

`processing-target:user-or-group`

The following table lists the information specified as ACEs.

Table 2-154 Information specified as ACEs in the dirsetacl command (when the -s, -m, or -x option is specified for the Classic ACL type)

Item	Specification

processing-target [1] [2]	Specify the target of ACL addition, modification, or deletion.
	
	`u` or `user`
	    Specify this option to set an ACL for the owner or for a specific user.
	
	`g` or `group`
	    Specify this option to set an ACL for the owner group or for a specific group.
	
	`m` or `mask`
	    Specify this option if you want to set a mask. You do not need to operate the mask for normal operation.
	
	`o` or `other`
	    Specify this option if you want to set an ACL for others.

user-or-group	Specify this argument if you want to add, modify, or delete the ACL for a specific user or group. Note that you cannot use any of the following characters in a string: dollar signs (`$`), and grave accent marks (`` ` ``). To specify a user, specify the user name or user ID here. To specify a group, specify the group name or group ID here. You cannot specify a Windows domain built-in user or group other than `Everyone`, `CREATOR GROUP`, and `CREATOR OWNER` for the user name or group name. You do not need to specify this argument in the following cases: • When you are to add, modify, or delete the ACL for the owner, owner group, or others. • When you are to set a mask.
access-permissions	Specify the access permissions to be added, changed, or deleted. Use a combination of characters or set an octal number representing the logical OR of the permissions. In octal notation, `r` (read permission), `w` (write permission), `x` (directory search permission), and `–` (not permitted) correspond to `4`, `2`, `1`, and `0`, respectively. For example, if you want to allow read and write access, specify `rw` or `6`.

#1: If you specify the `CREATOR OWNER` for the user name, you need to specify `u` or `user`.

#2: If you specify the `Everyone` or `CREATOR GROUP` for the group name, you need to specify `g` or `group`.

`-t advanced`

Specify this for the Advanced ACL type.

`-t classic`

Specify this for the Classic ACL type. You can omit this option.

`-x` *ACE*

For the Advanced ACL type, specify this option to delete the ACEs for the specified user or group. Specify this option with the `-e` option.

ACE

Specify the ACE to be deleted in the following format:

user-or-group:*account-type*

The following table lists the information specified as ACEs.

Table 2-155 Information specified as ACEs in the dirsetacl command (when the -x option is specified for the Advanced ACL type)

Item	Specification
user-or-group	Specify the name of the user of group for the ACE to be deleted.
	To specify a user, specify the user name or user ID here. To specify a group, specify the group name or group ID here. You cannot specify a Windows domain built-in user or group other than `Everyone`, `CREATOR GROUP`, and `CREATOR OWNER` for the user name or group name..
account-type [#1] [#2]	Specify the account type.
	`u`
	Specify this to delete the ACE for a user.
	`g`
	Specify this to delete the ACE for a group.

#1: If you specify the `CREATOR OWNER` for the user name, you need to specify `u`.

#2: If you specify the `Everyone` or `CREATOR GROUP` for the group name, you need to specify `g`.

path

Specify the absolute path beginning with `/mnt/` of the directory for which the ACL is to be set. You cannot include symbolic links in the path. Note that `.conflict`, `.conflict_longpath`, `.snaps` , `.history`, and `.lost +found` cannot be specified for a directory name.
Also, `.arc`, `.system_gi`, `.system_reorganize`, or `lost+found` cannot be specified for the name of a directory immediately under the file system.

For read-write-content-sharing file systems, the mount point must be specified.

Return values

Table 2-156 Return values of the dirsetacl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70, 71	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples (Advanced ACL type)

To add an ACE to the existing ACL according to the following conditions:

- The target directory is `/mnt/fs/share1`.
- The *List Folder / Read Data* and *Read Attributes* permissions are granted to the `Everyone` group.
  - The application destination is *This folder, subfolders, and files*.
  - The inheritance range is all folders and files under this folder.
- *Full Control* permission is granted to the `User1` user. The application destination is *This folder only*.

```
$ sudo dirsetacl -t advanced -e --allow Everyone:g:a:a:r::a --allow
User1:u:o:o:f  /mnt/fs/share1
```

To delete all existing ACEs and reset the ACE according to the following conditions:

- The target directory is `/mnt/fs/share1`.

- The *List Folder / Read Data* and *Traverse Folder / Execute File* permissions are granted to the `Everyone` group. The application destination is *This folder only*.

```
$ sudo dirsetacl -t advanced --replace Everyone:g:o:a:r::s /mnt/fs/share1
```

To delete all existing ACEs and reset the ACE according to the following conditions:

- The target directory is `/mnt/fs/share1`.
- The *List Folder / Read Data*, *Traverse Folder / Execute File*, and *Delete* permissions are granted to the `DOMAIN_NAME\CREATOR OWNER` user.
  - The application destination is *Subfolders only*.
  - The inheritance range is all folders and files under this folder.

```
$ sudo dirsetacl -t advanced --replace "DOMAIN_NAME\CREATOR
OWNER:u:u:a:r::s::d" /mnt/fs/share1
```

Examples (Classic ACL type)

To modify the access ACL for a directory according to the following conditions:

- The target directory is `/mnt/ACLCIFS/acldir`.
- Read and write permissions are granted to the `user01` user.
- Read permission is granted to the `ACL-users` group.

```
$ sudo dirsetacl -m u:user01:rw,g:ACL-users:r /mnt/ACLCIFS/acldir
```

To delete the default ACEs for a directory according to the following conditions:

- The target directory is `/mnt/ACLCIFS/acldir`.
- Delete the ACE for the `user01` user.
- Delete the ACE for the `ACL-users` group.

```
$ sudo dirsetacl -d -x u:user01,g:ACL-users /mnt/ACLCIFS/acldir
```

diskfreeget (Display the capacity of a volume group)

Synopsis

```
diskfreeget [-h]
```

Description

This command can be used for single node configurations with only one volume group.

The command displays the total and available capacity of a volume group.

You can display information for multiple volume groups by using the `vgrlist` command.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-157 Information displayed when executing the diskfreeget command

Item	Description
Total disk size(GB)	Displays the total capacity of the volume group in gigabytes.
Free disk size(GB)	Displays the available capacity of the volume group in gigabytes.

Return values

Table 2-158 Return values of the diskfreeget command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.
99[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

\#
   The command ended abnormally due to multiple causes.

dpreclaim (Release the unused area of virtual LUs)

Synopsis

```
dpreclaim [--ddev]  file-system-name
```

```
dpreclaim -h
```

Description

This command releases the unused area of virtual LUs used in a file system. If the capacity of the file system is less than 256 MB, this command cannot be used to release the unused area.

When this command is executed, the specified file system temporarily cannot be accessed. For this reason, access to the file system from a client or setup processing for Quota or file share might time out.

- If this command is executed while a client is accessing the file system, access from the client might time out.
- If you configure quota or file share settings during processing of this command, the operation might time out.

Notes:

- While using Hitachi AMS2000 series or HUS100 series storage systems, you might not be able to release the unused area of a virtual LU even if you execute the `dpreclaim` command. In this case, use Hitachi Storage Navigator Modular 2 to optimize the DP pool after you execute the command.
- Unused areas in the DP pool are released by the page, so these areas cannot be released until all areas in their page stop being used. Therefore, you might not be able to free the space of deleted files even if you execute the `dpreclaim` command.

Options and arguments

`--ddev`

    This option is not supported.

file-system-name

    Specify the name of the file system in which unused area is to be released.

Return values

Table 2-159 Return values of the dpreclaim command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10[#], 65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
10[#], 66[#], 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

dumpdel (Delete dump files)

Synopsis

```
dumpdel [-y]
dumpdel -h
```

Description

Deletes all dump files. Note that if dump files that are not converted exist after deleting dump files, this command converts the dump files.

This command is applied to the node on which the command is executed. In cluster configurations, this command must be executed on both nodes.

Execute this command if you are asked to do so by maintenance personnel.

Return values

Table 2-160 Return values of the dumpdel command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

dumpset (Specify whether to acquire dump files)

Synopsis

```
dumpset [--on|--off] [--vserver]
dumpset -h
```

Description

Specifies whether to acquire dump files. You can also use the command to view the current setting.

If you specify the option to acquire dump files, a dump file is acquired when the node is reset. The dump files are output to the `/dump/download/service` directory.

This command is applied to the node on which the command is executed. Therefore, this command must be executed on both nodes.

> Note:
>   Change this setting only when you are asked to do so by maintenance personnel.

Options and arguments

`--off`
    Specify this if you do not want to acquire dump files.

`--on`
    Specify this to acquire dump files. The initial setting is `--on`.

`--vserver`
    This option is not supported.

If you omit all options, the current setting is displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-161 Information displayed when executing the dumpset command

Item	Description
Physical Node	Displays whether dump files are to be acquired on the physical node.
	on
	Dump files are to be acquired on the physical node.
	off
	Dump files are not to be acquired on the physical node

Return values

Table 2-162 Return values of the dumpset command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To prevent dump files from being acquired:

```
$ sudo dumpset --off
```

emergencyshutdown (Emergency shutdown on a node)

Synopsis

```
emergencyshutdown --force
```

Description

Shuts down the OS on a node in an emergency regardless of the status of the node and resource groups.

In a single-node configuration, do not execute this command if the user disk was created on the internal hard disk.

Note:

Data might be lost if it is not written to the internal disk when executing this command.

Return values

Table 2-163 Return values of the emergencyshutdown command

Return value	Description
0	Normal termination

Return value	Description
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

encdisplaykey (Display a key to be saved outside the system as a common key used for local data encryption)

Synopsis

```
encdisplaykey [-h]
```

Description

Displays a key that is to be saved outside the system as a common key used for local data encryption.

In a cluster configuration, execute this command in either system to display the key.

This command uses a passphrase that was specified interactively to encrypt a common key used for local data encryption, and then displays a character string in hexadecimal format as the key, so that the key can be saved outside the system. Copy and paste the displayed character string to a text file, make sure that no linefeed characters are included, and then save the key in storage media outside the system.

The following conditions must be met before you can use this command:

- The local data encryption function is enabled.
- The common key was successfully acquired from the HCP system during the startup of the OS.

To end interactive entry and cancel the command execution, press **Ctrl**+**D** without entering anything for any of the items.

The following table lists the information items that can be set interactively.

Table 2-164 Information that can be specified interactively for the encdisplaykey command

Item	Description
`Enter passphrase`	Specify a passphrase used to create a key to be saved outside the system as a common key saved in the HCP. You can use 1 to 64 characters.
	You can use alphanumeric characters, exclamation marks (`!`), double quotation marks (`"`), hash marks (`#`), dollar signs (`$`), percent signs (`%`), ampersands (`&`), single quotation marks (`'`), left parentheses (`(`), right parentheses (`)`), asterisks (`*`), plus signs (`+`), commas (`,`), hyphens (`-`), periods (`.`), forward slashes (`/`), colons (`:`), semicolons (`;`), left angle brackets (`<`), equal signs (`=`), right angle brackets (`>`), question marks (`?`), at marks (`@`), left square brackets (`[`), backslashes (`\`), right square brackets (`]`), carets (`^`), underscores (`_`), grave accent marks (`` ` ``), left curly brackets (`{`), vertical bars (`|`), right curly brackets (`}`), tildes (`~`), and spaces.
	For security reasons, we recommend you specify a passphrase containing at least 10 characters using a combination of numbers and alphabetic letters.
`Confirm passphrase`	Specify the above passphrase again.

Note:

The character strings specified for `Enter passphrase` and `Confirm passphrase` are not displayed.

Return values

Table 2-165 Return values of the encdisplaykey command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`2, 10, 70, 71, 73, 75`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

encrecoverkey (Restore a common key used for local data encryption)

Synopsis

```
encrecoverkey [-h]
```

Description

Restores a common key used for local data encryption by decrypting the key saved in storage media outside the system.

If you execute this command in a cluster configuration, the command restores the common key for both nodes. Note, however, that if synchronization of the nodes fails, only the common key for the local node is restored. In this case, you must correct the failure in the remote node, and then restart the OS of the remote node and restore the common key.

If you stop or restart the OS of the node before recovering from an HCP access failure, re-execute the command to restore the common key.

The following conditions must be met before you can use this command:

- The local data encryption function is enabled.
- An attempt to acquire the common key from the HCP system has failed during the startup of the OS.

To end interactive entry and cancel the command execution, press **Ctrl**+**D** without entering anything for any of the items.

The following table describes the information you specify with the `encrecoverkey` command:

Table 2-166 Information you specify with the encrecoverkey command

Item	Description
Enter key	Specify the key saved in storage media outside the system.
Enter passphrase	Specify the passphrase specified for the `encdisplaykey` command.

Notes:

  - The character strings specified for `Enter passphrase` is not displayed.

  - When you specify the key saved in storage media outside the system, make sure that the key does not include a linefeed character.

Return values

Table 2-167 Return values of the encrecoverkey command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 3, 10, 70, 71, 75, 76, 77	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

encverifykey (Verify a common key used for local data encryption)

Synopsis

```
encverifykey [-h]
```

Description

Verifies that a key saved in storage media outside the system matches a common key used for local data encryption.

If the keys match, the KAQM05307-I message indicating that the keys match appears. If the keys do not match, take action according to the instructions given for the KAQM05306-E or KAQM05321-E message.

The following conditions must be met before you can use this command:

- The local data encryption function is enabled.
- The common key was successfully acquired from the HCP system during the startup of the OS.

To end interactive entry and cancel the command execution, press **Ctrl**+**D** without entering anything for any of the items.

The following table describes the information you specify with the `encverifykey` command:

Table 2-168 Information you specify with the encverifykey command

Item	Description
Enter key	Specify the key saved in storage media outside the system.
Enter passphrase	Specify the passphrase specified for the `encdisplaykey` command.

Notes:

- The character strings specified for `Enter passphrase` is not displayed.
- When you specify the key saved in storage media outside the system, make sure that the key does not include a linefeed character.

Return values

Table 2-169 Return values of the encverifykey command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 3, 10, 70, 71, 73, 75	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

eraselog (Delete the logs generated at command execution)

Synopsis

```
eraselog
```

Description

Delete the packet dump files and the log files that are created when the `nasipneigh`, `nasnetstat`, `nasping`, or `nastraceroute` command was executed.

Table 2-170 Return values of the eraselog command

Return value	Description
0	Normal termination

fpctl (Manage FC path settings)

Synopsis

```
fpctl -e auto-online [--on|--off]
fpctl -e load-balance [--on [--type {exlio|rr|exrr}]|--off] [-y]
fpctl -e health-check-interval [path-health-check-interval]
fpctl -h
```

Description

Displays and changes the settings about the FC path.

This command is applied to the node on which the command is executed. In cluster configurations, this command must be executed on both nodes.

You can execute the command when the status of the node that you are logged in to is `INACTIVE`.

In a single-node configuration, you can execute this command when connected to a storage system.

Options and arguments

`-e auto-online [--on|--off]`

Specify whether to automatically switch an FC path to online when the FC path recovers from an error. If you do not specify `--on` or `--off`, the current setting information applies. The initial setting is `--off`.

When you specify `--on`, frequent transitory errors in an FC path might affect client tasks. These risks must be fully considered before you enable automatic switching of a path to online.

`--on`

Specify this to enable automatic switching of an FC path to `Online`.

`--off`

Specify this to disable automatic switching of an FC path to `Online`.

`-e health-check-interval [ path-health-check-interval ]`

Specify the path health check interval in the range from 1 to 1,440 (unit: minutes). If you omit this option, the current settings are displayed. The initial setting is `30`.

`-e load-balance [--on [--type {exlio|rr|exrr}]|--off]`

Specify whether to use the load balancing function. If you do not specify `--on` or `--off`, the current setting information applies.

To use the load balancing function, select the Extended Least I/Os algorithm, the Round Robin algorithm, or the Extended Round Robin algorithm as the algorithm for switching the FC path. The initial setting is `--on` (extended lio), which means that the algorithm is the Extended Least I/Os algorithm and that the load balancing function is used. If you specify `--off` (the load balancing function is not used), access is concentrated on one FC path, which might degrade performance. The system administrator should set this option only after taking into account the performance risks.

`--on`

Specify this to use the load balancing function.

`--type {exlio|rr|exrr}`

Specify the algorithm to be used for the load balancing function. If you omit this option, the Extended Least I/Os algorithm is specified as the algorithm for switching the FC path.

`exlio`

Specify this to use the Extended Least I/Os algorithm.

`rr`

Specify this to use the round-robin method.

`exrr`

Specify this to use the extended round-robin method.

`--off`

Specify this if you do not want to use the load balancing function.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-171 Information displayed when executing the fpctl command (when the -e auto-online option is specified)

Item	Description

Status	Displays whether to automatically set the FC path online when the FC path is recovered from a failure.
	
	 `On`
	
	     The FC path is automatically set to online status.
	
	 `Off`
	
	     The FC path is not automatically set to online status.

Table 2-172 Information displayed when executing the fpctl command (when the -e load-balance option is specified)

Item	Description

Status	Displays whether the load balancing function is being used. If the load balancing function is being used, the algorithm that is being used is also displayed.
	
	`On(extended lio)`
	
	    The load balancing function is being used and the algorithm is the Extended Least I/Os algorithm.
	
	`On(round-robin)`
	
	    The load balancing function is being used, and the algorithm is the Round Robin algorithm.
	
	`On(extended round-robin)`
	
	    The load balancing function is being used, and the algorithm is the Extended Round Robin algorithm.
	
	`Off`
	
	    The load balancing function is not being used.

Return values

Table 2-173 Return values of the fpctl command

Return value	Description
`0`	Normal termination
`1, 3`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`97, 99, 101, 102`	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To view whether the load balancing function is being used, and if so, the algorithm that is being used:

```
$ sudo fpctl -e load-balance
On(extended lio)
```

To disable use of the load balancing function:

```
$ sudo fpctl -e load-balance --off
KAQM32038-Q Performance might decrease when the load-balance function is
disabled. Do you still want to change the setting? (y/n)
```

fpoffline (Switch an FC path to Offline)

Synopsis

```
fpoffline path
fpoffline --hostport host-port-name
fpoffline --arrayport storage-port-name --model model
    --serial serial-number
fpoffline -h
```

Description

Switches the status of an FC path to `Offline`. Switching FC paths is only possible when a path's alternate path is in the `Online` status. When you specify a host port or an storage port to switch the status of multiple FC paths to `Offline`, all the paths' alternate paths must be in the `Online` status.

Note that, when this command is executed, an FC path health check is performed.

This command is applied to the node on which the command is executed. In cluster configurations, this command must be executed on both nodes.

In a single-node configuration, you can execute this command when connected to a storage system.

Options and arguments

`--arrayport` *storage-port-name*

    If you want to switch the status of all the FC paths that pass through a specific FC port (storage port) in a storage system to `Offline`, specify the name of the storage port. Specify the value of `ArrayPort` that is displayed when the `fpstatus` command is executed.

`--hostport` *host-port-name*

    If you want to switch the status of all the FC paths that pass through a specific FC port (host port) on a node to `Offline`, specify the name of the host port. Specify the value of `HostPort` that is displayed when the `fpstatus` command is executed.

`--model` *model*

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

Specify the model of the storage system to which the target storage port belongs. Specify the value of `Model` that is displayed when the `fpstatus` command is executed.

You can specify one of the following models:

`AMS`

Specify this for the Hitachi AMS2000 series.

`HUS`

Specify this for the HUS100 series.

`HUS_VM`

Specify this for an HUS VM storage system.

`USP_V`

Specify this for a Universal Storage Platform V storage system.

`USP_VM`

Specify this for a Universal Storage Platform VM storage system.

`VSP`

Specify this for a Virtual Storage Platform storage system.

`VSP_G1000`

Specify this for a VSP G1000 storage system.

`VSP_Gx00`

Specify this for a VSP Fx00 model or VSP Gx00 model storage system.

`--serial` *serial-number*

Specify the serial number of the storage system where the target storage port exists. Specify the value of `Serial` that is displayed when the `fpstatus` command is executed.

path

Specify the target FC path. Specify the value of `Path` that is displayed when the `fpstatus` command is executed.

Return values

Table 2-174 Return values of the fpoffline command

Return value	Description
0	Normal termination
1, 2	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 11, 12, 67, 68, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output

Return value	Description
	message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To change the status of the FC path (`path000-0000-0A`) to `Offline`:

```
$ sudo fpoffline path000-0000-0A
```

To change the status of all FC paths that pass through the host port (port name: `fc0001`) to `Offline`:

```
$ sudo fpoffline --hostport fc0001
```

To change the status of all FC paths that pass through the storage port (port name: `1A`, model: `AMS`, serial number: `85011261`) to `Offline`:

```
$ sudo fpoffline --arrayport 1A --model AMS --serial 85011261
```

fponline (Switch an FC path to Online)

Synopsis

```
fponline path
fponline -h
fponline --hostport host-port-name
fponline --arrayport storage-port-name --model model
    --serial serial-number
```

Description

Switches the status of an FC path to `Online`.

Note that, when this command is executed, an FC path health check is performed.

This command is applied to the node on which the command is executed. In cluster configurations, this command must be executed on both nodes.

In a single-node configuration, you can execute this command when connected to a storage system.

Options and arguments

`--arrayport` *storage-port-name*

If you want to switch the status of all the FC paths that pass through a specific FC port (storage port) in a storage system to `Online`, specify the name of the storage port. Specify the value of `ArrayPort` that is displayed when the `fpstatus` command is executed.

`--hostport` *host-port-name*

If you want to switch the status of all the FC paths that pass through a specific FC port (host port) on a node to `Online`, specify the name of the host port. Specify the value of `HostPort` that is displayed when the `fpstatus` command is executed.

`--model` *model*

Specify the model of the storage system to which the target storage port belongs. Specify the value of `Model` that is displayed when the `fpstatus` command is executed.
You can specify one of the following models:

`AMS`

Specify this for the Hitachi AMS2000 series.

`HUS`

Specify this for the HUS100 series.

`HUS_VM`

Specify this for an HUS VM storage system.

`USP_V`

Specify this for a Universal Storage Platform V storage system.

`USP_VM`

Specify this for a Universal Storage Platform VM storage system.

`VSP`

Specify this for a Virtual Storage Platform storage system.

`VSP_G1000`

Specify this for a VSP G1000 storage system.

`VSP_Gx00`

Specify this for a VSP Fx00 model or VSP Gx00 model storage system.

`--serial` *serial-number*

Specify the serial number of the storage system where the target storage port exists. Specify the value of `Serial` that is displayed when the `fpstatus` command is executed.

path

Specify the target FC path. Specify the value of `Path` that is displayed when the `fpstatus` command is executed.

Return values

Table 2-175 Return values of the fponline command

Return value	Description
0	Normal termination
1, 2	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 11, 12, 66, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To change the status of the FC path (`path000-0000-0A`) to `Online`:

```
$ sudo fponline path000-0000-0A
```

To change the status of all FC paths that pass through the host port (port name: `fc0001`) to `Online`:

```
$ sudo fponline --hostport fc0001
```

To change the status of all FC paths that pass through the storage port (port name: `1A`, model: `AMS`, and serial number: `85011261`) to `Online`:

```
$ sudo fponline --arrayport 1A --model AMS --serial 85011261
```

fpstatus (Display the status and configuration of an FC path)

Synopsis

```
fpstatus [-c] [-v] [path]
fpstatus --allnode
fpstatus --lupath
fpstatus -h
```

Description

This command displays the status and configuration of FC paths.

Note that if you execute the `fpstatus` command, a path health check is performed.

In a single-node configuration, you can execute this command when connected to a storage system.

Options and arguments

`--allnode`

For a cluster configuration, specify this to display the status and configuration of the FC paths on both nodes.

For a single configuration, specify this to display the status and configuration of the FC paths on the node.

`-c`

Specify this to display the FC path status separated with colons (`:`).

`--lupath`

For a cluster configuration, specify this to display the information about the LU paths on both nodes. Note that if a cluster has not been configured, the information about LU paths on the logged-in node is displayed.

For a single configuration, specify this to display the information about the LU paths on the node.

`-v`

Specify this to view the model and serial number of the storage system.

path

Specify this to display the status and configuration of a specific FC path. If you omit this option, all the FC paths set in the node to which you are logged in are displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-176 Information displayed when executing the fpstatus command

Item	Description
Path	Displays the FC path. If the target cannot be identified, – is displayed. Note that this item is not displayed when the `--lupath` option is specified.
Target	Displays the target. If the target cannot be identified, – is displayed.

Item	Description
HostPort	Displays the name of the FC port (host port) on the node in the following format: fc *Hexadecimal-notation* If the FC port cannot be identified, - is displayed.
HostPortWWN	Displays the WWN of the FC port on the node.
ArrayPort	Displays the name of the FC port (storage port) in a storage system.
ArrayPortWWN	Displays the WWN of the FC port in the storage system. If the FC port cannot be identified, ---------------- is displayed. Note that this item is not displayed when the --lupath option is specified.
Model	Displays the storage system model. A hyphen (-) is displayed in the following cases: • Storage system whose LU is not operated in the HDI system • The information of the storage system has not been acquired because a problem occurred on the FC path during the node OS start time, or for some other reason. This item is displayed when the --allnode, --lupath, or -v option is specified.
Serial	Displays the serial number of the storage system. A hyphen (-) is displayed in the following cases: • Storage system of an unsupported model • Storage system whose LU is not operated in the HDI system • The information of the storage system has not been acquired because a problem occurred on the FC path during the node OS start time, or for some other reason. This item is displayed when the --allnode, --lupath, or -v option is specified.
Status	Displays the status of the FC path. Online The FC path is running normally. If a device file error has been detected, Online (LU Error) is displayed. Offline The system administrator has placed the FC path in the offline status. If a device file error has been detected, Offline (LU Error) is displayed. Error Any of the following conditions exists: - An error occurred in the FC path. - None of the device files belonging to the target FC path can be accessed.

Item	Description
	- No LU is allocated to the host group that was associated with the FC path.
	`Partially Online`
	Although the FC path is running normally, some device files cannot be accessed. If a device file error has been detected, `Partially Online (LU Error)` is displayed.
	`Configuration Mismatch`
	Allocation of LUs to the host groups associated with the FC path differs from the allocation for the alternate path, or there is no alternate path.
	`Unknown`
	The FC port of the node (host port) or the FC port of the storage system (storage port) cannot be identified.
`LDEV( hex)`	Displays the LDEV number of the device file. The value in parentheses is the corresponding hexadecimal value.
	If an LDEV number is not assigned to a user LUN, a hyphen (-) is displayed.
	This item is displayed when the `--lupath` option is specified.
`Mismatch`	Displays whether an alternate path for an LU path is set.
	`-`
	A hyphen (-) is displayed when an alternate path exists.
	`*`
	An asterisk (*) is displayed when an alternate path does not exist.
	This item is displayed when the `--lupath` option is specified.

Return values

Table 2-177 Return values of the fpstatus command

Return value	Description
`0`	Normal termination
`1, 2`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10`[#]`, 65`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`10`[#]`, 70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

fsautofo (Manage the automatic failover functionality used when a file system is blocked)

Synopsis

```
fsautofo [-s|-u] -a
fsautofo [-s|-u] file-system-name[ file-system-name...]
fsautofo -h
```

Description

Enables or disables automatic failovers, which occur when a file system is blocked due to an error in the software.

When the HDI system is first installed, automatic failover is enabled so that failover occurs if a file system becomes blocked. Change this setting as required, depending on how the HDI system is to be used.

If you omit the -s and -u option, the automatic failover settings are displayed separately for each file system.

If you execute this command while processing for a cluster, node, or resource group is in progress, the automatic failover setting might not complete normally. Execute the command so as to avoid contention with cluster, node, or resource group operations.

Options and arguments

-a

Specify this option if you want to enable or disable automatic failover for all file systems mounted on the node you are logged in to. If the command processing fails for any file system, processing continues for the other file systems.

-s

Specify this option to enable automatic failover when a file system is blocked.

-u

Specify this option to disable automatic failover so that failover does not occur when a file system is blocked.

file-system-name [*file-system-name* ...]

Specify the file system names if you want to enable or disable automatic failover for specific file systems. You can specify an asterisk (*) or question mark (?) as a wildcard. Separate multiple file system names with spaces.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-178 Information displayed when executing the fsautofo command

Item	Description
file-system-name	Displays the file system name.

status	Displays whether automatic failover that occurs when the file system is blocked is enabled.
	
	On
	
	    Automatic failover is enabled.
	
	Off
	
	    Automatic failover is disabled.

Return values

Table 2-179 Return values of the fsautofo command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Example

To enable automatic failover for all the file systems mounted on the node you are logged in to, so that failover occurs when one of the file systems is blocked:

```
$ sudo fsautofo -s -a
```

fscreate (Create a file system)

Synopsis (for cluster configurations)

```
fscreate [-i inode]
    [-l log-size] [-d division-size]
    [-v {use|do_not_use}] [-c {on|off}]
    [-t {classic|advanced}]
    [-p [-P stripe-size]] [-r resource-group-name]
    [-w [-M maximum-retention-period] [-m minimum-retention-period]
     [-a {auto|manual|on|off} [-A auto-commit-period]
      [-D default-retention-period]]
     [-R {allow|deny}]]
    [-L {allow|deny}]
    [--hcp {ro --namespace-fqdn namespace-FQDN
      [--ex-hcp-host host-name-that-has-been-made-external-and-is-
       used-to-connect-to-the-HCP]
      [--hcp-replica-host host-name-of-the-replica-HCP
       [--ex-hcp-replica-host host-name-that-has-been-made-external-
        and-is-used-to-connect-to-the-replica-HCP]]
     --hcp-account user-name --hcp-password password |
     roaming --namespace namespace-name
     [--no-accesstest] |
     sharing --namespace namespace-name
     [--no-accesstest]}]
    [--versioning {use|do_not_use}]
    [--period-to-hold past-version-retention-period]
    [--custom-schedule {use|do_not_use}]
    [--schedule-setting schedule[,schedule...]]
    [--bypass {on|off}]
    [-y]
    file-system-name
    dev-name[,dev-name...]
```

Synopsis (for single node configurations)

```
fscreate [-i inode]
    [-c {on|off}] [-t {classic|advanced}]
    [-w [-M maximum-retention-period] [-m minimum-retention-period]
     [-a {auto|manual|on|off} [-A auto-commit-period]
      [-D default-retention-period]]
     [-R {allow|deny}]]
    [-L {allow|deny}]
    [--hcp {ro --namespace-fqdn namespace-FQDN
      [--ex-hcp-host host-name-that-has-been-made-external-and-is-
```

```
   used-to-connect-to-the-HCP]
    [--hcp-replica-host host-name-of-the-replica-HCP
     [--ex-hcp-replica-host host-name-that-has-been-made-external-
      and-is-used-to-connect-to-the-replica-HCP]]
  --hcp-account user-name --hcp-password password |
  roaming --namespace namespace-name
  [--no-accesstest] |
  sharing --namespace namespace-name
  [--no-accesstest]}]
 [--versioning {use|do_not_use}]
 [--period-to-hold past-version-retention-period]
 [--custom-schedule {use|do_not_use}]
 [--schedule-setting schedule[,schedule...]]
 [--vgr volume-group-name]
 [--bypass {on|off}]
 [-y]
 -s file-system-capacity
 file-system-name
```

Synopsis (to reference the command syntax)

```
fscreate -h
```

Description

Creates a file system. The maximum total size of device files is 1 PB. The limit on the total number of file systems is 256 per single node, and 511 per cluster.

Note that if you use a volume manager, part of the area of each device file is used as the management region. This means that there is a difference between the total size of the device files and the size available for the file system.

After a file system has been created, its capacity can be expanded. However, the maximum capacity after expansion varies depending on the initial capacity of the file system. The following table lists the initial capacity of a created file system and the maximum possible capacity after expansion.

Table 2-180 Initial capacity of a created file system and the maximum capacity after expansion

Initial capacity of a created file system (m: initial file system capacity)	Maximum capacity after expansion
128 MB <= m < 128 MB + 16 MB	2 TB
128 MB + 16 MB <= m < 256 MB + 16 MB	4 TB
256 MB + 16 MB <= m < 512 MB + 16 MB	8 TB
512 MB + 16 MB <= m < 1 GB + 16 MB	16 TB
1 GB + 16 MB <= m < 2 GB + 16 MB	32 TB
2 GB + 16MB <= m < 4 GB + 16 MB	64 TB
4 GB + 16 MB <= m < 8 GB + 16 MB	128 TB

Initial capacity of a created file system (m: initial file system capacity)	Maximum capacity after expansion
8 GB + 16 MB <= m < 16 GB + 16 MB	256 TB
16 GB + 16 MB <= m < 32 GB + 16 MB	512 TB
32 GB + 16 MB <= m < 1 PB	1 PB

Note:

If the `-d` option is used to specify a file system division size, the maximum expanded capacity of file systems is different from that shown above. For details about the maximum expanded capacity of file systems when the division size is specified, see .

Options and arguments

`-a {auto|manual|on|off}`

Use this command to specify whether to enable the autocommit function (which automatically turns a file not changed in the specified period into a WORM file) in auto mode or manual mode for WORM file systems. You cannot disable the autocommit function after enabling it.

Specify this option together with the `-w` option. If you specify this option to enable the autocommit function, a confirmation message is output. If you omit this option, `off` is set.

`auto`

Specify this option to enable the autocommit function in auto mode.

In auto mode, all ordinary files, except for the system files and files in the system directories, are subject to the autocommit functionality.

`manual` or `on`

Specify this option to enable the autocommit function in manual mode.

In manual mode, files that are specified as read-only files by clients are subject to the autocommit functionality.

`off`

Specify this to disable the autocommit function.

`-A` *auto-commit-period*

Specify the wait period for turning a file into a WORM file in the following format. After you have specified the setting, you cannot change it.

days-hours-minutes

Specify a value in the range from 1 minute to 36,500 days.

Specify the `-w` option and the `-a` option with `auto`, `manual`, or `on` specified. If you omit this option, `0-0-15` (15 minutes) is set.

For linkage with the HCP, you must set this option so that the autocommit period is shorter than the execution interval of migration.

`--bypass {on|off}`

Specify whether to enable the CIFS bypass traverse checking function. If you omit this option, `on` is set. However, if you omit this option and specify the `--hcp roaming` option, `off` is set.

`on`

Specify this option to enable the CIFS bypass traverse checking function. You cannot specify this argument together with the `--hcp roaming` option.

`off`

Specify this option to disable the CIFS bypass traverse checking function.

`-c {on|off}`

Specify whether to record the file creation time in the file system. If you omit this option, `off` is set. Specify `on` if you intend to create and use CIFS shares in the file system you are creating.

`on`

Records the file creation time.

`off`

Does not record the file creation time.

If NFS shares are to be created and used in the file system, the file creation times cannot be viewed from the NFS clients even if you specify `on`.

`--custom-schedule {use|do_not_use}`

Specifies whether the custom schedule is to be used. If you omit this option, `do_not_use` is set.

`use`

Specify this to use the custom schedule. Specify this option together with the `--schedule-setting` option.

`do_not_use`

Specify this if you do not want to use a custom schedule.

This option cannot be specified with the following options: `--hcp ro, --versioning do_not_use`

`-d` *division-size*

Specify a file system division size that is appropriate to the file system size. If you omit this option, the system automatically sets a file system division size appropriate for the file system capacity (recommended). If you do not sets a file system division size automatically , it may influence the performance.

When specifying a division size, you must specify the first character of the unit. For example, specify 128M for a division size of 128 MB and 4G for a division size of 4 GB.

The table below describes the specifiable division sizes and the default settings.

Table 2-181 Specifiable file system division sizes and default settings

File system capacity (m: File system capacity)	Specifiable file system division size	Default setting
128 MB <= m < 128 MB + 16 MB	64 MB	64 MB
128 MB + 16 MB <= m < 256 MB + 16 MB	128 MB,64 MB	128 MB
256 MB + 16 MB <= m < 512 MB + 16 MB	256 MB,128 MB,64 MB	256 MB
512 MB + 16 MB <= m < 1 GB	512 MB,256 MB,128 MB,64 MB	512 MB
1 GB <= m < 1 GB + 16 MB	512 MB,256 MB,128 MB	512 MB
1 GB + 16 MB <= m < 2 GB	1 GB,512 MB,256 MB,128 MB	1 GB
2 GB <= m < 2 GB + 16 MB	1 GB,512 MB,256 MB	1 GB
2 GB + 16 MB <= m < 4 GB	2 GB,1 GB,512 MB,256 MB	2 GB
4 GB <= m < 4 GB + 16 MB	2 GB,1 GB,512 MB	2 GB
4 GB + 16 MB <= m < 8 GB	4 GB,2 GB,1 GB,512 MB	4 GB
8 GB <= m < 8 GB + 16 MB	4 GB,2 GB,1 GB	4 GB
8 GB + 16 MB <= m < 16 GB	4 GB,2 GB,1 GB	8 GB
16 GB <= m < 16 GB + 16 MB	4 GB,2 GB	8 GB
16 GB + 16 MB <= m < 32 GB	4 GB,2 GB	16 GB
32 GB <= m < 32 GB + 16 MB	4 GB	16 GB
32 GB + 16 MB <= m < 64 GB + 16 MB	4 GB	32 GB
64 GB + 16 MB <= m < 128 GB + 16 MB	4 GB	64 GB
128 GB + 16 MB <= m < 16 TB	4 GB	128 GB
m <= 16 TB	--	128 GB

Legend:

   <=: Less than or equal to, --: Cannot be specified.

Note:

The specified division size determines the maximum capacity to which the file system can be expanded. The table below describes the relationship between the division size and the maximum capacity of the expanded file system.

Table 2-182 Relationship between the division size and the maximum capacity of the expanded file system

Division size	File system capacity (maximum)
64 MB	2 TB
128 MB	4 TB
256 MB	8 TB
512 MB	16 TB
1 GB	32 TB
2 GB	64 TB
4 GB	128 TB

-D *default-retention-period*

Specify, in the following format, the retention period to be set for the file for which the autocommit function was executed.

days-hours-minutes

Specify a value in the range from 1 minute to 36,500 days.

If you want to set an infinite default retention period, specify `infinite`. Specify the -w option and the -a option with `auto`, `manual`, or `on` specified. If you omit this option, `10-0-0` (10 days) is set. However, if `infinite` is specified for the minimum retention period, `infinite` is set.

You must specify a default retention period that is equal to or greater than the minimum retention period, and that is equal to or smaller than the maximum retention period.

--ex-hcp-host *host-name-that-has-been-made-external-and-is-used-to-connect-to-the-HCP*

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. Specify this together with the --hcp ro option and the --namespace-fqdn option. If you omit this option, no host name or IP address is set.

--ex-hcp-replica-host *host-name-that-has-been-made-external-and-is-used-to-connect-to-the-replica-HCP*

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. Specify this option together with --hcp ro, --namespace-fqdn, and --hcp-replica-host. if you omit this option, no host name or IP address is set.

--hcp {ro|roaming|sharing}

Specify the method for sharing HCP data migrated from other HDI systems.

ro

Specify this option if the data from other HDI systems is to be referenced as read-only. This argument also automatically checks whether the namespace specified for the `--namespace-fqdn` option can be accessed. This argument cannot be specified when the `--period-to-hold` option or `--versioning use` option is specified.

roaming

Specify this option to enable roaming among HDI systems for the data from the home directory created for each end-user. This argument also automatically checks whether the namespace specified for the `--namespace` option can be accessed. This argument cannot be specified when the `--bypass on` option or `-w` option is specified.

sharing

Specify this option if the data is shared among HDI systems using the read-write-content-sharing functionality. This argument also automatically checks whether the namespace specified for the `--namespace` option can be accessed. This argument cannot be specified when the `-w` option is specified.

If you do not want to synchronizing the data with other HDI systems via linked HCP systems, create the file system first, and then configure migration settings by using the Migration Tasks dialog box.

`--hcp-account` *user-name*

Specify the user name used to access a namespace in an HCP system. Specify this option together with the `--hcp ro` option.

`--hcp-password` *password*

Specify the password of a user who can access a namespace in an HCP system. Specify this option together with the `--hcp ro` option.

`--hcp-replica-host` *host-name-of-the-replica-HCP*

Specify in FQDN format the host name of the replica HCP system. Specify this option together with the `--hcp ro` option. If this option is omitted, the host name of the replica HCP system is not set.

`-i` *inode*

Specify the capacity of an inode, as a percentage of the file system capacity. Specify a value from 1 to 100. If you omit this option, it defaults to 25. The maximum capacity that can be used as an inode is 1 TB.

`-l` *log-size*

Specify the size of space to be used for logging (in MB). Specify a value from 2 to 128. Specify a value smaller than the file system division size specified in the `-d` option.

If you omit this option, the most appropriate value is set based on the file system capacity.

`-L {allow|deny}`

Specify whether to allow the creation of hard links on the file system that is to be created.

`allow`

> Specify this to allow the creation of hard links. Note that if `allow` is set for a file system, and then information regarding a migration-destination HCP system is specified, this setting is changed to `deny`.

`deny`

> Specify this to deny the creation of hard links.

`-m` *minimum-retention-period*

> Specify the minimum retention period for a WORM file system in the following format:
>
> *days-hours-minutes*
>
> Specify a value in the range from 0 minutes to 36,500 days.
>
> If you want to set an infinite minimum retention period, specify `infinite`. Specify this together with the `-w` option. If you omit this option, `0-0-0` (0 minutes) is set.
>
> You must specify a minimum retention period that is equal to or smaller than the maximum retention period. In addition, if you enable the autocommit function, you must specify a minimum retention period that is equal to or smaller than the default retention period.

`-M` *maximum-retention-period*

> Specify the maximum retention period for a WORM file system in the following format:
>
> *days-hours-minutes*
>
> Specify a value in the range from 1 minute to 36,500 days.
>
> If you want to set an infinite maximum retention period, specify `infinite`. Specify this together with the `-w` option. If you omit this option, `10950-0-0` (10,950 days, approximately 30 years) is set. Note, however, that if you specify `infinite` for the minimum retention period or default retention period, `infinite` is set.
>
> You must specify a maximum retention period that is equal to or greater than the minimum retention period. In addition, if you enable the autocommit function, you must specify a maximum retention period that is equal to or greater than the default retention period.

`--namespace` *namespace-name*

> Specify the name of the HCP namespace. Specify this option together with the `--hcp roaming` or `--hcp sharing` option.

`--namespace-fqdn` *namespace-FQDN*

> Specify the name of the HCP namespace in FQDN format. Specify this option together with the `--hcp ro` option.

`--no-accesstest`

Specify this when the HDI system does not need to check whether it can access the HCP namespace. Specify this option together with the `--hcp roaming` or `--hcp sharing` option.

`-p`

Specify this to create a file system that has a striped configuration.

`-P` *stripe-size*

Specify a stripe size (unit: KB) when you create a file system that has a striped configuration. Specify this option together with the `-p` option. You can specify `8`, `16`, `32`, `64`, `128`, `256`, `512`, or `1024`. If you omit this option, `64` is used.

`--period-to-hold` *past-version-retention-period*

Specify the number of days the past version of files migrated to the HCP system is retained. Specify a value in the range from 1 to 36,500. If you omit this option, `7` is set.

You cannot specify this option together with the `--hcp ro` and `--versioning do_not_use` option.

`-R` {allow|deny}

Specify whether to allow the renaming of empty directories in WORM file systems. If you omit this option, `deny` is set. This option must be specified with the `-w` option.

`allow`

Allows empty directories to be renamed.

`deny`

Prevents empty directories from being renamed.

`-r` *resource-group-name*

Specify the name of the resource group in which to register the file system to be created. When executing the command with a virtual IP address specified, specify the name of a resource group with the `-r` option in case of a failover.

If you omit this option, the file system is registered in the resource group that belongs to the node you are logged in to.

`-s` *file-system-capacity*

This option can be used in single-node configurations. Specify the file system capacity (units: GB). You can specify a value from 1 to the user disk free capacity. Specify a value from 1 to the available capacity of the volume group.

`--schedule-setting` *schedule*[,*schedule*...]

Specifies settings for the custom schedule. Specify this option together with the `--custom-schedule` option. To specify multiple schedules, separate each schedule by using commas (`,`).

When using this option, note the following points:

- If the custom schedule is used, you cannot specify `0` for all time units. Specify a value other than `0` for at least one time unit.

- Be sure to specify a number of days greater than or equal to the recommended value calculated by the formula for the retention period of the past-version directories.

For details about custom scheduling of the file version restore functionality or the formula for recommended values of the retention period, see the *Installation and Configuration Guide*.

The following table describes the format for specifying custom schedules in this option.

Table 2-183 Format for specifying custom schedules by using the fscreate command

Specification format	Description
`m`–*minutes*	The oldest past version directory with 15-minute time units (hour *n*, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. For *minutes*, specify 0, 15, 30, 45, or 60. If you specify 0, schedules with 15-minute time units become invalid.
`h`–*hours*	The oldest past version directory with hourly time units (hour n, minutes 00 to 59) is kept for the number of units specified. For *hours*, specify in the range from 0 to 48. If you specify 0, schedules with hourly time units become invalid.
`D`–*days*	The oldest past version directory with daily time units (day *n*, 00:00 to 23:59) is kept for the number of units specified. For *days*, specify in the range from 0 to 62. If you specify 0, schedules with daily time units become invalid.
`W`–*weeks*	The oldest past version directory with weekly time units (week *n*, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. For *weeks*, specify in the range from 0 to 156. If you specify 0, schedules with weekly time units become invalid.
`M`–*months*	The oldest past version directory with monthly time units (month *n*, 1st day, 00:00 to *last-day*, 23:59) is kept for the number of units specified. For *months*, specify in the range from 0 to 72. If you specify 0, schedules with monthly time units become invalid.
`Y`–*years*	The oldest past version directory with yearly time units (year *n*, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. For *years*, specify in the range from 0 to 100.

Specification format	Description
	If you specify 0, schedules with yearly time units become invalid.

-t {classic|advanced}

Specify the ACL type of the file system. If you omit this option, classic will be set by default. Note that if you create a WORM file system with the -w option specified, you will not be able to change the ACL type.

classic

Specify this if you want to create a file system of the Classic ACL type.

advanced

Specify this if you want to create a file system of the Advanced ACL type. Once the file system is created with the Advanced ACL type specified, you cannot change the ACL type to the Classic ACL type.

Note that when you create a file system of the Advanced ACL type, the following ACE is set.

Table 2-184 ACE that is set when a file system of the Advanced ACL type is created

Item	Settings
User	Everyone
Account type	Group
Application destination	This folder, subfolders, and files
Inheritance range	All folders and files under this folder
ACE type	Allow
Access permission	Full Control

Note that if you create a WORM file system with the -w option specified, you will not be able to change the ACL type.

-v {use|do_not_use}

Specify whether to use a volume manager. When you create a file system from multiple device files, specify use. If you omit this option, it defaults to use.

use

Specify this if you want to use a volume manager.

do_not_use

Specify this if you do not want to use a volume manager.

--versioning {use|do_not_use}

Specify whether to allow clients to access the past version of files migrated to the HCP system. If you omit this option, use is set. Note,

however, that if you omit this option when `ro` is specified for the `--hcp` option, `do_not_use` is set.

`use`

> Specify this to allow clients to access the past version of files migrated to the HCP system. You cannot specify this argument together with the `--hcp ro` option.

`do_not_use`

> Specify this to prohibit clients from accessing the past version of files migrated to the HCP system. You cannot specify this argument together with the `--period-to-hold` option.

`--vgr` *volume-group-name*

> This option can be used in single-node configurations. You can omit this option if only one volume group has been created.

`-w`

> Specify this to create a WORM file system. You cannot specify this option when the `--hcp roaming` and `--hcp sharing` option is specified.

> Note that if you create a WORM file system, you can no longer change it.

file-system-name

> Specify the name of the file system to be created. Specify a unique name within a cluster. Specify a string of no more than 16 characters consisting of alphanumeric characters and underscores (_).

dev-name `[`, *dev-name* `...]`

> Specify the names of device files to be used in the file system. For example, if the device file path is `/dev/enas/lu01`, specify `lu01`. If you want to create a file system that consists of multiple device files using a volume manager, separate the device file names with commas (,). Specify the device files of one storage system.

> When using a volume manager, specify an LU of no less than 65 MB. If virtual LUs will be used, the total size of the selected device files must be at least 256 MB. If virtual LUs will not be used, the total size of the selected device files must be at least 130 MB.

> When you to create a file system that has a striped configuration, specify 2 to 128 device files of the same size. The number of specified device files is the number of stripes. Striping is performed in the order of the specified device files.

Return values

Table 2-185 Return values of the fscreate command

Return value	Description
0	Normal termination

Return value	Description
1, 10#	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10#, 66#, 70, 74, 75, 76, 77	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66#, 68, 99#	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71, 72, 73	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99#	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Examples

To create a file system according to the following conditions:

- The maximum capacity that can be used as an inode is 50% of the file system capacity.
- A volume manager is to be used.
- File creation times are to be recorded.
- The ACL type of the file system is Advanced ACL.
- A striped configuration is used.
- The file system name is FS_1.
- The device files /dev/enas/lu2B and /dev/enas/lu3C are to be used.

```
$ sudo fscreate -i 50 -v use -c on -t advanced -p FS_1 lu2B,lu3C
```

To create a WORM file system according to the following conditions:

- The maximum capacity that can be used as an inode remains the same as the initial setting.
- A volume manager is to be used.
- The date and time that a file is created are not to be recorded.
- The ACL type of the file system is Advanced ACL.
- The maximum retention period is 30 years (10,950 days).

- The minimum retention period is 1 year (365 days).
- The autocommit function is enabled.
- The autocommit period is 30 minutes.
- The default retention period is 10 years (3,650 days).
- The file system name is `FS_2`.
- The device file `/dev/enas/lu01` is to be used.

```
$ sudo fscreate -v use -c off -t advanced -w -M 10950-0-0 -m 365-0-0 -a on
-A 0-0-30 -D 3650-0-0 FS_2 lu01
```

fsctl (Manage an active file system)

Synopsis

```
fsctl -f [-s|-u]
    {-a|file-system-name[ file-system-name...]}
fsctl -m [-s [-o monitoring-target=warning-threshold
    [,monitoring-target=warning-threshold]|-u]]
    {-a|file-system-name[ file-system-name...]}
fsctl -m [-s [-o monitoring-target=warning-threshold
    [,monitoring-target=warning-threshold]]
    [-O monitoring-target=warning-threshold
    [,monitoring-target=warning-threshold]|-u]]
    file-system-name[ file-system-name...]
fsctl -c [-s|-u] [-o create_time|-o advanced_acl]
    {-a|file-system-name[ file-system-name...]}
fsctl -c -x
    file-system-name[/directory-name[/directory-name...]]
    [ file-system-name[/directory-name[/directory-name]...]...]
fsctl -c -x -o advanced_acl [-p priority]
    file-system-name[ file-system-name...]
fsctl -c -s -o advanced_acl_overwrite_rename={allow|deny}
    {-a|file-system-name[ file-system-name...]}
fsctl -c -o advanced_acl_overwrite_rename
    {-a|file-system-name[ file-system-name...]}
fsctl -c -x -o add_exeauth[=suffix[,suffix...]]
    file-system-name[/directory-name[/directory-name...]]
    [ file-system-name[/directory-name[/directory-name]...]...]
fsctl -l {-a|file-system-name[ file-system-name...]}
fsctl -U [on|off]
fsctl -i
fsctl -h
```

Description

Manages the following settings for specific file systems:

- Enables or disables automatic failovers, which occur when a file system is blocked due to an error in the software (`-f` option).[#]

The same operations can be performed as with the `fsautofo` command.

- Enables and disables warning notification that is sent when file system usage exceeds a threshold value (`-m` option).[#]

  The same operations can be performed as with the `fsfullmsg` command.

- Enables and disables recording of the creation time for files in the file system (`-c` option).[#]

  This command can also set creation times for files (`-x` option).

- Converts the ACL type of files in a file system from the Classic ACL type to the Advanced ACL type (`-o advanced_acl` option).

- Enables or disables existing files and directories with duplicate names to be overwritten when you move other files and directories of the Advanced ACL type file system from an NFS client or FTP client, or when you rename files and directories (the `-o advanced_acl_overwrite_rename` option).

- Adds the execution access permissions to the files (`-o add_exeauth` option).

  Before you change the type of file system from the Classic ACL type to the Advanced ACL type, execute this command.

- Displays the access suppression status for a file system (`-l` option).

[#]

- If you omit both the `-s` option and `-u` option, the current settings are displayed for each file system.
- You can also change settings in interactive mode (`-i` option).

Options and arguments

`-a`

Specify this option if you want to enable or disable automatic failover for all file systems mounted on the node to which you are logged in. If the command processing fails for any file system, processing continues for the other file systems.

`-c`

Specify this option to enable or disable extended attributes for the file system, or to view the extended attribute settings.

`-f`

Specify this option to enable or disable automatic failover that occurs when a file system is blocked, or to view the automatic failover settings.

`-i`

Specify this option to execute this command in interactive mode.

`-l`

Specify this option to display the access suppression status for a file system.

`-m`

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

Specify this option to enable or disable the warning notification that is sent when file system usage exceeds a threshold value, or to view the warning notification settings.

-o add_exeauth[= *suffix* [, *suffix* ...]]

Specify this option to add the execution access permissions to the files that have specified extensions. If you fail to specify the extensions, `exe` or `bat` will be set as the extensions. Specify this option together with the `-c` and `-x` options.

No more than 6 characters (without a period (.)) can be specified for an extension. The maximum number of specifiable extensions is 128.

If you do not add the execution access permissions to the files before you change the type of file system from the Classic ACL type to the Advanced ACL type, you will be unable to execute the files that you were able to execute by the CIFS client before the change.

Also note that if the parent directory does not have the execution access permissions, and you add the execution access permissions to the files, the access permissions will differ between the parent directory and the files even though they used to have the same access permissions settings.

Note:

This option cannot be used for WORM file systems.

-o advanced_acl

Specify this option to convert the ACL type of files in a file system from the Classic ACL type to the Advanced ACL type, or to view the ACL type of a file system. Specify this option together with the `-c` and `-x` options.

Note:

Before converting the ACL type of files, you must stop the target file system. If a client moves a file during conversion of the ACL type, the ACL type of that file might not be converted. (However, the ACL type of this file will be converted automatically the next time that a client accesses the file.) In addition, this option cannot be used for WORM file systems.

-o advanced_acl_overwrite_rename[=allow|=deny]

Specify this option to set whether existing files and directories with duplicate names of the Advanced ACL type file system are overwritten when other files and directories are moved from an NFS client or FTP client, or when you rename files and directories. Specify this option together with the `-c` and `-s` options.

=allow

Specify this to allow existing duplicate files and directories to be overwritten when you have the delete permission for those files and directories.

=deny

Specify this to disable the overwriting of duplicate files and directories.

If you execute the command without specifying the values `=allow` and `=deny`, you can view the current setting for the specified Advanced ACL type file system. Specify this option together with the `-c` option.

`-o create_time`

Specify this to enable or disable recording of the creation time for files in the file system, or to view the creation time settings. Specify this option together with the `-c` option.

`-o` *monitoring-target* = *warning-threshold* [, *monitoring-target* = *warning-threshold*]

Specify this option together with the `-m` option and the `-s` option. Specify a parameter to be monitored and a threshold value for issuing a warning. If you omit this option, the current setting information applies.

If you specify `0` as the threshold value, a warning will be issued only when file system usage reaches the upper limit.

`blimit=` *warning-threshold*

Specify the warning threshold value in bytes or as a percentage (`%`) when you monitor file system usage by the number of blocks used. Note that if this option is specified, the file system usage is monitored when using blocks, and the warning threshold value is output in bytes or as a percentage (`%`).

To specify the value in bytes:

Specify a number followed by the letter `M`, `G`, or `T` for the unit (`M`: MB; `G`: GB; `T`: TB).

If the unit is MB: `blimit=500M`

If the unit is GB: `blimit=5G`

If the unit is TB: `blimit=1T`

To specify the value as a percentage (`%`):

Specify a number followed by the letter `P` (upper case).

Example: `blimit=80P`

The warning threshold is set from the specified percentage (`%`) of the file system capacity.

If you expand the file system, the warning threshold is re-calculated according to the increase in the file system capacity. Therefore, the warning threshold is automatically expanded when you expand the file system.

If you specify a number followed by the letter `p` (lower case), the byte count calculated from the specified percentage of the file system capacity at the time of command execution will be set as the warning threshold. The warning threshold is not re-calculated when you expand the file system.

`ilimit=` *warning-threshold*

If you are monitoring file system usage by the number of inodes, specify the warning threshold value as a number or percentage (`%`) of inodes that are in use. Note that if this option is specified, the file

system usage is monitored at every one hour, and the warning threshold is output as the number of inodes or as a percentage (%).

To specify the value as the number of inodes:

Example: `ilimit=9000`

To specify the value as a percentage (%):

Specify a number followed by the letter `P` (upper case).

Example: `ilimit=80P`

The warning threshold is set from the specified percentage (%) of the inode capacity that has been specified when the file system was created.

If you expand the file system, the warning threshold is re-calculated according to the increase in the inode capacity. Therefore, the warning threshold is automatically expanded if the inode capacity is expanded. The warning threshold is only calculated when you create or expand the file system, whereas the total number of usable inodes changes dynamically depending on the file system usage.

If you specify a number followed by the letter `p` (lower case), the inode count, which is calculated from the specified percentage of the total number of usable inodes at the time of command execution, will be set as the warning threshold. Therefore, the warning threshold is not re-calculated when you expand the file system. Similarly, the warning threshold is not re-calculated when the total number of usable inodes changes dynamically based on the file system usage.

`-O` *monitoring-target* = *warning-threshold* [, *monitoring-target* = *warning-threshold*]

This option is not supported.

`-p` *priority*

Specify the priority of the processing for converting the ACL type of files in a file system from the Classic ACL type to the Advanced ACL type. Specify this option together with the `-c`, `-x`, and `-o advanced_acl` options.

`high`

Specify this to give higher priority than usual to the processing to quickly complete the conversion.

`low`

Specify this to give lower priority than usual to the processing so that the conversion does not interrupt other processes.

`-s`

Specify this option in the following cases:

○ With the `-f` option to enable automatic failover that occurs when a file system is blocked.

○ With the `-m` option to enable the warning notification that is sent when file system usage exceeds a threshold value.

- With the `-c` option to enable recording of the creation time for files in the file system.

`-u`

Specify this option in the following cases:

- With the `-f` option to disable automatic failover that occurs when a file system is blocked.
- With the `-m` option to disable the warning notification that is sent when file system usage exceeds a threshold value.
- With the `-c` option to disable recording of the creation time for files in the file system.

`-U {on|off}`

Specify whether to perform background deletion on files that take time to delete in file systems.

This option applies to all file systems on a node. If this option is omitted, the current setting is displayed.

`on`

Specify this to enable background deletion of files.

`off`

Specify this to disable background deletion of files.

`-x`

Specify this option in the following cases:

- Specify this option together with the `-c` option to set the creation time for files.

  The oldest of the times for last access (`atime`), last change (`ctime`), and last modification (`mtime`) is set as the creation time. The command processing time is approximately one minute to set the creation times for 100,000 files.

  Note that, even if the file system is set so as to record the file creation time, the time cannot be viewed from an NFS client.

- Specify this option together with the `-c` and `-o advanced_acl` options to convert the ACL type of the files from the Classic ACL type to the Advanced ACL type. The command processing time is approximately ten minutes to convert the ACL type of 100,000 files.

- Specify this option together with the `-c` and `-o add_exeauth` options to add the execution access permissions to the files. The command processing time is approximately two minutes to add the execution access permissions to 100,000 files.

When you execute the command, `Wait ...` is displayed. A period (.) is displayed each time 10,000 files are processed.

If the command being executed with this option specified is interrupted, files with different settings might exist in the specified file system. You must therefore execute the command again with the same options specified.

file-system-name[/*directory-name*[/*directory-name*...]]

> If you want to execute the command for a specific file system, specify the name of the file system. If you want to execute the command for specific directories, specify their relative paths from the mount-point directory. For example, to execute the command for the `/mnt/FS1/dir01` directory, specify `FS1/dir01`.
>
> To specify multiple directories, separate each directory with a space. You can use asterisks (`*`) and question marks (`?`) as wildcard characters.
>
> To specify a space in a directory name string, use the appropriate escape character for the remote host environment. To specify an asterisk (`*`) or question mark (`?`) in a directory name string, add a backslash (`\`) before the asterisk (`*`) or question mark (`?`), and then use the appropriate escape character for the remote host environment.

Subcommands

You can display the associated prompt by specifying `autofo`, `fullmsg`, or `extfunc` after `func`. An execution example in interactive mode and the subcommands are described below.

Line	Example
1	`$ sudo fsctl -i`
2	`fsctl> func fullmsg`
3	`fsctl fullmsg> list filesystem1` `  filesystem1      Off(50G,50000)`
4	`fsctl fullmsg> set -o blimit=80G,ilimit=80000 filesystem1`
5	`fsctl fullmsg> exit`
6	`fsctl> exit`

1: Executes the `fsctl` command in interactive mode.

2: Calls for a subcommand to enable or disable warning notification that is sent when file system usage exceeds a threshold value.

3: Displays the settings for file system `filesystem1`.

These are the settings for file system `filesystem1`.

4: Sets a warning threshold value for file system `filesystem1`.

5: Ends the subcommand for the enabling/disabling warning notification that is sent when the file system usage exceeds a threshold value.

6: Ends the `fsctl` command.

`exit`

> Specify this if you want to end the `fsctl` command or its subcommand.

`func autofo`

Specify this to enable or disable automatic failover that occurs when a file system is blocked, or to view the automatic failover settings. When the prompt is displayed, you can execute subcommands in the following formats:

```
list {-a|file-system-name[ file-system-name...]}
set {-a|file-system-name[ file-system-name...]}
unset {-a|file-system-name[ file-system-name...]}
```

list

Displays whether automatic failover is enabled or disabled.

set

Enables automatic failover.

unset

Disables automatic failover.
File system names and the -a option can be specified and are handled the same way as in normal mode.

func extfunc

Specify this to enable or disable extended attributes for the file system, or to view the extended attribute settings. When the prompt is displayed, you can execute subcommands in the following formats:

```
list [-o create_time] {-a|file-system-name[ file-system-name...]}
set [-o create_time] {-a|file-system-name[ file-system-name...]}
unset [-o create_time] {-a|file-system-name[ file-system-name...]}
set_ctime {file-system-name[ file-system-name...]|
   directory-name[ directory-name...]}
```

list

Displays whether recording of file creation times is enabled or disabled, and the ACL type of the file system.
When you want to only display whether recording of file creation times is enabled, specify this option together with the -o create_time option.

set

Enables recording of file creation times.

unset

Disables recording of file creation times.

set_ctime

Sets the creation times of files.
The command processing for this option takes approximately one minute per 100,000 files that are contained in the specified file system or directory. When you execute the command, Wait ... is

displayed and then a period (`.`) is displayed each time 10,000 files are processed.

File system names, directory names, the `-a` option and `-o create_time` option can be specified and are handled the same way as in normal mode.

`func fullmsg`

Specify this to enable or disable the warning notification that is sent when file system usage exceeds a threshold value, or to view the warning notification settings. When the prompt is displayed, you can execute subcommands in the following formats:

```
list {-a|file-system-name[ file-system-name...]}
set [-o monitoring-target=warning-threshold
   [,monitoring-target=warning-threshold]]
   {-a|file-system-name[ file-system-name...]}
unset {-a|file-system-name[ file-system-name...]}
```

`list`

Displays whether the warning notification is enabled or disabled.

`set`

Enables the warning notification.

`unset`

Disables the warning notification.

The `-o` option, `-a` option, and file system names can be specified and are handled the same way as in normal mode.

`help`

Specify this to view the syntax of the subcommands that can be executed in interactive mode.

`quit`

Specify this if you want to end the `fsctl` command or its subcommand.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-186 Information displayed when executing the fsctl command (when the -f, -m or -i option is specified)

Item	Description
file-system-name	Displays the file system name.

status	Displays the current settings.
	
	`On`
	
	The settings are enabled.
	
	`Off`

Item	Description
	The settings are disabled.
	If the -m option has been specified, the thresholds for the block usage and inode usage are also displayed.

Table 2-187 Information displayed when executing the fsctl command (when the -c option is specified)

Item	Description
Filesystem	Displays the file system name.
Create_time	Displays whether the recording of the file creation time has been enabled. On The recording of the file creation time has been enabled. Off The recording of the file creation time has been disabled.
Acl_type	Displays the ACL type of the file system. Advanced Advanced ACL type Classic Classic ACL type
Overwrite_rename	Displays whether existing files and directories with duplicate names are overwritten when you move other files and directories of the Advanced ACL type file system, or when you rename files and directories. allow Existing duplicate files and directories are overwritten when you have the delete permission for those files and directories. deny Existing duplicate files and directories are not overwritten. -- A file system of the Classic ACL type has been specified.

Table 2-188 Information displayed when executing the fsctl command (when the -l option is specified)

Item	Description
Filesystem	Displays the file system name.
Status	Displays the access suppression status for a file system. Normal Access from clients has not been suppressed. Frozen

Item	Description
	Access from clients has been suppressed.

Return values

Table 2-189 Return values of the fsctl command (when the -f option is specified)

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

[#]
   The command ended abnormally due to multiple causes.

Table 2-190 Return values of the fsctl command (when the -m option is specified)

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

    The command ended abnormally due to multiple causes.

Table 2-191 Return values of the fsctl command (when the -c option is specified)

Return value	Description
0, 2[#1]	Normal termination
1, 10[#2]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10[#2], 99[#2]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99[#2]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99[#2]	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#1

    The ACL type of the specified file system is the Advanced ACL type (output when one file system name and `-o advanced_acl` are specified).

\#2

    The command ended abnormally due to multiple causes.

Table 2-192 Return values of the fsctl command (when the -l option is specified)

Return value	Description
0, 2[#1]	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 99[#2]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If

Return value	Description
	this error occurs repeatedly, contact maintenance personnel.
99[#2]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99[#2]	The error cannot be handled by the system administrator. Contact maintenance personnel.

#1

Access from a client to the specified file system is suppressed (output when one file system name is specified).

#2

The command ended abnormally due to multiple causes.

Examples

To check whether automatic failover that occurs when file system `FS_1` is blocked is enabled or disabled:

```
$ sudo fsctl -f FS_1
 FS_1            On
```

To enable the warning notification that is sent when usage of file system `FS_1` exceeds a threshold value according to the following conditions:

○ The warning threshold for block usage is 80G.

○ The warning threshold for inode usage is 20,000.

```
$ sudo fsctl -m -s -o blimit=80G,ilimit=20000 FS_1
BlockLimit=80GB, InodeLimit=20000 (FS_1)
```

To enable the warning notification that is sent when usage of file system `FS_2` exceeds a threshold value according to the following conditions:

○ The warning threshold for block usage is 80%.

○ The warning threshold for inode usage is 80%.

```
$ sudo fsctl -m -s -o blimit=80P,ilimit=80P FS_2
BlockLimit=80%, InodeLimit=80% (FS_2)
```

To set the creation times for the files (100,000 files) in file system `FS_1`:

```
$ sudo fsctl -c -x FS_1
FS_1: Wait ............. Success
```

To set the ACL type of the files (100,000 files) in file system `FS_1`:

○ Set a higher priority than usual for the processing.

- Convert the Classic ACL type to the Advanced ACL type.

```
$ sudo fsctl -c -x -o advanced_acl -p high FS_1
FS_1: Wait ............. Success
```

To enable automatic failover that occurs when a file system is blocked (interactive mode):

a. Interactive mode is started.

b. Check whether automatic failover is enabled.

c. Enable automatic failover that occurs when a file system is blocked.

d. Interactive mode is exited.

```
$ sudo fsctl -i
fsctl> func autofo
fsctl autofo> list -a
 filesystem1       Off
 filesystem2       Off
fsctl autofo> set -a
fsctl autofo> exit
fsctl> exit
```

fsdelete (Delete a file system)

Synopsis

```
fsdelete file-system-name
fsdelete -h
```

Description

Deletes a file system.

Options and arguments

file-system-name
> Specify the name of the file system to be deleted.

Return values

Table 2-193 Return values of the fsdelete command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10[#], 65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation.

Return value	Description
	If this error occurs repeatedly, contact maintenance personnel.
10[#], 66, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

fsedit (Change the file system settings)

Synopsis

```
fsedit [-w [-M maximum-retention-period]
    [-m minimum-retention-period]
    [-a {auto|manual|on} [-A auto-commit-period]]
    [-D default-retention-period]
   [-R {allow|deny}]]
   [-L {allow|deny}]
   [--ex-hcp-host host-name-that-has-been-made-external-and-is-used-
    to-connect-to-the-HCP]
   [--hcp-replica-host host-name-of-the-replica-HCP]
   [--ex-hcp-replica-host host-name-that-has-been-made-external-and-
    is-used-to-connect-to-the-replica-HCP]
   [[--hcp-account user-name] --hcp-password password]
   [--versioning {use|do_not_use}]
   [--period-to-hold past-version-retention-period]
   [--custom-schedule {use|do_not_use}]
   [--schedule-setting schedule[,schedule...]]
   [--bypass {on|off}] [-y] file-system-name
fsedit -h
```

Description

Changes the settings of a file system.

Options and arguments

-a {auto|manual|on}

Specify auto mode or manual mode for the enabled autocommit function in a WORM file system; the autocommit function automatically turns a file into a WORM file if no changes are made to it during the specified period. Specify this together with the -w option. If you specify this option to change the autocommit function from disabled to enabled, a confirmation

message is output. You cannot disable the autocommit function after enabling it.

`auto`

> Specify this option to enable the autocommit function in auto mode.
>
> In auto mode, all ordinary files, except for the system files and files in the system directories, are subject to the autocommit functionality.
>
> When you change the settings to use the autocommit function in auto mode, the autocommit management information of a WORM file system is rebuilt. Accordingly, access performance is temporarily affected. After the processing is completed, the KAQM37139-I message is output to the system messages.

`manual` or `on`

> Specify this option to enable the autocommit function in manual mode.
>
> In manual mode, files that are specified as read-only files by clients are subject to the autocommit functionality.

`-A` *auto-commit-period*

> Specify the wait period for turning a file into a WORM file in the following format. After you have specified the setting, you cannot change it.
>
> `days-hours-minutes`
>
> Specify a value from 1 minute to 36,500 days.
>
> Specify the `-w` option and the `-a` option with `auto`, `manual`, or `on` specified. If you omit this option, `0-0-15` (15 minutes) is set.
>
> For linkage with the HCP, you must set this option so that the autocommit period is shorter than the execution interval of migration.

`--bypass {on|off}`

> Specify this option to change the setting of whether to enable the CIFS bypass traverse checking function.
>
> `on`
>
> > Specify this option to enable the CIFS bypass traverse checking function. Note, however, that you cannot specify this argument if the target file system is a home-directory-roaming file system.
>
> `off`
>
> > Specify this option to disable the CIFS bypass traverse checking function.

`--custom-schedule {use|do_not_use}`

> Specify this to change the setting for using the custom schedule.
>
> `use`
>
> > Specify this to use the custom schedule. Note that this argument needs to be mounted while read and write is available for the specified file system.
>
> `do_not_use`

Specify this if you do not want to use a custom schedule.

You cannot specify this option when the `--versioning do_not_use` option is specified.

`-D` *default-retention-period*

Specify in the following format the retention period that is specified for the file for which the autocommit function is enabled.

days-hours-minutes

Specify a value from 1 minute to 36,500 days.

If you want to set an infinite default retention period, specify `infinite`. Specify this together with the `-w` option.

If you omit this option, the specified value varies depending on the options you specify and the current configuration values.

○ If the autocommit function is changed from disabled to enabled : `10-0-0` (10 days)

○ If the minimum retention period is set to `infinite` : `infinite`

Specify a default retention period that is equal to or greater than the minimum retention period, and that is equal to or smaller than the maximum retention period.

`--ex-hcp-host` *host-name-that-has-been-made-external-and-is-used-to-connect-to-the-HCP*

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. If you do not want to set a host name, specify two double quotation marks ("") or two single quotation marks ('').

This option can be specified if the target file system is set to reference the data from another HDI system as read-only at the file system level.

`--ex-hcp-replica-host` *host-name-that-has-been-made-external-and-is-used-to-connect-to-the-replica-HCP*

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. If you do not want to set a host name, specify two double quotation marks ("") or two single quotation marks ('').

This option can be specified if the target file system is set to reference the data from another HDI system as read-only at the file system level or if the host name of a replica HCP is set.

`--hcp-account` *user-name*

Specify this to change the user name used to access an HCP namespace. This option can be specified if the target file system is set to reference the data from another HDI system as read-only at the file system level.

`--hcp-password` *password*

Specify this to change the password of the user who accesses the namespace of an HCP system. This option can be specified if the target file system is set to reference the data from another HDI system as read-only at the file system level.

`--hcp-replica-host` *host-name-of-the-replica-HCP*

When you change the replica HCP system that is used for sharing data, use this option to set the new host name of the replica HCP system. If you do not want to set a host name, specify two double quotation marks (`""`) or two single quotation marks (`''`). This option can be specified if the target file system is set to reference the data from another HDI system as read-only at the file system level.

`-L {allow|deny}`

Specify this to change the setting whether to allow the creation of hard links on the file system. Note that this option takes effect only when the specified file system is mounted as read/write enabled.

`allow`

Specify this to allow the creation of hard links.

Do not set `allow` for a file system whose data is migrated to an HCP system. For such file systems, hard links are not restored when the data is restored from the HCP system.

`deny`

Specify this to deny the creation of hard links.

Note:

If the NFSv3 or NFSv4 protocol is being used, changes to the setting for hard link creation are not applied even when this command is executed while the file system is mounted. To enable the setting, unmount the file system from the NFS client, change the setting, and then mount the file system again.

`-m` *minimum-retention-period*

Specify this to change the minimum retention period for a WORM file system.

Specify the minimum retention period in the following format:

`days-hours-minutes`

Specify a value in the range from 0 minutes to 36,500 days.

If you want to set an infinite minimum retention period, specify `infinite`. Specify this together with the `-w` option. If you omit this option, the current setting information applies.

The minimum retention period must be equal to or smaller than the maximum retention period. In addition, if the autocommit function is enabled, the minimum retention period must be equal to or smaller than the default retention period.

`-M` *maximum-retention-period*

Specify this to change the maximum retention period for a WORM file system.

Specify the maximum retention period in the following format:

days-hours-minutes

Specify a value in the range from 1 minute to 36,500 days.

If you want to set an infinite maximum retention period, specify `infinite`. Specify this together with the `-w` option. If you omit this option, the current setting information applies.

The maximum retention period must be equal to or greater than the minimum retention period. In addition, if the autocommit function is enabled, the maximum retention period must be equal to or greater than the default retention period.

`--period-to-hold` *past-version-retention-period*

Specify this to change the retention period for the past version of files migrated to the HCP system. This option takes effect when clients are allowed to access the past version of files migrated to the HCP system. Note that you need to specify the version retention period for the HCP system in advance, a period that is one day longer than the value you specify here.

`-R {allow|deny}`

Specify whether to allow the renaming of empty directories in WORM file systems. This option must be specified with the `-w` option.

`allow`

Allows empty directories to be renamed.

`deny`

Prevents the renaming of empty directories.

`--schedule-setting` *schedule*`[,`*schedule*`...]`

Specify this to change the custom schedule settings. Specify this option together with the `--custom-schedule` option. To specify multiple schedules, separate each schedule by using commas (`,`).

When using this option, note the following points:

o You cannot specify 0 for all time units of the custom schedule. Specify a value other than 0 for at least one time unit.

o Be sure to specify a number of days greater than or equal to the recommended value calculated by the formula for the retention period of the past-version directories.

For details about custom scheduling of the file version restore functionality or the formula for recommended values of the retention period, see the *Installation and Configuration Guide*.

The following table describes the format for specifying custom schedules in this option.

Table 2-194 Format for specifying custom schedules by using the fsedit command

Specification format	Description
m–*minutes*	The oldest past version directory with 15-minute time units (hour *n*, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. For *minutes*, specify 0, 15, 30, 45, or 60. If you specify 0, schedules with 15-minute time units become invalid.
h–*hours*	The oldest past version directory with hourly time units (hour n, minutes 00 to 59) is kept for the number of units specified. For *hours*, specify in the range from 0 to 48. If you specify 0, schedules with hourly time units become invalid.
D–*days*	The oldest past version directory with daily time units (day *n*, 00:00 to 23:59) is kept for the number of units specified. or *days*, specify in the range from 0 to 62. If you specify 0, schedules with daily time units become invalid.
W–*weeks*	The oldest past version directory with weekly time units (week *n*, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. For *weeks*, specify in the range from 0 to 156. If you specify 0, schedules with weekly time units become invalid.
M–*months*	The oldest past version directory with monthly time units (month *n*, 1st day, 00:00 to *last-day*, 23:59) is kept for the number of units specified. For *months*, specify in the range from 0 to 72. If you specify 0, schedules with monthly time units become invalid.
Y–*years*	The oldest past version directory with yearly time units (year *n*, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. For *years*, specify in the range from 0 to 100. If you specify 0, schedules with yearly time units become invalid.

--versioning {use|do_not_use}

Specify this to change the setting for allowing clients to access the past version of files migrated to the HCP system. If you change the setting to prohibit clients from accessing the past version of files migrated to the HCP system, the retention period for the past version of these files is initialized.

For file systems that reference the data from other HDI systems as read-only, do not change the setting from do_not_use.

use

Specify this to allow clients to access the past version of files migrated to the HCP system. Note that you cannot specify this argument when data sharing with another HDI system using the HCP system is enabled.

do_not_use

Specify this to prohibit clients from accessing the past version of files migrated to the HCP system. If you specify this argument, a confirmation message is output. Note that this argument needs to be mounted while read and write is available for the specified file system. You cannot specify this argument when the --custom-schedule use option is specified.

-w

Specify this to change the settings of a WORM file system. Note that this option takes effect only when the specified file system is mounted as read/write enabled.

file-system-name

Specify the name of the target file system.

Return values

Table 2-195 Return values of the fsedit command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10[#], 65, 66[#], 68, 99[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
10[#], 66[#], 70, 74, 75, 76, 77	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
71, 72, 73	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Example

To change settings of the WORM file system according to the following conditions:

- The maximum retention period is to be changed to 30 years (10,950 days).
- The minimum retention period is to be changed to 1 year (365 days).
- The autocommit function is enabled.
- The autocommit period is 1 hour.
- The default retention period is 10 years (3,650 days).
- The file system name is FS_2.

```
$ sudo fsedit -w -M 10950-0-0 -m 365-0-0 -a on -A 0-1-0 -D 3650-0-0 FS_2
```

fsexpand (Expand a file system)

Synopsis (for cluster configurations)

```
fsexpand [-i inode] file-system-name
    device-file-name[,device-file-name...]
```

Synopsis (for single node configurations)

```
fsexpand [-i inode] -s [+]capacity file-system-name
fsexpand -i inode file-system-name
```

Synopsis (to reference the command syntax)

```
fsexpand -h
```

Description

Expands the capacity of a file system. Alternatively, the command changes the capacity of an inode (as a percentage of the file system capacity).

The expanded file system must be no more than 1 PB, which is the total size of the device files. Note, however, that the maximum capacity after expansion might be smaller than 1 PB depending on the file system. For details, see Table 2-180 Initial capacity of a created file system and the maximum capacity after expansion on page 2-323.

Note:

This command automatically reconfigures the inode area and moves up to 10 GB of data outside of the inode area if it is used to expand the file system capacity when all of the following conditions are met:

- The capacity of the file system after expansion is 1 TB or more.
- The file system does not support 64-bit inodes.

The system message KAQM04288-I is output when reconfiguration of the inode area starts, and the system message KAQM04289-I is output when reconfiguration is complete. In addition, reconfiguration of the inode area is performed as a background process, and takes up to about 50 minutes at maximum. Because this processing affects the access performance of the system, execute the command at a time when the system is accessed less frequently.

Options and arguments

-i *inode*

Specify the capacity of an inode, as a percentage of the file system capacity. Specify a value from 1 to 100. If you omit this option, the current setting information applies. The maximum capacity that can be used as an inode is 1 TB.

If you specify a value smaller than the currently used inode capacity, the currently used inode capacity will be set as the maximum capacity.

-s [+] *capacity*

This option can be used in single-node configurations. Specify the file system capacity (units: GB). If you want to specify the total capacity after expansion, specify the capacity without using a plus sign (+). If you want to specify additional capacity, specify the capacity with a plus sign (+). For this option, specify a value so that the capacity after expansion is in the range from *current-file-system-capacity* to *current-file-system-capacity + free-space*. Specify an expanded capacity that is larger than the current file system capacity, but not greater than the total of the current file system capacity and the free space available in the volume group.

file-system-name

Specify the name of the file system to be expanded.

device-file-name [, *device-file-name* ...]

Specify the names of device files to be added in the file system. The capacity of each device file must be 160 MB or more. For example, if the device file path is /dev/enas/lu01, specify lu01. When specifying multiple device files, use commas (,) to separate them. Specify device files that are in the same storage system as the device files that make up the file system. You can specify a maximum of 256 device files.

When you create a file system that has a striped configuration, specify device files of the same size. The number of device files to be specified here must be the same as the number of device files (number of stripes) specified when the file system is created. For example, if you specified three device files when creating a file system, add three device files. Striping is performed in the order of the specified device files.

Return values

Table 2-196 Return values of the fsexpand command

Return value	Description
0	Normal termination
1, 10[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10[#], 65, 66[#], 99[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
10[#], 66[#], 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
    The command ended abnormally due to multiple causes.

Examples

To expand a file system under the following conditions:

- The target file system is FS_1.
- The device files /dev/enas/lu2B and /dev/enas/lu3C are to be used.

```
$ sudo fsexpand FS_1 lu2B,lu3C
```

To change the capacity of an inode (as a percentage of the file system capacity):

- The maximum ratio that can be used as an inode is 60%.
- The target file system is FS_2.

```
$ sudo fsexpand -i 60 FS_2
```

fsexport (Disconnect a file system from the HDI system)

Synopsis

```
fsexport [-y] -f file-system-name
fsexport -h
```

Description

Disconnects the specified file system from the HDI system.

If you execute this command, any device files that make up the specified file system can no longer be distinguished from normal device files that are not in use. Therefore, we recommend that you save the settings for the target device files beforehand.

If you execute this command or the `fsimport` command, the HCP linkage settings are not inherited. If your file system is linked with HCP and you want to connect the file system with another node, rebuild the file system on that node without executing this command or the `fsimport` command. Then, execute the `arcrestore` command to restore data in the rebuilt file system.

> *Note:*
>
> A device file that you used before disconnecting the file system must not be used for purposes other than connecting the file system. If the device file is used for any other purpose, the contents of the file system in the device file will be disabled.

This command can be executed when the following conditions are satisfied:

- The file system is unmounted.
- The file system is not a WORM file system.

Options and arguments

`-f` *file-system-name*

Specify the name of the file system to be disconnected from the HDI system.

Return values

Table 2-197 Return values of the fsexport command

Return value	Description
0	Normal termination
4, 5, 6, 7	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 12[#], 20, 25, 28, 30, 46, 58, 75, 76, 77, 97, 98	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If

Return value	Description
	this error occurs repeatedly, contact maintenance personnel.
12#, 15, 29, 91, 93, 94, 95	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
90, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

fsfullmsg (Manage the warning notification functionality for file system usage)

Synopsis

```
fsfullmsg [-s [-o monitoring-target=warning-threshold
    [,monitoring-target=warning-threshold]]|-u]
    -a
fsfullmsg [-s [-o monitoring-target=warning-threshold
    [,monitoring-target=warning-threshold]]
    [-O monitoring-target=warning-threshold
    [,monitoring-target=warning-threshold]]|-u]
    file-system-name[ file-system-name...]
fsfullmsg -h
```

Description

Enables or disables the warning notification that is sent when file system usage exceeds a threshold value. Also displays the warning notification settings.

If you omit the -s option and -u option, the warning notification settings are displayed for each file system.

Even if you disable the warning notification, the previously set threshold value is saved. You can therefore omit the -o option if you want to apply the same threshold value when you next enable the warning notification.

Options and arguments

-a

Specify this option if you want to enable or disable automatic failover for all file systems mounted on the node to which you are logged in. If the command processing fails for any file system, processing continues for other file systems.

`-o` *monitoring-target* = *warning-threshold* `[`, *monitoring-target* = *warning-threshold* `]`

Specify this option if you specify the `-s` option. Specify the warning threshold value to trigger notification of the monitored target and warnings. If you omit this option, the current setting information applies.

If you specify `0` as the warning threshold value, a warning will be issued only when file system usage reaches the upper limit.

`blimit=` *warning-threshold*

Specify the warning threshold value in bytes or as a percentage (`%`) when you monitor file system usage by the number of blocks used. Note that if this option is specified, the file system usage is monitored when using blocks, and the warning threshold value is output in bytes or as a percentage (`%`).

To specify the value in bytes:

Specify a number followed by the letter `M`, `G`, or `T` for the unit (`M`: MB; `G`: GB; `T`: TB).

If the unit is MB: `blimit=500M`

If the unit is GB: `blimit=5G`

If the unit is TB: `blimit=1T`

To specify the value as a percentage (`%`):

Specify a number followed by the letter `P` (upper case).

Example: `blimit=80P`

The warning threshold is set from the specified percentage (`%`) of the file system capacity.

If you expand the file system, the warning threshold is re-calculated according to the increase in the file system capacity. Therefore, the warning threshold is automatically expanded when you expand the file system.

If you specify a number followed by the letter `p` (lower case), the byte count calculated from the specified percentage of the file system capacity at the time of command execution will be set as the warning threshold. The warning threshold is not re-calculated when you expand the file system.

`ilimit=` *warning-threshold*

If you are monitoring file system usage by the number of inodes, specify the warning threshold value as a number or percentage (`%`) of inodes that are in use. Note that if this option is specified, the file system usage is monitored at every one hour, and the warning threshold is output as the number of inodes or as a percentage (`%`).

To specify the value as the number of available inodes:

Example: `ilimit=9000`

To specify the value as a percentage (`%`):

Specify a number followed by the letter `P` (upper case).

Example: `ilimit=80P`

The warning threshold is set from the specified percentage (`%`) of the inode capacity that has been specified when the file system was created.

If you expand the file system, the warning threshold is re-calculated according to the increase in the inode capacity. Therefore, the warning threshold is automatically expanded if the inode capacity is expanded. The warning threshold is only calculated when you create or expand the file system, whereas the total number of usable inodes changes dynamically depending on the file system usage.

If you specify a number followed by the letter `p` (lower case), the byte count calculated from the specified percentage of the file system capacity at the time of command execution will be set as the warning threshold. The warning threshold is not re-calculated when you expand the file system. Similarly, the warning threshold is not re-calculated when the total number of usable inodes changes dynamically based on file system usage.

`-O` *monitoring-target* = *warning-threshold* [, *monitoring-target* = *warning-threshold*]

This option is not supported.

`-s`

Specify this option to enable the warning notification that is sent when file system usage exceeds the threshold value.

`-u`

Specify this option to disable the warning notification that is sent when file system usage exceeds the threshold value.

file-system-name [*file-system-name* ...]

Specify the file system names if you want to apply settings to the specified file systems only. You can use an asterisk (`*`) or question mark (`?`) as a wildcard. Separate multiple file system names with spaces.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-198 Information displayed when executing the fsfullmsg command

Item	Description
file-system-name	Displays the file system name.

setting	Displays whether the warning notification that is sent when file system usage exceeds a threshold value is enabled.
	`On`
	
	    Warning notification is enabled.
	`Off`

Item	Description
	Warning notification is disabled.
block-usage-threshold	Displays the threshold value for block usage.
i-node-usage-threshold	Displays the threshold value for inode usage.

Return values

Table 2-199 Return values of the fsfullmsg command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

#
The command ended abnormally due to multiple causes.

Example

To enable the warning notification that is sent when used block space of a file system mounted on the node exceeds 50 GB:

```
$ sudo fsfullmsg -s -o blimit=50G -a
BlockLimit=50GB (FS_1)
BlockLimit=50GB (FS_2)
BlockLimit=50GB (FS_3)
BlockLimit=50GB (FS_4)
```

fsifreeget (Display the number of files that can be created)

Synopsis

```
fsifreeget file-system-name
fsifreeget -h
```

Description

Displays the number of files that can be created.

Options and arguments

file-system-name

    Specify the name of the file system for which you want to view the number of files that can be created.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-200 Information displayed when executing the fsifreeget command

Item	Description
file-system-name	Displays the file system name.
number-of-files-that-can-be-created	Displays the number of files that can be created. However, depending on the usage of the file system, the displayed value might be more than the number of files that can actually be created.

Return values

Table 2-201 Return values of the fsifreeget command

Return value	Description
0	Normal termination
1#	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
1#	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

    The command ended abnormally due to multiple causes.

fsimport (Connect a file system)

Synopsis

```
fsimport -f file-system-name
    -d device-file-number[,device-file-number...]
    [-r resource-group-name]
fsimport -h
```

Description

Connects a file system to the HDI node that is currently being used.

After disconnecting and then re-connecting a file system, the file system settings might be changed. Check the setting values after connecting the file system.

The limit on the total number of file systems (including the file systems to be connected to) is 256 per single node, and 511 per cluster.

The following settings are the same as those before the file system was disconnected:

- ACL type of the file system
- WORM-related settings
- Setting for whether to allow creation of hard links
- Warning notification settings for file system usage
- Settings for the automatic-failover functionality used when a file system is blocked
- Quota settings
- Subtree quota settings

If you execute this command or the `fsexport` command, the HCP linkage settings are not inherited. If your file system is linked with HCP and you want to connect the file system with another node, rebuild the file system on that node without executing this command or the `fsexport` command. Then, execute the `arcrestore` command to restore data in the rebuilt file system.

Options and arguments

-d *device-file-number* [, *device-file-number* ...]

Specify the device numbers of the device files that constitute the file system. If you want to specify the device file `lu0F`, specify `0F`.

When the file system consists of multiple device files, use a comma (,) to separate all device file numbers specifying.

-f *file-system-name*

Specify the name of the file system to be created. Specify a unique name within a cluster.

-r *resource-group-name*

Specify the name of the resource group to which you want to register the file system. When executing the command with a virtual IP address specified, specify the name of a resource group with the -r option in case of a failover.

If you omit this option, the file system is registered in the resource group that belongs to the node you are logged in.

Return values

Table 2-202 Return values of the fsimport command

Return value	Description
0	Normal termination
4, 5, 6, 7, 9	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 22, 24, 40, 44, 45, 48, 50, 54, 55, 88, 89, 97, 98	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
74, 91, 93, 94	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
90, 92, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To connect a file system that exists in the device file named lu42 to a node in the HDI system, as a file system named fs001:

```
$ sudo fsimport -f fs001 -d 42
```

To connect a file system that exists in the device file named lu45 and lu43 to a node in the HDI system, as a file system named fs002:

```
$ sudo fsimport -f fs002 -d 45,43
```

fsinodectl (Management of Inodes)

Synopsis

```
fsinodectl [-m {inode64|alloc1TB}] file-system-name
fsinodectl -h
```

Description

This command supports 64-bit inodes, in order to reserve an inode area in the file system. You can also browse the current settings.

The settings for this command are applied at the time of subsequent mountings or of failovers in the file system.

Note that in a file system configured using versions earlier than 4.2.3-03, the system might be configured to store file extension attributes in an area that occupies the first 1 TB of the file system, which is also used to store inodes. To move file extension attributes stored in the first 1 TB of the file system to another area, use this command to configure storage of file extension attributes in an area separate to inode storage, and then use the `fsmoveattr` command.

Options and arguments

`-m {inode64|alloc1TB}`

Specify this option when you set whether to support 64-bit inodes or to store the file extension attributes in an area other than the first 1 TB from the top of the file system storing the inode. If you omit this option, the current settings are displayed.

`inode64`

Specify this argument to support 64-bit inodes. Once you set this to support 64-bit inodes, you cannot revert the setting. For notes about supporting 64-bit inodes, see the *Installation and Configuration Guide*.

`alloc1TB`

Specify this argument to store the file extension attributes in an area other than the first 1 TB from the top of the file system storing the inode. The initial setting for file systems built with system versions 4.2.3-03 and later is `alloc1TB`.

file-system-name

Specify the name of the file system.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-203 Information displayed when executing the fsinodectl command (when the -m option is omitted)

Item	Description

Current	Displays the current settings.
	`inode64`
	    This value is displayed if 64-bit inodes are supported.
	`alloc1TB`

Item	Description
	This value is displayed if file extension attributes are stored in an area other than the first 1 TB from the top of the file system storing the inode.
	`Off`
	This value is displayed if file extension attributes are stored in the same first 1 TB from the top of the file system storing the inode.
	`Not Mounted`
	This value is displayed if the file system is unmounted.
`New`	Displays the settings that will be applied at the time of subsequent mountings or failovers in the file system.
	`inode64`
	This value is displayed if 64-bit inodes are supported.
	`alloc1TB`
	This value is displayed if file extension attributes are stored in an area other than the first 1 TB from the top of the file system storing the inode.
	`Off`
	This value is displayed if file extension attributes are stored in the same first 1 TB from the top of the file system storing the inode.
	`Not Mounted`
	This value is displayed if the file system is unmounted.

Return values

Table 2-204 Return values of the fsinodectl command

Return value	Description
`0`	Normal termination
`1`[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`1`[#], `10`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
    The command ended abnormally due to multiple causes.

fsinodespace (Reconfigure the inode area)

Synopsis

```
fsinodespace [-s maximum-size] file-system-name
fsinodespace -h
```

Description

In order to increase the available capacity of the inode area, this command reconfigures the inode area by moving file data within the inode area out of that area.

This command is executed in the background. If an error occurs while background processing is being executed, a system message is output. The system message KAQM04288-I is output when reconfiguration of the inode area starts, and the system message KAQM04289-I is output when reconfiguration is complete. Use the `fslist` command to view system information before and after reconfiguration of the inode area, and check that `I-node free` (the number of remaining inodes) has increased.

To avoid impacting access performance, consider the time required for processing and execute the command when the system is accessed less frequently. Moving about 10 GB of data takes about 50 minutes. For a check of the time required to move more than 10 GB of data, execute the command without the `-s` option, measure the processing time required to move 10 GB of data, and then use the following formula to estimate the total time required.

(maximum-volume-of-data-to-be-moved(unit: GB) / 10) x *time-required-to-execute-command -without--s-option*

This command can be executed when the target file system meets the following conditions:

- The target file system is mounted as read/write enabled.
- The capacity of the target file system is 1 TB or more.
- The target file system does not support 64-bit inodes.

Options and arguments

-s maximum-size

Specify the maximum volume of data to be moved, as a value from 1 to 1024 (unit: GB). If this option is omitted, this value defaults to `10`.

file-system-name

Specify the name of the file system to be reorganized.

Table 2-205 Return values of the fsinodespace command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

fsiusedlist (Display information about the files that are using the inode area)

Synopsis

```
fsiusedlist [-b] [-s|-t] [-n number-of-lines] directory-name
fsiusedlist -h
```

Description

Displays information about the files that are using the inode area.

Options and arguments

-b

    This option is not applicable and will be ignored.

-n *number-of-lines*

    Specify the number of lines on which file information will be displayed.

-s

    Specify this to display the file information in order from largest to smallest of the used capacity of the inode area.

-t

    Specify this to display the file information in chronological order of last modified time.

directory-name

> Specify the name of the directory whose file information is to be viewed. Information for the files in the directory you specify here will be displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-206 Information displayed when executing the fsiusedlist command

Item	Description
i-node-area-size	Displays the capacity of the allocated inode area on the disk used by the file (units: bytes).
file-mode	Displays the file mode.
number-of-links	Displays the number of links.
owner	Displays the owner.
owner-group	Displays the owner group.
file-size	Displays the file size in bytes.
last-modified-time	Displays the last modified time.
file-name	Displays the file name.

Return values

Table 2-207 Return values of the fsiusedlist command

Return value	Description
0	Normal termination
1[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
1[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

> The command ended abnormally due to multiple causes.

fslist (List file system information)

Synopsis (for cluster configurations)

```
fslist [-c] [-e] [-d] [-t] [-b] [-p]
    [-m] [-i] [-w] [-L] [-v] [file-system-name]
```

Synopsis (for single node configurations)

```
fslist [-c] [-t] [-b]
    [-i] [-w] [-L] [-v] [file-system-name]
```

Synopsis (to reference the command syntax)

```
fslist -h
```

Description

Lists information related to one or more file systems.

When a resource group is failed over from one node in the cluster, this command also displays information about the file systems belonging to that resource group.

Options and arguments

-b

> Specify this to view the block space of the file system.

-c

> Specify this to output each file system's information separated with colons (:).
> Note that, if the information is not supported, nothing is displayed.

-d

> Specify this to append the drive type to the device file name.

-e

> Specify this to append a hash mark (#) to the end of the path for a device file residing in an external storage system.

-i

> Specify this to view the capacity of an inode (as a percentage of the file system capacity).

-L

> Specify this to view the setting for whether the creation of hard links is allowed.

-m

> Specify this to view the model and serial number of the storage system where device files exist.

-p

Specify this to view the number of stripes and the stripe size.

`-t`

Specify this to view the ACL type of the file system.

`-v`

Specify this to view all information about the file system.

`-w`

Specify this to view the WORM-related settings for the WORM file system.

file-system-name

Specify the name of a file system to view information about that file system. If you omit *file-system-name*, information about all the file systems on the node will be displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-208 Information displayed when executing the fslist command

Item	Description

`File system(used by)`	Displays the name of the file system. The following values in parentheses indicate how the file system is being used:
	
	 `Active Migration`
	
	  The file system is being used by the function of Active File Migration.
	
	 `WORM`
	
	  The file system is a WORM file system.
	
	 `WORM, Active Migration`
	
	  The file system is a WORM file system that is being used by the function of Active File Migration.

`Total disk capacity(GB)` [#]	Displays the file system capacity (total size of the device files). For a single node configuration, the total capacity of the file system specified when the file system was created or expanded is displayed.

`Device status`	Displays the status of device files that constitute the file system.
	
	 `normal`
	
	  The status is normal.
	
	 `error`
	
	  An error was detected while accessing a device file.

`Device files`	Displays, in ascending order, the names of device files that are used in the file system. For hexadecimal numbers, numbers in the range from `00` to `FF` are displayed as a 2-digit number, and numbers in the range from `0100` to `03FF` are

Item	Description
	displayed as a 4-digit number. If the `-p` or `-v` option is specified, the names of device files are displayed in the order in which they were specified when the file system was created or expanded (in the order in which striping is performed). When the `-e` or `-v` option is specified, a hash mark (`#`) is appended to the end of the device files name that are in an external storage system.
	If the `-d` option is specified, the drive type is appended to the device file name.
	`device-file-name(drive-type)`
	One of the following is displayed for *drive-type*:
	`FC/SAS`
	This is displayed for an FC or SAS drive.
	`SAS7K`
	This is displayed for a SAS 7.2K drive.
	`SATA`
	This is displayed for a SATA drive.
	`SSD`
	This is displayed for a solid-state drive.
	`-`
	Displayed in either of the following cases:
	- This is displayed when an error has occurred in the FC path.
	- This is displayed for a device file that is in an external storage system.
	- When a virtual LU in a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system is being used.
	- When a virtual LU that uses HUS100 series Dynamic Tiering is being used.
`Block capacity(GB)` [#]	Displays the block space when the file system is mounted properly.
	This is not displayed when the file system is not mounted properly.
`Block used(GB)` [#]	Displays the amount of used blocks when the file system is mounted properly.
	This is not displayed when the file system is not mounted properly.
`Block free(GB)` [#]	Displays the remaining block space when the file system is mounted properly.
	This is not displayed when the file system is not mounted properly.
`I-node used`	Displays the number of inode in use when the file system is mounted properly.
	This is not displayed when the file system is not mounted properly.

Item	Description
I-node free	Displays the number of remaining inodes when the file system is mounted properly.
	This is not displayed when the file system is not mounted properly.
Max i-node area(%)	Displays the capacity of an inode (as a percentage of the file system capacity).
Volume manager	Displays whether the file system uses the volume manager.
	use
	Displayed if the file system uses the volume manager.
	--
	Displayed if the file system does not use the volume manager.
Mount status	Displays the mount status of the file system.
	ro
	Displayed if the file system is read-only.
	rw
	Displayed if both read and write operations are permitted.
	fatal error
	Displayed if the file system is blocked. For details on how to resolve the problem, see the *Troubleshooting Guide*.
	expanding
	Displayed when processing to expand the file system is being executed or an error occurs during the expansion processing. Wait a while, and then re-execute the fslist command. If the error occurs again after re-executing the fslist command, an error might have occurred during the expansion processing. Acquire all of the log data, and then contact maintenance personnel.
	reclaiming
	Displayed when the unused area of the virtual LU that is used by the file system is being released.
	--
	Displayed if the file system is not mounted.
Quota	Displays the Quota setting at the time of mounting.
	on
	Displayed if the Quota setting is enabled.
	off
	Displayed if the Quota setting is disabled.
	--
	Displayed if the file system is not mounted.
	If the device file or the file system is blocked, the status in effect before the occurrence of the failure is displayed.
	Additionally, off is displayed after a failure under one of the following conditions:

Item	Description
	• The Quota setting had been disabled before the failure occurred. • The Quota setting had been enabled before the failure occurred. However, the status was changed when, for example, an unmount operation was performed after the failure.

ACL type	Displays the ACL type of the file system.
	`Advanced ACL`
	　Advanced ACL type
	`Classic ACL`
	　Classic ACL type
	`Unknown`
	　The ACL type could not be acquired.

Stripes	Displays the number of stripes. Displays -- if a file system does not have a striped configuration.
Stripe size(KB)	Displays the stripe size. Displays -- if a file system does not have a striped configuration.
Model	Displays the model of the storage system where device files exist.
Serial number	Displays the serial number of the storage system where device files exist.
Max retention	Displays the maximum retention period in the following format: *days-hours-minutes* If the maximum retention period is set to infinite, `infinite` is displayed. If the information cannot be acquired, `Unknown` is displayed. If the file system is not a WORM file system, -- is displayed. Nothing appears if the file system has not been mounted properly.
Min retention	Displays the minimum retention period in the following format: *days-hours-minutes* If the minimum retention period is set to infinite, `infinite` is displayed. If the information cannot be acquired, `Unknown` is displayed. If the file system is not a WORM file system, -- is displayed. Nothing appears if the file system has not been mounted properly.

Auto commit	Displays whether the autocommit function is enabled.
	`on`
	　The autocommit function is enabled.
	`off`

Item	Description
	The autocommit function is disabled.
	Unknown
	This is displayed if information could not be acquired.
	--
	The file system is not a WORM file system.
	Nothing appears if the file system has not been mounted properly.
Commit mode	Displays the commit mode of the autocommit function.
	auto
	The autocommit function is in auto mode.
	manual
	The autocommit function is in manual mode.
	Unknown
	This is displayed if information could not be acquired.
	--
	The file system is not a WORM file system, or when the autocommit function is disabled.
	Nothing appears if the file system has not been mounted properly.
Auto commit period	Displays, in the following format, how long to wait until files are turned into WORM files:
	days-hours-minutes
	If the information cannot be acquired, Unknown is displayed. If the file system is not a WORM file system or if the autocommit function is disabled, -- is displayed.
	Nothing appears if the file system has not been mounted properly.
Default retention	Displays, in the following format, the retention period set for the file for which the autocommit function was executed:
	days-hours-minutes
	If the retention period is set to infinite, infinite is displayed. If the information cannot be acquired, Unknown is displayed. If the file system is not a WORM file system or if the autocommit function is disabled, -- is displayed.
	Nothing appears if the file system has not been mounted properly.
Rename empty directories	Displays whether the renaming of empty directories is allowed in WORM file systems.
	allow
	Empty directories can be renamed.
	deny
	Empty directories cannot be renamed.
	--
	The file system is not a WORM file system.
	Unknown

Item	Description
	Information about the file system could not be acquired.
	This item is not displayed if the file system is not mounted correctly.
Hard link creation	Displays the setting for whether the creation of hard links is allowed.
	allow
	The creation of hard links is allowed.
	deny
	The creation of hard links is denied.
	Unknown
	This is displayed if hard link information could not be acquired.
	Nothing appears if the file system has not been mounted properly.
Namespace access type	Displays how to share HCP data migrated from other HDI systems.
	ro
	Displayed if the data from other HDI systems is to be referenced as read-only.
	rw
	Displayed if the data is not synchronized with other HDI systems via linked HCP systems.
	roaming
	Displayed if roaming among HDI systems is possible for the data from the home directory created for each end user.
	sharing
	Displayed if the data is shared among HDI systems using the read-write-content-sharing functionality.
	--
	An HCP system is not linked.
HCP namespace	Displays the name of an HCP namespace.
	Note that the displayed information depends on the value for Namespace access type as follows:
	If Namespace access type is ro:
	If the data from other HDI systems is referenced as read-only, the specified FQDN is displayed from the beginning (the period (.) at the end is not displayed). Additionally, if the data from other HDI systems is referenced at the share level as read-only, -- is displayed.
	If Namespace access type is rw:
	If data is migrated at the share level, Using Subtree Namespace is displayed.
	If Namespace access type is --:
	-- is displayed.

Item	Description
HCP namespace FQDN	Displays the FQDN for the name of the HCP namespace. However, if `Namespace access type` is `ro` and the data from other HDI systems is referenced at the share level as read-only, `Using Subtree Namespace` is displayed. If `Namespace access type` is not `ro`, `--` is displayed.
External HCP host	Displays the host name or IP address that has been made external and is used to connect to the HCP system. Note that `--` is displayed if no host name or IP address is set.
HCP replica host	The host name of the replica HCP system is displayed in FQDN format. Note that, in the following cases, `--` is displayed: • `Namespace access type` is not `ro`. • The data from other HDI systems is referenced at the share level as read-only. • The host name of the replica HCP system has not been set.
External HCP replica host	Displays the host name or IP address that has been made external and is used to connect to the replica HCP system. Note that `--` is displayed if no host name or IP address is set.
HCP account user	Displays the user name used to access an HCP namespace. However, if `Namespace access type` is not `ro`, and the data from other HDI systems is referenced at the share level as read-only, `--` is displayed.

Versioning	Displays the setting for whether to allow clients to access the past version of files migrated to the HCP system.
	
	`use`
	    Displayed if the clients are allowed to access the past version of files migrated to the HCP system.
	
	`do_not_use`
	    Displayed if the clients are not allowed to access the past version of files migrated to the HCP system.
	
	`--`
	    Displayed if data migration to the HCP system is not set.

Period to hold(day)	Displays the retention period for the past version of files migrated to the HCP system. If `Versioning` is `do_not_use`, `--` is displayed.

Custom schedule	Whether a custom schedule is enabled is displayed.
	
	`use`
	    If `Versioning` is `use` and the custom schedule is enabled, `use` is displayed.
	
	`do_not_use`
	    If `Versioning` is `use` and the custom schedule is disabled, `do_not_use` is displayed.
	
	`--`

Item	Description
	If versioning is other than use, -- is displayed.
Minute	The value specified for a custom schedule in 15-minute units is displayed (unit: minutes). Note that, in the following cases, -- is displayed: • If Versioning is not use. • If Versioning is use and a custom schedule in 15-minute units is disabled.
Hourly	The value specified for an hourly custom schedule is displayed (unit: hours). Note that, in the following cases, -- is displayed: • If Versioning is not use. • If Versioning is use and an hourly custom schedule is disabled.
Daily	The value specified for a daily custom schedule is displayed (unit: days). Note that, in the following cases, -- is displayed: • If Versioning is not use. • If Versioning is use and a daily custom schedule is disabled.
Weekly	The value specified for a weekly custom schedule is displayed (unit: weeks). Note that, in the following cases, -- is displayed: • If Versioning is not use. • If Versioning is use and a weekly custom schedule is disabled.
Monthly	The value specified for a monthly custom schedule is displayed (unit: months). Note that, in the following cases, -- is displayed: • If Versioning is not use. • If Versioning is use and a monthly custom schedule is disabled.
Yearly	The value specified for a yearly custom schedule is displayed (unit: years). Note that, in the following cases, -- is displayed: • If Versioning is not use. • If Versioning is use and a yearly custom schedule is disabled.
Single instancing	This item is not supported.
Volume group	For a single-node configuration, displays the name of the volume group used by the file system.
CIFS bypass traverse checking	Displays whether the CIFS bypass traverse checking function is enabled. on

Item	Description

	The CIFS bypass traverse checking function is enabled.
	
	`off`
	
	The CIFS bypass traverse checking function is disabled.
	
	`Unknown`
	
	Information about the file system could not be acquired.
	
	No information is displayed if the file system is not mounted properly.

#:

The value is displayed to three decimal places.

Return values

Table 2-209 Return values of the fslist command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99#	The error cannot be handled by the system administrator. Contact maintenance personnel.
99#	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

fsmount (Mount a file system)

Synopsis

```
fsmount -w [-u {update|do_not_update}] [-q {on|off}] [-c]
    file-system-name
fsmount -r file-system-name
fsmount -h
```

Description

Mounts a file system at the following mount point directory:

/mnt/*file-system-name*

The previous setting does not apply if you unmount and then re-mount the file system. If you omit the -u option or -q option, the default setting applies.

Options and arguments

-c

    Specify this if you want to change the ACL type of the file system from the Classic ACL type to the Advanced ACL type. Specify this option together with the -w option. Once the ACL type has been changed to the Advanced ACL type, you cannot change it to the Classic ACL type.

    To convert the ACL type of files in a file system, you must execute the fsctl command after executing this command.

    Note that this option is valid only for non-WORM file systems.

-q {on|off}

    Specify whether to enable the quota function. Specify this option together with the -w option. If you omit this option, it defaults to on.

    on

        Specify this to enable the quota function.

    off

        Specify this to disable the quota function.

-r

    Specify this if you do not want to permit writing to the file system.

-u {update|do_not_update}

    Specify whether to update the last access time when the file system is accessed. Specify this option together with the -w option. If you omit this option, it defaults to do_not_update.

    update

        Specify this if you want to update the last access time to the inode access time.

    do_not_update

        Specify this if you do not want to update the last access time.

-w

    Specify this if you want to permit writing to the file system.

file-system-name

    Specify the name of the file system to be mounted.

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

Return values

Table 2-210 Return values of the fsmount command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10[#], 65, 66, 99[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
10[#], 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

fsmoveattr (Moving extension attributes from the inode area)

Synopsis

```
fsmoveattr [-f] [-s block-size] file-system-name
fsmoveattr -p file-system-name
fsmoveattr -h
```

Description

This command moves file extension attributes stored in the inode area to a different area. If the file system is set to store the file extension attributes in an area other than that for the inode, you can move the attributes using the `fsinodectl` command.

This command can be executed when the target file system meets the following conditions:

- The target file system is mounted as read/write enabled.
- The capacity of the target file system is 1 TB or more.

- The target file system does not support 64-bit inodes.
- The target file system is configured with a system version earlier than 4.2.3-03.

Moving file extension attributes is performed as a background process, and takes up to about 55 minutes. Because this processing affects the access performance of the system, execute the command at a time when the system is accessed less frequently.

Options and arguments

`-f`

Specify this option to restart the suspended process to move the file extension attributes from the beginning. If this option is omitted, the suspended process is resumed.

`-p`

Specify this option to display whether the file system is available to move the file extension attributes stored in the same area as the inode to another area.

`-s` *block-size*

Specify the block size (units: GB) of the extension attribute to be moved. If `0` is specified, all extension attributes stored in the same area as the inode are moved to another area. If you omit this option, it defaults to `10`.

file-system-name

Specify the name of the file system for which the file extension attributes are moved.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-211 Information displayed when executing the fsmoveattr command (when the -p option is specified)

Item	Description
`alloc1TB`	Here, the setting is displayed for whether the file system is set to store the extension attributes in an area other than that storing the inode. The extension attributes can be moved in a file system for which `On` is displayed.
	`ON`
	This value is displayed if the file system is set to store the extension attributes in an area other than that storing the inode.
	`OFF`
	This value is displayed if the file system is not set to store the extension attributes in an area other than that storing the inode.

Table 2-212 Information displayed when executing the fsmoveattr command (when the -p option is not specified)

Item	Description
`traverse files`	Displays the number of searched files.
`target files`	Displays the number of files for which extension attributes are to be moved.
`move files`	Displays the number of files for which extension attributes have been moved.
`skip files`	Displays the number of files for which the movement of extension attributes has been canceled.
`move size`	Displays the total size of the files for which extension attributes have been moved.

Return values

Table 2-213 Return values of the fsmoveattr command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`2`, `3`, `4`, `11`, `13`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`14`, `16`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`98`, `99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

If the extension attributes are moved from the inode area:

- The name of the file system is `fs01`.
- The block size of the extension attributes to be moved should be 1 GB.

```
$ sudo fsmoveattr -s 1 fs01
traverse files : 259531
target  files : 259523
move    files : 259522
```

```
skip      files : 1
move      size  : 1063002112
```

fsrepair (Check the integrity of and repair a file system)

Synopsis

```
fsrepair [-L|-d|-n|-s] file-system-name
fsrepair -h
```

Description

Checks the integrity of a blocked file system and repairs the file system. If you omit all the options, only the integrity check is performed.

When this command is repairing a file system, the processing progress is displayed. Depending on the status of the file system, the `fsrepair` command might not be able to repair the file system. If the `fsrepair` command cannot repair the file system, restore the file system from the backup data.

Depending on the size of the file system and the number of files, processing might take considerable time.

When the namespace quota has been set for the target file system share, executing this command reduces the block of space used. This can cause migration failures for updated data before the next migration is executed. We recommend you execute the migration task by using the `arcmigrun` command, immediately after executing this command.

After the file system is repaired by using this command, perform either of the following according to the operation:

For single-node configurations:

Restart the resource group by using the `rgstop` and `rgstart` commands.

> *Note:*
>
> Make sure to execute this command in accordance with the instructions from maintenance personnel.

Options and arguments

`-d`

Specify this option to display information about unmounted file systems.

`-L`

Specify this option if you want to repair the file system. Repairing a file system causes the journal to be cleared, so any data in the journal that has not been written to the disk drive will be lost.

`-n`

Specify this option if you want to check the integrity of the file system. If the check finds no lack of integrity in the file system, the blocked status is released and the file system becomes eligible for mounting.

-s

Specify this option to view whether the file system is blocked.

file-system-name

Specify the name of the file system.

Displayed information

The following table lists the information displayed when you execute the command with the -d option specified.

Table 2-214 Information displayed when executing the fsrepair command with the -d option specified

Item	Description
file-system-name	Displays the specified file system name.
Size	Displays the capacity of the file system. If the value after the first decimal place is 50 or smaller, the first decimal place is rounded down. If the value after the first decimal place is 51 or larger, the first decimal place is rounded up.
Used	Displays the total capacity of the blocks that are in use. If the value after the first decimal place is 50 or smaller, the first decimal place is rounded down. If the value after the first decimal place is 51 or larger, the first decimal place is rounded up.
Available	Displays the total capacity of the blocks that are not in use. If the value after the first decimal place is 50 or smaller, the first decimal place is rounded down. If the value after the first decimal place is 51 or larger, the first decimal place is rounded up.
Use%	Displays the usage rate of the file system.
Inodes	Displays the maximum number of inodes.
IUsed	Displays the number of inodes that are in use.
IAllocate	Displays the number of inodes to which the inode space is assigned and are not in use.
IFree	Displays the number of inodes that are not in use.
IUse%	Displays the usage rate of inode space.
AGcount	Displays the number of partitions for the file system.
Quota	Displays the Quota setting at the time of mounting. on Displayed if the Quota setting is enabled. off

Item	Description
	Displayed if the `Quota` setting is disabled.

The following table lists the information displayed when you execute the command with the `-s` option specified.

Table 2-215 Information displayed when executing the fsrepair command with the -s option specified

Item	Description
file-system-name	Displays the specified file system name.

status	Displays the file system status.
	`Normal`
	    Displayed if the file system is normal.
	`Blocked`
	    Displayed if the file system is blocked.

Return values

Table 2-216 Return values of the fsrepair command (when the -d option is specified)

Return value	Description
`0`	Normal termination
`1`[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`1`[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`1`[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.
`2`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.

#
    The command ended abnormally due to multiple causes.

Table 2-217 Return values of the fsrepair command (when the -n option is specified)

Return value	Description
0	Normal termination
1[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
1[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
1[#], 2[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
1[#], 2[#], 3	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Table 2-218 Return values of the fsrepair command (when the -L option is specified)

Return value	Description
0	Normal termination
1[#]	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
1[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
1[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
1[#], 2[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
1[#], 2[#], 3	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Table 2-219 Return values of the fsrepair command (when the -s option is specified)

Return value	Description
0	Normal termination
1[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
1[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
2[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2[#], 3	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
The command ended abnormally due to multiple causes.

fsumount (Unmount a file system)

Synopsis

```
fsumount file-system-name
fsumount -h
```

Description

Unmounts a file system.

Options and arguments

file-system-name
Specify the name of the file system to be unmounted.

Return values

Table 2-220 Return values of the fsumount command

Return value	Description
0	Normal termination

Return value	Description
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10[#], 65, 66[#], 99[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
10[#], 66[#], 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

ftpget (Display the FTP service configuration)

Synopsis

```
ftpget [-h]
```

Description

Displays the FTP service configuration.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-221 Information displayed when executing the ftpget command

Item	Description

FXP	Displays whether FXP is enabled
	
	On
	
	    FXP is enabled.
	
	Off
	
	    FXP is disabled.

Table 2-222 Return values of the ftpget command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
65, 68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
68[#], 70, 95	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

ftpset (Change the FTP service configuration)

Synopsis

```
ftpset --fxp {on|off}
ftpset -h
```

Description

Changes the FTP service configuration on the node you are logged in to.

You cannot use FXP in an IPv6 environment.

Specify the same settings on both nodes in the cluster. Also specify the same settings for the FTP servers that transfer files.

When you have changed the FTP service configuration, restart the FTP service. The new configuration will not be applied until you restart the FTP service.

Options and arguments

--fxp {on|off}

Specify whether to enable FXP. The initial setting is off.

on

Specify this to enable FXP.

off

Specify this to disable FXP.

Return values

Table 2-223 Return values of the ftpset command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
46, 68[#], 70, 95	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Example

To enable FXP:

```
$ sudo ftpset --fxp on
```

grpadd (Add a group)

Synopsis

```
grpadd -g group-ID [-C]
    [-u {user-name|user-ID}[,{user-name|user-ID}...]] group-name
grpadd -F CSV-file-name [-o result-file-name] [-t] [-V]
grpadd -h
```

Description

Adds a group or groups. You can register up to 2,000 groups per cluster.

Before batch-registering groups using a CSV file, you must transfer the CSV file to the SSH account home directory (`/home/nasroot`). We recommend that you specify the `-o` option when you execute this command. If you specify the `-o` option, the execution results are output to a file. If you omit the `-o` option, the results of command processing will not be output. For details about how to create a CSV file, see [Format of a CSV file used for batch registration or batch deletion of group information on page B-8](#). For details about how to check the execution results, see [Format of result file used for batch registration or batch deletion of group information on page B-10](#).

Options and arguments

`-C`

> Specify this to add a group that uses ACLs for accessing CIFS shares.

`-F` *CSV-file-name*

> To batch-register groups, specify the name of the CSV file containing the group information.
>
> The name of the CSV file must be no more than 255 characters. You can use alphanumeric characters, hyphens (`-`), and underscores (`_`). You can also use periods (`.`), except at the beginning or end of the character string.

`-g` *group-ID*

> Specify the group ID in the range from 200 to 2147483147. You cannot specify a group ID that is already registered by File Services Manager, the NIS server, or the LDAP server for user authentication. You cannot specify 65534. If user mapping is used, you cannot specify a group ID within the range set for user mapping.

`-o` *result-file-name*

> To output the execution results to a file, specify a file name of no more than 255 characters. You can use alphanumeric characters, hyphens (`-`), and underscores (`_`). You can also use periods (`.`), except at the beginning or end of the character string.
>
> The execution results file will be output immediately under the SSH account home directory (`/home/nasroot`). The file cannot have the same name as an existing file in the `/home/nasroot` directory.

`-t`

> Specify this to check the information in the CSV file without adding any group.

`-u` { *user-name* | *user-ID* }[,{ *user-name* | *user-ID* }...]

> Specify the users who belong to the group, by user name or user ID. The specified users must be registered with File Services Manager. When specifying multiple users, use a comma (`,`) to separate them.

`-V`

> Specify this to display the progress of the batch-registration processing or CSV file-check processing.

group-name

Specify the group name using no more than 16 characters, beginning with an alphanumeric character. From the second character, you can use alphanumeric characters, hyphens (-), and underscores (_). Alphabetic characters are not case sensitive in Windows. Specify a name that is unique regardless of the case. You cannot specify a name that duplicates a group name already registered by File Services Manager, the NIS server, or the LDAP server for user authentication. When you use the ACL function for the group being added, you cannot specify a name that is identical to that of any user configured to access CIFS shares.

You cannot specify the following group names, which are reserved in the OS on a node:

Table 2-224 Group names reserved in the OS on a node

Start character	Group name
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
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

Return values

Table 2-225 Return values of the grpadd command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 66[#], 70, 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
96, 97, 98, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Example

To batch-register groups under the following conditions:

- The CSV file name is `groupadd100.csv`.
- The result file name is `result_addgroup.txt`.

```
$ sudo grpadd -F groupadd100.csv -o result_addgroup.txt
```

grpdel (Delete a group)

Synopsis

```
grpdel [-f] group-name
grpdel -F CSV-file-name [-o result-file-name] [-t] [-V] [-f]
grpdel -h
```

Description

Deletes a group or groups.

Before batch-deleting groups using a CSV file, you must transfer the CSV file to the SSH account home directory (`/home/nasroot`). We recommend that you specify the `-o` option when you execute this command. When you specify

the `-o` option, the execution results are output to a file. If you omit the `-o` option, the results of command processing will not be output. For details about how to create a CSV file, see Format of a CSV file used for batch registration or batch deletion of group information on page B-8. For details about how to check the execution results, see Format of result file used for batch registration or batch deletion of group information on page B-10.

Options and arguments

`-f`

Specify this to prevent the confirmation message from appearing.

`-F` *CSV-file-name*

To batch-delete groups, specify the name of the CSV file containing the group information.

The name of the CSV file must be no more than 255 characters. You can use alphanumeric characters, hyphens (-), and underscores (_). You can also use periods (.), except at the beginning or end of the character string.

`-o` *result-file-name*

To output the execution results to a file, specify a file name of no more than 255 characters. You can use alphanumeric characters, hyphens (-), and underscores (_). You can also use periods (.), except at the beginning or end of the character string.

The execution results file will be output immediately under the SSH account home directory (`/home/nasroot`). The file cannot have the same name as an existing file in the `/home/nasroot` directory.

`-t`

Specify this to check the information in the CSV file without applying it.

`-V`

Specify this to display the progress of the batch-deletion processing or CSV file-check processing.

group-name

Specify the name of the group to be deleted.

Return values

Table 2-226 Return values of the grpdel command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 66[#], 70, 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the

Return value	Description
	problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66#	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
96, 97, 98, 99#	The error cannot be handled by the system administrator. Contact maintenance personnel.

#
   The command ended abnormally due to multiple causes.

Example

To batch delete groups under the following conditions:

- ○ The CSV file name is `groupdel100.csv`.
- ○ The result file name is `result_delgroup.txt`.

```
$ sudo grpdel -F groupdel100.csv -o result_delgroup.txt
KAQM07077-Q Do you want to perform a batch deletion? (y/n)
```

grplist (List group information)

Synopsis
```
grplist [-c] [group-name|group-ID]
grplist -h
```

Description

Lists information about groups registered by File Services Manager.

Options and arguments

-c
   Specify this to display group information separated with colons (:).

group-name | *group-ID*
   Specify the group name or group ID to view information about a specific group.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-227 Information displayed when executing the grplist command

Item	Description
Group name	Displays the group name.
GID	Displays the group ID.

Return values

Table 2-228 Return values of the grplist command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

hcpaccesstest (Check the access to the HCP system)

Synopsis

```
hcpaccesstest --namespace namespace-name [--replica]
hcpaccesstest --namespace-fqdn namespace-FQDN --hcp-account user-name
    --hcp-password password
    [--ex-host host-name-that-has-been-made-external-and-is-used-to-
     connect-to-the-HCP]
hcpaccesstest -h
```

Description

Checks whether access to the namespace in the HCP system is available. The hcpaccesstest command finishes successfully after confirming that access is available.

If you want to check whether the HCP system used for referencing the data from other HDI systems as read-only is accessible, specify the `--namespace-fqdn` option and execute the command.

Options and arguments

`--ex-host` *host-name-that-has-been-made-external-and-is-used-to-connect-to-the-HCP*

> 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.

`--hcp-account` *user-name*

> Specify the user name used to access the namespace in the HCP system.

`--hcp-password` *password*

> Specify the password of the user used to access the namespace in the HCP system.

`--namespace` *namespace-name*

> Specify the namespace in the HCP system to be accessed.

`--namespace-fqdn` *namespace-FQDN*

> Specify the FQDN of the namespace in the HCP system to be accessed.

`--replica`

> Specify the namespace of the replica HCP system to be accessed.

Return values

Table 2-229 Return values of the hcpaccesstest command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 11, 70, 71[#], 75, 76, 77	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
66, 67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
68, 71[#], 72, 73	The system might be temporarily disabled for communication. After checking the communication status,

Return value	Description
	wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

    The command ended abnormally due to multiple causes.

Examples

To check whether access to the namespace `ns1` is available:

```
$ sudo hcpaccesstest --namespace ns1
KAQM37099-I A connection to HCP was established.
```

To check whether access to the namespace (FQDN) in the HCP system is available according to the following conditions:

- The namespace (FQDN) is `ns1.tenant1.example.com`.
- The account name is `user1`.
- The password is `passpass`.

```
$ sudo hcpaccesstest --namespace-fqdn ns1.tenant1.example.com --hcp-
account user1 --hcp-password passpass
KAQM37099-I A connection to HCP was established.
```

hcpdisplaykey (Displaying the common encryption key used for data stored on an HCP system to save the data outside of the system)

Synopsis

```
hcpdisplaykey [-h]
```

Description

Displays the common key used for encryption of data stored on an HCP system so that the data can be saved to external media.

In a cluster configuration, execute this command in either system to display the key.

This command uses a passphrase that was specified interactively to encrypt a common key used for local data encryption, and then displays a character string in hexadecimal format as the key, so that the key can be saved outside the system. Copy and paste the displayed character string to a text file, make sure that no linefeed characters are included, and then save the key in storage media outside the system.

This command can be executed when encryption functions are enabled for data stored on an HCP system.

To end interactive entry and cancel the command execution, press **Ctrl**+**D** without entering anything for any of the items.

The following table lists the information items that can be set interactively.

Table 2-230 Information that can be specified interactively for the hcpdisplaykey command

Item	Description
Enter passphrase	Specify a passphrase used to create a key to be saved outside the system as a common key saved in the HCP. You can use 1 to 64 characters.
	You can use alphanumeric characters, exclamation marks (!), double quotation marks ("), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), asterisks (*), plus signs (+), commas (,), hyphens (-), periods (.), forward slashes (/), colons (:), semicolons (;), left angle brackets (<), equal signs (=), right angle brackets (>), question marks (?), at marks (@), left square brackets ([), backslashes (\), right square brackets (]), carets (^), underscores (_), grave accent marks (`), left curly brackets ({), vertical bars (|), right curly brackets (}), tildes (~), and spaces.
	For security reasons, we recommend you specify a passphrase containing at least 10 characters using a combination of numbers and alphabetic letters.
Confirm passphrase	Specify the above passphrase again.

Note:

The character strings specified for Enter passphrase and Confirm passphrase are not displayed.

Return values

Table 2-231 Return values of the hcpdisplaykey command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 70, 71, 73, 75	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

hcpobjdelget (Display the data deletion settings in the HCP system when files are deleted)

Synopsis

```
hcpobjdelget --file-system file-system-name
hcpobjdelget -h
```

Description

Displays the data deletion settings in the HCP system when files migrated to the HCP system are deleted.

This command can be used if the target file system is mounted as read/write enabled.

Options and arguments

`--file-system` *file-system-name*
Specify the name of the target file system.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-232 Information displayed when executing the hcpobjdelget command

Item	Description
HCP object deletion	Displays the data deletion setting in the HCP system when files migrated to the HCP system are deleted.
	Delay
	When the next migration is performed, data in the HCP system is deleted asynchronously with the file deletion processing.
	Immediately
	Data in the HCP system is deleted synchronously with the file deletion processing.

Table 2-233 Return values of the hcpobjdelget command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 4, 10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

hcpobjdelset (Data deletion settings in the HCP system when files are deleted)

Synopsis

```
hcpobjdelset {--delay|--immediately} --file-system file-system-name
hcpobjdelset -h
```

Description

Sets whether data in the HCP system is deleted synchronously with the file deletion processing, when files migrated to the HCP system are deleted.

The following conditions must be met before you can use this command:

- The target file system is mounted as read/write enabled.
- The target file system does not support home-directory-roaming functionality.
- The target file system does not support read-write-content-sharing functionality.

Options and arguments

`--delay`

Specify this option to delete data in the HCP system asynchronously with the file deletion processing, when next migration is performed. If free space in the file system is insufficient, data in the HCP system is deleted

synchronously with the file deletion processing even if this option is specified. The initial setting is `--delay`.

`--file-system` *file-system-name*

Specify the name of the target file system.

`--immediately`

Specify this option to delete data in the HCP system synchronously with the file deletion processing.

Return values

Table 2-234 Return values of the hcpobjdelset command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 4, 5, 10, 15, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

hcporphanrestore (Check the integrity of and recover the files in both the HDI and HCP systems)

Synopsis

```
hcporphanrestore [--display] --file-system file-system-name
hcporphanrestore -h
```

Description

This command checks the integrity of the files in the HDI system and the migrated files in the HCP system, and then displays the inconsistent files. Use this command for the file systems only immediately after the `arcrestore` command is executed for those file systems. For details, see the error recovery procedures in the *Troubleshooting Guide*.

If files that exist only in the HCP system are detected, the recovery target directories depend on how data is migrated to the HCP system.

- If data is migrated at the file system level:

  /mnt/*file-system-name*/.lost+found directory and its subdirectories

- If data is migrated at the share level:

  /mnt/*file-system-name*/*shared-directory-name*/.lost+found directory and its subdirectories

The processing time of the command depends on the detected results or scale of the file system. If you execute the command for a file system that contains 100,000 directories and 10,000,000 files, and 100 files that are only in the HCP system are detected, it will take about 17 hours to complete the processing.

For file systems that are configured so that a request to delete a file stored in the HCP system is not sent when a file is deleted from the HDI system, all the files that were deleted from the HDI system after migration will be determined to be only in the HCP system if you execute this command.

Note

If migration to an HCP system is performed during command execution, files that are inconsistent might also be recovered.

Options and arguments

--display

   Specify this if you want the inconsistent files between the HDI and HCP systems to be displayed but not recovered.

--file-system *file-system-name*

   For this option, specify the name of the file system for which you want to check the integrity of the files between the HDI and HCP systems.

Displayed information

The following table lists the information displayed when inconsistent files between the HDI and HCP systems are detected. If multiple files are detected, a blank line is used to separate the files.

Table 2-235 Information displayed when the hcporphanrestore command is executed

Item	Description
Inconsistency type	The reason why the files between the HDI and HCP systems are inconsistent is displayed.
	Duplication
	Indicates that multiple files in the HDI system are referencing a single object in the HCP system.
	Orphan

Item	Description
	Indicates that files are only in the HCP system, not in the HDI system.
	After all the files that were determined as `Duplication` are displayed, the files that were determined as `Orphan` are displayed.
URLs of the files in the HCP system	The URLs of the inconsistent files in the HCP system are displayed.
Paths of the files in the HDI system	According to the inconsistency type, the following information is displayed:
	When the inconsistency type is `Duplication`:
	The paths of the files at the time they were last migrated are displayed.
	When the inconsistency type is `Orphan`:
	The paths of the files at the time they were first migrated are displayed.

Return values

Table 2-236 Return values of the hcporphanrestore command

Return value	Description
`0`	Normal termination
`1, 3`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`2, 5, 8, 10, 12, 23, 31, 70,` `71`[#]`, 74, 75`[#]`, 77, 79, 80`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`66`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`71`[#]`, 72, 73, 75`[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`97, 98, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

  The command ended abnormally due to multiple causes.

Examples

When checking the integrity of the files for the file system `fs01` and recovering the files that were determined to be inconsistent:

```
$ sudo hcporphanrestore --file-system fs01
Duplication
https://namespace10.test.hcp-c.hsp2f.co.jp/rest/16d/36/16d361f2-a88a-4940-
b35f-dd1eb15f9c96
/mnt/test5/dir103/file15

Duplication
https://namespace10.test.hcp-c.hsp2f.co.jp/rest/917/11/91711953-b31b-4962-
bb04-e3b8c6a3d0f4
/mnt/test5/dir103/file53

Orphan
https://namespace9.test.hcp-c.hsp2f.co.jp/rest/a45/02/a450228d-f261-493d-
bf6b-d9ff0f2e6a1f
/mnt/test4/dir6/file12

Orphan
https://namespace9.test.hcp-c.hsp2f.co.jp/rest/cc2/64/cc2649ee-fdb6-4115-
b576-8bb046cb14c1
/mnt/test4/dir10/file39
```

When only checking the integrity of the files for the file system `fs01` but not recovering the files that were determined to be inconsistent:

```
$ sudo hcporphanrestore --display --file-system fs01
Duplication
https://namespace10.test.hcp-c.hsp2f.co.jp/rest/16d/36/16d361f2-a88a-4940-
b35f-dd1eb15f9c96
/mnt/test5/dir103/file15

Duplication
https://namespace10.test.hcp-c.hsp2f.co.jp/rest/917/11/91711953-b31b-4962-
bb04-e3b8c6a3d0f4
/mnt/test5/dir103/file53

Orphan
https://namespace9.test.hcp-c.hsp2f.co.jp/rest/a45/02/a450228d-f261-493d-
bf6b-d9ff0f2e6a1f
/mnt/test4/dir6/file12

Orphan
https://namespace9.test.hcp-c.hsp2f.co.jp/rest/cc2/64/cc2649ee-fdb6-4115-
b576-8bb046cb14c1
/mnt/test4/dir10/file39
```

hcprecoverkey (Restoring the common key used for encryption of data stored on an HCP system)

Synopsis

```
hcprecoverkey [-h]
```

Description

Decodes a key recorded on external media, and restores this key as the common key used for encryption of data on an HCP system.

If you execute this command in a cluster configuration, the command restores the common key for both nodes. Note, however, that if synchronization of the nodes fails, only the common key for the local node is restored. In this case, you must correct the failure in the remote node, and then restart the OS of the remote node and restore the common key.

If you stop or restart the OS of the node before recovering from an HCP access failure, re-execute the command to restore the common key.

The following conditions must be met before you can use this command:

- The `syslurestore` command has been executed, and the system settings LU file was restored.
- The encryption function for data stored on an HCP system is enabled.

To end interactive entry and cancel the command execution, press **Ctrl**+**D** without entering anything for any of the items.

The following table describes the information you specify with the `hcprecoverkey` command:

Table 2-237 Information you specify with the hcprecoverkey command

Item	Description
Enter key	Specify the key saved in storage media outside the system.
Enter passphrase	Specify the passphrase specified for the `hcpdisplaykey` command.

Notes:

- The character strings specified for `Enter passphrase` is not displayed.
- When you specify the key saved in storage media outside the system, make sure that the key does not include a linefeed character.

Return values

Table 2-238 Return values of the hcprecoverkey command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 3, 70, 71, 75, 76, 77	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output

Return value	Description
	message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

hcpverifykey (Verifying common keys used for encryption of data stored on an HCP system)

Synopsis

```
hcpverifykey [-h]
```

Description

Verifies whether the key code saved on external media matches a common key used for HCP data encryption.

If the keys match, the KAQM05307-I message indicating that the keys match appears. If the keys do not match, take action according to the instructions given for the KAQM05306-E or KAQM05321-E message.

This command can be executed when encryption functions are enabled for data stored on an HCP system.

To end interactive entry and cancel the command execution, press **Ctrl**+**D** without entering anything for any of the items.

The following table describes the information you specify with the `hcpverifykey` command:

Table 2-239 Information you specify with the hcpverifykey command

Item	Description
Enter key	Specify the key saved in storage media outside the system.
Enter passphrase	Specify the passphrase specified for the `hcpdisplaykey` command.

Notes:

- The character strings specified for `Enter passphrase` is not displayed.

- When you specify the key saved in storage media outside the system, make sure that the key does not include a linefeed character.

Return values

Table 2-240 Return values of the hcpverifykey command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2, 3, 70, 71, 73, 75	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

hnasmpasswd (Change the password of the management server)

Synopsis

```
hnasmpasswd
```

Description

Interactively changes the password used by the management server to connect to a node.

Execute this command on every node to ensure that all passwords to nodes within the cluster are identical.

The following table describes the information you specify with the `hnasmpasswd` command:

Table 2-241 Information you specify with the hnasmpasswd command

Item	Description
New password	Specify 4 to 256 characters for the new password. You can use alphanumeric characters, hash marks (#), plus signs (+), hyphens (-), periods (.), and at marks (@).
Re-enter new password	Specify the new password again.

Note:

> The character strings you entered in the `New password` and `Re-enter new password` will not be displayed.

Return values

Table 2-242 Return values of the hnasmpasswd command

Return value	Description
0	Normal termination
1, 2, 3	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
4	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

horcconflist (Display the CCI instance numbers currently being used)

Synopsis

```
horcconflist [-c] [-nomsg]
horcconflist -h
```

Description

The `horcconflist` command obtains the number of each CCI instance being used, and displays it together with the host name of the node that is currently using that instance number.

If the command is unable to obtain instance numbers from some nodes, it displays only the instance numbers it has obtained.

The host name of the physical node is displayed for the added instance numbers (`20` to `499`).

Options and arguments

`-c`

> Specify this option to separate each piece of information with a colon (`:`), rather than displaying the item names. This is handy when you want to

use the resulting information that is output from this command for the execution of another command right after this one.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-243 Information displayed when executing the horcconflist command

Item	Description
`instance`	Displays the instance numbers being used, in ascending order.
`node number`	Displays in the following format the host name of the node that is using the instance number: *node-number(node-host-name)*

Return values

Table 2-244 Return values of the horcconflist command

Return value	Description
`0`	Normal termination
`4`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`13, 14, 19, 80`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`68`	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
`74`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

horcdevlist (Display configuration information about a device file)

Synopsis

```
horcdevlist [-c] [-e] [-v]
    [-d {device-file-number|device-file-number-device-file-number}
```

```
    [,{device-file-number|device-file-number-device-file-number}...]]
    [-nomsg]
horcdevlist -h
```

Description

The `horcdevlist` command displays configuration information about a device file such as the device file number, size, and status.

Options and arguments

`-c`

Specify this option to display each piece of information delimited with colons (`:`), rather than showing the item names. This is effective when immediately executing another command using the output from device file configuration information.

`-d` { *device-file-number* | *device-file-number – device-file-number* }`[,{` *device-file-number* | *device-file-number – device-file-number* `}...]`

To view the configuration information for a specific device file, specify the target device file number.

For example, if you are referencing the configuration information of a device file located at `/dev/enas/lu0F`, specify `0F`. Use a comma (`,`) as the delimiter when referencing the configuration information of multiple device files.

To view the configuration information for multiple device files, specify the range by separating the device file numbers with a hyphen (`-`). This is effective when referencing configuration information of multiple device files.

Specify the smallest device file number (hexadecimal) before the hyphen, and specify the largest device file number (hexadecimal) after the hyphen. For example, if you are referencing the configuration information of device files located at `/dev/enas/lu0F`, `/dev/enas/lu10`, and `/dev/enas/lu11`, specify `0F-11`. When specifying multiple ranges, use a comma (`,`) as the delimiter.

If you do not specify this option, the list of available device files on a node that you executed this command is displayed.

`-e`

Specify this option to add a hash mark (`#`) to the end of the device file number for a device file that is in an external storage system.

`-v`

Specify this option to view the detailed information about the device files.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-245 Information displayed when executing the horcdevlist command

Item	Description

dev	Displays the specified device file number in the following format:
	
	Hexadecimal-notation[#1] *Type-of-storage*[#2]
	
	#1
	
	    LUNs in the range from `00` to `FF` are displayed as a 2-digit number, and LUNs in the range from `0100` to `03FF` are displayed as a 4-digit number.
	
	#2
	
	    This item is displayed when the `-e` option is specified. A space character is displayed for device files that exist in the local storage system. A hash mark (`#`) is displayed for device files that are in an external storage system.

serial	Displays the serial number of the storage system that contains the specified device file.
LDEV	Displays the LDEV number of the specified device file. When the LUN Expansion functionality is being used, the ID of the LDEV at the head of the linked LDEVs is displayed.

type	The displayed information differs depending on the model of the storage system that contains the specified device file.
	
	• For a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system
	
	    The emulation type of the device file is displayed.
	
	• For Hitachi AMS2000 and HUS100 series storage systems
	
	    `--` is always displayed.

size	Displays the size (in gigabytes) of the specified device file.
LUSE	Displays the number of LUs using the LUN Expansion functionality. `--` is displayed if the specified device file is not using the LUN Expansion functionality.

VLL	The displayed information differs depending on the model of the storage system that contains the specified device file.
	
	• For a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system
	
	    Whether the specified device file is a device file created by using the VLL functionality is displayed:
	
	    `VLL`
	
	    The specified device file is a device file created by using the VLL functionality.
	
	    `--`
	
	    The specified device file is not a device file created by using the VLL functionality.
	
	• For Hitachi AMS2000 and HUS100 series storage systems
	
	    `--` is always displayed.

Item	Description
DCTL	A hyphen (-) is always displayed.
status	Displays the status of the specified device file. Normal Displayed when the status of the specified device file is normal. Error Displayed if an error occurred in the specified device file. Acquire all the log data, and then contact maintenance personnel. Undef Displayed when the specified device file is not assigned.
used function	Displays the usage state of the device file and the names of functions that are using the device file. File: *file-system-name* Displayed when the specified device file is used within the file system. When the -c option is specified, the colon (:) is not displayed. Mig: *file-system-name* Displayed when the specified device file is being used by the function of Active File Migration. The name of the file system for which the work space is set up is displayed as the file system name. When the -c option is specified, the colon (:) is not displayed. WORM: *file-system-name* Displayed when the specified device file is being used by a WORM file system. When the -c option is specified, a colon (:) is not displayed. WORM,Mig: *file-system-name* Displayed when the specified device file is being used by the function of Active File Migration and the file system for which the work space are set up is a WORM file system. The name of the file system for which the work space are set up is displayed for the file system name. When the -c option is specified, a colon (:) is not displayed. Defined Displayed when the specified device file is reserved as the copy-destination of the file system by the functionality for linking with array volume replication functions. Free Displayed when the specified device is not being used. Unknown Displayed either when the specified device usage status has changed during the command execution, or an attempt to acquire device file configuration information failed. If Unknown is displayed, re-execute the command. If Unknown is displayed again, the processing of another command might have been cancelled. Perform the operations that are necessary when a command is cancelled, and then re-execute the horcdevlist command.

Item	Description
	If the processing of the command was not actually cancelled or the status does not change after you perform the necessary operations in the event of a command cancellation, check whether there are any failures displayed on the **List of RAS Information** page (for `List of other log files`) in the Check for Errors dialog box, and then remove the cause of any such failures. If no failures are found, acquire all the log data, and then contact maintenance personnel. `--` Displayed when the specified device file is not being used but an error has occurred in that file, or when the specified device file is not assigned (that is, when `Undef` is displayed as `status`).

`node`	Displays the relationship between the node to which you are logged in, and node on which the specified device file is being used or has been reserved.
	`Own`
	
	Displayed when the specified device file is either being used or reserved by the node to which you are logged in.
	`Other`
	
	Displayed when the specified device file is either being used by a resource group of the other node in the cluster, or being reserved by the other node in the cluster.
	`--`
	
	Displayed when the specified device file either is not being used or is not assigned (that is, when `Undef` is displayed as `status`).

`model`	Displays the model name of the storage system that contains the specified device file.
`target`	Displays the target of the specified device file.

`drive`	Displays the drive type of the specified device file.
	`FC/SAS`
	
	Displayed when the drive type is FC or SAS.
	`SAS7K`
	
	Displayed when the drive type is SAS 7.2K.
	`SATA`
	
	Displayed when the drive type is SATA.
	`SSD`
	
	Displayed when the drive type is an SSD.
	`--`
	
	Displayed in either of the following cases:
	- When the specified device file exists in an external storage system
	- When the specified device file a virtual LU in a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system.
	- When the specified device file a virtual LU that uses HUS100 series Dynamic Tiering.

Item	Description

DP	Displays whether the specified device file is a Dynamic Provisioning virtual LU.
	
	`DP`
	
	    The specified device file is a Dynamic Provisioning virtual LU.
	
	`--`
	
	    The specified device file is not a Dynamic Provisioning virtual LU.

Notes:

- When the specified device file has not been assigned:

  `--` is displayed for the items below. – is displayed for `DCTL`.

  `serial`, `LDEV`, `type`, `size`, `LUSE`, `VLL`, `DCTL`, `used function`, `node`, `model`, `target`, and `drive`

- When an error has occurred in the storage system:

  `--` is displayed for `size`.

  `LDEV`, `type`, `size`, `LUSE`, `VLL`, and `DCTL`

- When an error has occurred on the FC path:

  `--` is displayed for the items below. – is displayed for `DCTL`, and a space is displayed for *Type-of-storage*.

  Type-of-storage, `type`, `size`, `LUSE`, `VLL`, `DCTL`, `drive`, `DP`

  The information displayed for an unused device file is the same as the information displayed for an unassigned device.

Return values

Table 2-246 Return values of the horcdevlist command

Return value	Description
`0`	Normal termination
`4, 8, 9`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`14, 19, 80, 97`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`74, 91`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`90`	The error cannot be handled by the system administrator. Contact maintenance personnel.

horcexport (Disconnect the copy-destination file system from a node)

Synopsis

```
horcexport -f copy-destination-file-system-name [-nomsg]
horcexport -h
```

Description

The `horcexport` command disconnects the copy-destination file system from a node. Device files that were in use by the copy-destination file system are reserved as copy destinations.

To execute this command, the file system must have been unmounted.

If command processing is interrupted, re-execute the `horcexport` command with the same argument specified.

Options and arguments

`-f` *copy-destination-file-system-name*

Specify the name of the copy-destination file system to be disconnected from a node.

Return values

Table 2-247 Return values of the horcexport command

Return value	Description
0	Normal termination
4, 5, 6, 7	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
12, 15, 29, 69, 74, 91, 93, 95	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
14, 19, 20, 25, 28, 46, 58, 75, 76, 77, 80, 94, 97, 98	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
59	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
90	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To disconnect the copy-destination file system from a node:

```
$ sudo horcexport -f FS_1
Aug 17 04:48:15 KAQB11801-I The horcexport command has started.
Aug 17 04:48:27 KAQB11802-I The horcexport command has finished.
```

horcfreeze (Suppress access from clients to the copy-source file system)

Synopsis

```
horcfreeze -f copy-source-file-system-name [-nomsg]
horcfreeze -h
```

Description

If the copy-source file system has been mounted, the `horcfreeze` command suppresses access from clients.

Execute the `horcfreeze` command before splitting a volume pair created by using ShadowImage, TrueCopy, or Universal Replicator.

You can check the file system access suppression status by using the `fsctl` command.

Note the following points when executing the `horcfreeze` command:

- Do not perform any of the operations listed below between the time the `horcfreeze` command is executed and the time the `horcunfreeze` command is executed.

  ○ Starting or stopping a cluster, or performing a forced stop for a cluster
  ○ Starting or stopping a node, or performing a forced stop for a node
  ○ Starting or stopping a resource group, performing a forced stop for a resource group, or changing the execution node of a resource group
  ○ Mounting or deleting a copy-source file system

  Performing any of these operations might make the copy-destination file system unusable.

  Also, an attempt to unmount a file system for a file system other than the copy-source file system might fail.

- Notify CIFS clients of the file systems to which you want to suppress access. If a CIFS client accesses a file system to which you have suppressed access, the CIFS client will no longer be able to access any file system.

- When the `horcfreeze` command is executed, the specified file system temporarily cannot be accessed. For this reason, access to the file system

from a client might time out. After completing the required operations, execute the `horcunfreeze` command as soon as possible.

- After you execute the `horcfreeze` command to split the volume pair created by ShadowImage, TrueCopy, or Universal Replicator immediately execute the `horcunfreeze` command. After you execute the `horcfreeze` command, if you execute an operation other than splitting the volume pair on the mounted file system before you execute the `horcunfreeze` command, then it might take a long time for processing to start, and a timeout might occur.

- If the `horcfreeze` command is executed while the `dpreclaim` command is being executed to release unused areas in virtual LUs used by the file system, processing for the `horcfreeze` command might time out. Complete the processing to release unused areas in virtual LUs before executing the `horcfreeze` command.

- If command processing is interrupted, re-execute the `horcfreeze` command with the same argument specified.

Options and arguments

`-f` *copy-source-file-system-name*
> Specify the name of the copy-source file system for which you want to suppress access from clients.

Return values

Table 2-248 Return values of the horcfreeze command

Return value	Description
0	Normal termination
4, 5, 6, 7	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
14, 19, 20, 26, 27, 80, 97, 98	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
73, 74, 91, 93, 95	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
82, 83, 90, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To suppress access from clients to the copy-source file system:

```
$ sudo horcfreeze -f FS_1
Aug 17 01:50:59 KAQB11801-I The horcfreeze command has started.
Aug 17 01:51:02 KAQB11802-I The horcfreeze command has finished.
```

horcimport (Connect the copy-destination file system to the node when a volume manager is not being used)

Synopsis

```
horcimport -f copy-destination-file-system-name
    -d device-file-number [-r resource-group-name] [-nomsg]
horcimport -h
```

Description

The `horcimport` command connects the copy-destination file system for which a volume pair created by ShadowImage, TrueCopy, or Universal Replicator has been split to the node. If a copy-destination file system that was created without using a volume manager is to be connected to the node, use the `horcimport` command. Note that this command cannot connect a WORM file system to the node.

If TrueCopy or Universal Replicator is used, the pair must be split, specifying the Read/Write mode.

The limit on the total number of file systems (including the copy-destination file systems to be connected to) is 256 per single node, and 511 per cluster.

The following settings of the copy-source file system are copied to the copy-destination file system:

• ACL type of the file system
• Setting for whether to allow creation of hard links
• Warning notification settings for file system usage
• Settings for the automatic-failover functionality used when a file system is blocked
• Quota settings
• Subtree quota settings

Other settings might differ from those of the copy-source file system. After connecting the copy-destination file system, check the setting values.

If command processing is interrupted, re-execute the `horcimport` command with the same argument specified.

Note:
    If the copy-destination file system to be connected to the node was set up by using a volume manager, use the `horcvmimport` command.

Options and arguments

-d *device-file-number*

Specify the number of the device file that was used as the copy-destination file system. For example, if the path of the device file is `/dev/enas/lu0F`, specify `0F`.

-f *copy-destination-file-system-name*

Specify the name of the copy-destination file system by using no more than 16 characters. You can use alphanumeric characters and underscores (_). Do not specify a name that already exists for a file system in the cluster.

-r *resource-group-name*

Specify the name of the resource group in which you want to register the copy-destination file system. When executing the command with a virtual IP address specified, specify the name of a resource group with the `-r` option in case of a failover. If you do not specify this option, the copy-destination file system is registered in the resource group that belongs to the node on which the command is executed.

Return values

Table 2-249 Return values of the horcimport command

Return value	Description
0	Normal termination
4, 5, 6, 7, 8, 9	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
14, 19, 22, 24, 30, 31, 40, 41, 44, 45, 47, 48, 50, 51, 52, 54, 80, 88, 89, 94, 97, 98	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
74, 91, 93	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
87	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
90, 92, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To connect a copy-destination file system created without using a volume manager to the node:

```
$ sudo horcimport -f FS_1 -d 01
Aug 17 04:46:53 KAQB11801-I The horcimport command has started.
Aug 17 04:47:04 KAQB11802-I The horcimport command has finished.
```

horclogremove (Delete CCI logs)

Synopsis

```
horclogremove [-i instance-number] [-nomsg]
horclogremove -h
```

Description

The `horclogremove` command deletes the log files and traces output by the CCI daemon.

This command is applied to the node on which the command is executed. This command must be executed on both nodes.

Before executing this command, you must stop the CCI daemon that outputs logs.

Options and arguments

-i *instance-number*

Specify the daemon instance number to delete the log files and traces output by the daemon that has the specified instance number.

`16`, `17`, or `20` to `499` can be specified for the instance number.

If you do not specify this option, the command will use the instance number set in the environment variable `HORCMINST`.

Return values

Table 2-250 Return values of the horclogremove command

Return value	Description
0	Normal termination
4	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
13, 14, 19, 56, 57, 64, 80	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
74	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation.

Return value	Description
	If this error occurs repeatedly, contact maintenance personnel.

horcprintenv (Display the CCI environment variable)

Synopsis

```
horcprintenv [environment-variable-name] [-nomsg]
horcprintenv -h
```

Description

The `horcprintenv` command displays the value of the specified CCI environment variable that will take effect the next time you log in.

You can view the values set for the following environment variables:

- `HORCC_MRCF`
- `HORCC_REST`
- `HORCC_RSYN`
- `HORCC_SPLT`
- `HORCMINST`

Options and arguments

environment-variable-name

Specify the name of the CCI environment variable. Specify this argument when you want to view a specific environment variable. If you do not specify an argument, only environment variables (from `HORCC_MRCF`, `HORCC_REST`, `HORCC_RSYN`, `HORCC_SPLT`, or `HORCMINST`) for which values have been set are displayed.

Displayed information

The following table lists the information displayed as the CCI environment variable.

Table 2-251 Information displayed by executing the horcprintenv command

Item	Description
environment variable	Displays the name of the CCI environment variable.
value	Displays the value set up in the environment variable.

Table 2-252 Return values of the horcprintenv command

Return value	Description
0	Normal termination
4	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 14, 19, 80	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
74	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
86	The error cannot be handled by the system administrator. Contact maintenance personnel.

horcsetconf (Add a CCI instance)

Synopsis

```
horcsetconf -i instance-number [-nomsg]
horcsetconf -h
```

Description

The `horcsetconf` command adds a CCI instance for the specified instance number.

For one node, a maximum of 16 instances can be added by executing this command. This is in addition to the 2 instances that are generated when the system is installed.

In cluster configurations, this command also executes processing on the other node in the cluster.

If command processing is interrupted, re-execute the `horcsetconf` command with the same argument specified.

Options and arguments

`-i` *instance-number*

  Specify an instance number to be assigned to the CCI instance that will be created.
  You can specify a value from `20` to `499` for the instance number.

Make sure that you specify an instance number that is not currently in use on either node. To check the instance numbers that are in use on the nodes, execute the `horcconflist` command.

Return values

Table 2-253 Return values of the horcsetconf command

Return value	Description
0	Normal termination
4, 60	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
13, 14, 19, 61, 62, 63, 80	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
38	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
74	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Example

To add a CCI instance for instance number 123:

```
$ sudo horcsetconf -i 123
Aug 17 01:08:29 KAQB11801-I The horcsetconf command has started.
Aug 17 01:08:29 KAQB11802-I The horcsetconf command has finished.
```

horcsetenv (Set up or modify the CCI environment variable)

Synopsis

```
horcsetenv environment-variable-name setting-value [-nomsg]
horcsetenv -h
```

Description

The `horcsetenv` command sets up or modifies the values specified in the following CCI environment variables:

- HORCC_MRCF
- HORCC_REST

- `HORCC_RSYN`
- `HORCC_SPLT`
- `HORCMINST`

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

After you have executed this command, the specified environment variable setting is applied automatically when you log in to the node via SSH or when CCI commands are executed automatically by a shell script you create. Note that the values of the environment variables set by this command are applied only on the node on which the command is executed.

If you execute this command when you are logged in to the node via SSH, the specified environment variable setting takes effect the next time you log in. If you create a shell script to execute this command automatically, the specified value will take effect once the command finishes executing.

Do not execute this command while a shell script that automatically executes a CCI command is running. If you execute this command by mistake, the environment variable will be changed during the operation, and the CCI command might be executed using a non-assumed value.

If command processing is interrupted, re-execute the `horcsetenv` command with the same argument specified.

Options and arguments

environment-variable-name
 Specify the name of the environment variable to be set up or modified.

setting-value
 Specify the value to be set for the environment variable. The following table shows the values set for each environment variable.

Table 2-254 Values set for the environment variables that are set up or modified by the horcsetenv command

Environment variable	Description
`HORCC_MRCF`	Sets whether you want to use CCI commands for ShadowImage, or for TrueCopy or Universal Replicator.
	If you want to use ShadowImage for the functionality for linking with array volume replication functions, specify `1`. Do not specify any value if you want to use TrueCopy or Universal Replicator for the functionality for linking with array volume replication functions.
`HORCC_REST`	Sets the pair synchronization mode when the paired volumes are synchronized in the reverse direction.
	You can specify `NORMAL` or `QUICK` when you use ShadowImage for the functionality for linking with array volume replication functions.

Environment variable	Description
HORCC_RSYN	Sets the pair synchronization mode when the paired volumes are resynchronized.
	You can specify NORMAL or QUICK when you use ShadowImage for the functionality for linking with array volume replication functions.
HORCC_SPLT	Sets the split type used when the volume pair is split.
	You can specify NORMAL or QUICK when you use ShadowImage for the functionality for linking with array volume replication functions.
HORCMINST	Sets the CCI instance number.
	Specify 16, 17, or 20 to 499.

Return values

Table 2-255 Return values of the horcsetenv command

Return value	Description
0	Normal termination
4	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
14, 19, 64, 80	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
74	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
86	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To set up the CCI environment variable:

```
$ sudo horcsetenv HORCC_MRCF 1
Aug 17 01:09:15 KAQB11801-I The horcsetenv command has started.
Aug 17 01:09:15 KAQB11879-W Settings are applied only to the node on which
the command was executed. Apply the same settings to the other node in the
cluster as necessary.
Aug 17 01:09:15 KAQB11802-I The horcsetenv command has finished.
```

horcunfreeze (Re-open access from clients to the copy-source file system)

Synopsis

```
horcunfreeze -f copy-source-file-system-name [-nomsg]
horcunfreeze -h
```

Description

If the copy-source file system has been mounted, the `horcunfreeze` command re-opens access to the copy-source file system from clients.

Execute the `horcunfreeze` command after splitting the volume pair created by ShadowImage, TrueCopy or Universal Replicator.

You can check the file system access suppression status by using the `fsctl` command.

If command processing is interrupted, re-execute the `horcunfreeze` command with the same argument specified.

Options and arguments

`-f` *copy-source-file-system-name*

Specify the name of the copy-source file system for which you want to re-open access from clients.

Return values

Table 2-256 Return values of the horcunfreeze command

Return value	Description
`0`	Normal termination
`4, 5, 6, 7`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`14, 19, 20, 26, 27, 80, 97`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`73, 74, 91, 93, 95`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`84, 85, 90, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To re-open access to the copy-source file system from clients:

```
$ sudo horcunfreeze -f FS_1
Aug 17 01:52:27 KAQB11801-I The horcunfreeze command has started.
Aug 17 01:52:29 KAQB11802-I The horcunfreeze command has finished.
```

horcunsetconf (Delete a CCI instance)

Synopsis

```
horcunsetconf -i instance-number [-y] [-nomsg]
horcunsetconf -h
```

Description

The `horcunsetconf` command deletes a CCI instance for the specified instance number.

In cluster configurations, the `horcunsetconf` command also executes processing on the other node in the cluster.

Before executing this command, you need to stop the daemon for the instance number that will be deleted on both nodes.

If command processing is interrupted, re-execute the `horcunsetconf` command with the same argument specified.

Options and arguments

`-i` *instance-number*

> Specify the instance number for the CCI instance that you want to delete. You can specify a value from `20` to `499` for the instance number.

Return values

Table 2-257 Return values of the horcunsetconf command

Return value	Description
0	Normal termination
4, 60	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
13, 14, 19, 61, 64, 65, 80	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
39	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
74	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

horcunsetenv (Delete the CCI environment variable)

Synopsis

```
horcunsetenv environment-variable-name [-nomsg]
horcunsetenv -h
```

Description

The `horcunsetenv` command deletes a CCI environment variable and prevents the environment variable from being set the next time you log in. You can delete the following environment variables:

- `HORCC_MRCF`
- `HORCC_REST`
- `HORCC_RSYN`
- `HORCC_SPLT`

  Note:

    The environment variable `HORCMINST` cannot be deleted.

This command deletes the specified environment variable from only the node on which the command is executed. This command must be executed on both nodes.

If you execute this command when you are logged in to the node via SSH, the specified environment variable will be deleted the next time you log in. If you create a shell script and execute this command automatically, the environment variable will be deleted once the command finishes executing.

Do not execute this command while a shell script that automatically executes a CCI command is running. If you execute this command by mistake, the environment variable will be deleted during the operation, and the CCI command might be executed using a non-assumed value.

If command processing is interrupted, re-execute the `horcunsetenv` command with the same arguments specified.

Options and arguments

environment-variable-name

Specify the name of the environment variable to be deleted.

Return values

Table 2-258 Return values of the horcunsetenv command

Return value	Description
0	Normal termination
4	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
11, 14, 19, 80	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
74	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
86	The error cannot be handled by the system administrator. Contact maintenance personnel.

horcvmdefine (Reserve device files)

Synopsis

```
horcvmdefine -d device-file-number[,device-file-number...]
    [-nomsg]
horcvmdefine -h
```

Description

The `horcvmdefine` command reserves the device file that will be used as the copy-destination of a file system.

Before creating or re-synchronizing a copy-destination file system by using ShadowImage, TrueCopy, or Universal Replicator, reserve the device file that is to be used as the copy-destination of the file system. By reserving the device file, you will prevent other system administrators from using the specified device file when they perform operations such as creating a file system.

If command processing is interrupted, re-execute the `horcvmdefine` command with the same arguments specified.

Options and arguments

-d *device-file-number* [, *device-file-number* ...]

> Specify the number of the device file to be used as the copy-destination of the file system. For example, if the path of the target device file is /dev/enas/lu0F, specify 0F. When specifying multiple device files, specify all the device file numbers, separated by commas (,).

> If you specify multiple device files, make sure that all the specified device files are located in the same storage system.

Return values

Table 2-259 Return values of the horcvmdefine command

Return value	Description
0	Normal termination
4, 8, 9, 78	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
14, 19, 40, 43, 44, 45, 47, 48, 80, 97, 98	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
74, 91	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
90, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To reserve a device file that is to be used as the copy-destination of a file system:

```
$ sudo horcvmdefine -d 19,1A,1B
Aug 17 01:12:53 KAQB11801-I The horcvmdefine command has started.
Aug 17 01:13:04 KAQB11802-I The horcvmdefine command has finished.
```

horcvmdelete (Release device files)

Synopsis

```
horcvmdelete -d device-file-number[,device-file-number...]
    [-nomsg]
horcvmdelete -h
```

Description

The `horcvmdelete` command releases a device file reserved by the `horcvmdefine` command if a volume pair created by ShadowImage, TrueCopy, or Universal Replicator has been deleted without connecting the copy-destination file system to the node.

This command also releases the device file reserved by the node that is not the node the command was executed on.

If command processing is interrupted, re-execute the `horcvmdelete` command with the same arguments specified.

Options and arguments

`-d` *device-file-number* [, *device-file-number* . . .]
Specify the number of the device file used for the copy-destination file system. For example, if the path of the target device file is `/dev/enas/lu0F`, specify `0F`. When multiple device files make up the copy-destination file system, specify all the device file numbers, separated by commas (,).

Return values

Table 2-260 Return values of the horcvmdelete command

Return value	Description
0	Normal termination
4, 8, 9	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
14, 19, 40, 43, 45, 47, 48, 80, 97	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
74, 91	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
90, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To release the device file for the copy-destination file system:

```
$ sudo horcvmdelete -d 19,1A,1B
Aug 17 01:14:12 KAQB11801-I The horcvmdelete command has started.
Aug 17 01:14:20 KAQB11802-I The horcvmdelete command has finished.
```

horcvmimport (Connect a copy-destination file system to a node when a volume manager is being used)

Synopsis

```
horcvmimport -f copy-destination-file-system-name
    -d device-file-number[,device-file-number...]
    [-r resource-group-name] [-nomsg]
horcvmimport -h
```

Description

When a volume pair created by ShadowImage, TrueCopy, or Universal Replicator has been split, the `horcvmimport` command connects the copy-destination file system to the node. This command needs to be used if the copy-destination file system to be connected to the node has been set up by using a volume manager. Note that this command cannot connect a WORM file system to the node.

If TrueCopy or Universal Replicator is used, the pair must be split with Read/Write mode specified.

The limit on the total number of file systems (including the copy-destination file systems to be connected to) is 256 per single node, and 511 per cluster.

The following settings of the copy-source file system are copied to the copy-destination file system:

- ACL type of the file system
- Setting for whether to allow creation of hard links
- Warning notification settings for file system usage
- Settings for the automatic-failover functionality used when a file system is blocked
- Quota settings
- Subtree quota settings

Other settings might differ from those of the copy-source file system. After connecting the copy-destination file system, check the setting values.

If command processing is interrupted, re-execute the `horcvmimport` command with the same arguments specified.

Note:
   If the copy-destination file system to be connected to the node was set up without using a volume manager, use the `horcimport` command.

Options and arguments

-d *device-file-number* [, *device-file-number* ...]
   Specify the number of the device file that was used as the copy-destination file system. For example, if the path of the target device file is `/dev/enas/lu0F`, specify `0F`. When multiple device files make up the

copy-destination file system, specify all the device file numbers, separated by commas (,). You can specify a maximum of 256 device files.

If you specify multiple device files, make sure that all the specified device files are located in the same storage system.

-f *copy-destination-file-system-name*

Specify the name of the copy-destination file system by using no more than 16 characters. You can use alphanumeric characters and underscores (_). Do not specify a name that already exists for a file system in the cluster.

-r *resource-group-name*

Specify the name of the resource group in which you want to register the copy-destination file system. When executing the command with a virtual IP address specified, specify the name of a resource group with the -r option in case of a failover. If you do not specify this option, the copy-destination file system is registered in the resource group that belongs to the node on which the command is executed.

Return values

Table 2-261 Return values of the horcvmimport command

Return value	Description
0	Normal termination
4, 5, 6, 7, 8, 9, 78	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
14, 19, 22, 24, 30, 31, 40, 42, 44, 45, 47, 48, 49, 50, 51, 53, 54, 55, 80, 88, 89, 94, 97, 98	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
74, 91, 93	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
87	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
90, 92, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To connect a copy-destination file system that was created by using a volume manager to the node:

```
$ sudo horcvmimport -f FS_1 -d 19,1A,1B
Aug 17 01:55:22 KAQB11801-I The horcvmimport command has started.
Aug 17 01:55:39 KAQB11802-I The horcvmimport command has finished.
```

hwstatus (Display the hardware status)

Synopsis

```
hwstatus [-h]
```

Description

Displays the status of hardware on the node to which you are logged in.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-262 Information displayed when executing the hwstatus command

Item	Description	
Model Information	The model name is displayed in the following format: *manufacturer product-name* If the information cannot be acquired, a hyphen (-) is displayed for each item.	
SerialNumber Information	The device identification number is displayed. Any spaces in the device identification number are replaced with hyphens (-). If the information cannot be acquired, a hyphen (-) is displayed.	
Fan Information	Displays information about the fans in the following format: *index-number fan-status vendor-specific-detailed-information* If the information cannot be acquired, a hyphen (-) is displayed for each item.	

	fan-status	Displays the fan status.
		 `ok`
		     The fan is normal.
		 `failed`
		     An error occurred or the fan has not been installed.

	vendor-specific-detailed-information	Displays detailed information specific to the fan vendor.

Item	Description	
`Temperature Information`	Displays temperature information in the following format: *index-number temperature-sensor-detection-results vendor-specific-detailed-information* If the information cannot be acquired, a hyphen (-) is displayed for each item.	

	temperature-sensor-detection-results	Displays the detected results of the temperature sensor.
		`ok`
		　The results are normal.
		`failed`
		　The results are abnormal.

	vendor-specific-detailed-information	Displays detailed information specific to the temperature sensor vendor.
`PowerSupply Information`	Displays information about the power supply units in the following format: *index-number power-supply-unit-status vendor-specific-detailed-information* If information could not be acquired or in the case of HDI Remote Server, a hyphen (-) is displayed for each item.	

	power-supply-unit-status	Displays the power supply unit status.
		`ok`
		　The power supply unit is normal.
		`failed`
		　An error occurred.
		`not_installed`
		　The power supply unit has not been installed.

	vendor-specific-detailed-information	Displays detailed information specific to the power supply unit vendor.
`Memory Information`	Displays information about memory in the following format: *index-number memory-status vendor-specific-detailed-information* If the information cannot be acquired, a hyphen (-) is displayed for each item.	

	memory-status	Displays the memory status.
		`installed`
		　Memory is installed.
		`not_installed`
		　Memory has not been installed.

	vendor-specific-detailed-information	Displays detailed information specific to the memory vendor.

Item	Description
`MemoryTotal` `Information`	Displays the information about the total memory capacity in the following format: *index-number* `size:`*memory-capacity-recognized-by-the-system*`(`*installed-memory-capacity*`)* If the information cannot be acquired, a hyphen (-) is displayed for each item. Note that the memory capacity recognized by the system is displayed less than the installed memory capacity depending on the system configuration.
`InternalHDD` `Information`	Displays information about the internal HDDs in the following format: *index-number internal-HDD-status vendor-specific-detailed-information* If the information cannot be acquired or internal HDDs are not mounted, a hyphen (-) appears for each item.

	internal-HDD-status	Displays the status of the internal HDD.
		`ok`
		    The hard disk is normal.
		`rebuild`
		    The hard disk is currently being formatted or RAID is being constructed.
		`failed`
		    An error occurred.
		`removed`
		    The hard disk was removed from the RAID group.
		`nodevice`
		    The hard disk was removed from the node.
		`setup`
		    The hard disk installed on the node is not included in the RAID group.
		`not_supported`
		    Displayed if a program for acquiring information is not installed.

	vendor-specific-detailed-information	Displays detailed information specific to the internal-HDD vendor.

Item	Description
`InternalRAIDBattery` `Information`	Displays information about the internal RAID batteries in the following format: *index-number internal-RAID-battery-status vendor-specific-detailed-information* If the information cannot be acquired, internal RAID batteries are not mounted, or the monitoring of internal RAID batteries is not required, a hyphen (-) is displayed for each item.

Command Reference

Item		Description

	internal-RAID-battery-status	Displays the status of the internal RAID battery.
		
		`ok`
		    The battery has been charged.
		
		`charging`
		    The battery is being charged.
		
		`failed`
		    An error occurred.
		
		`not_supported`
		    A program for acquiring information is not installed.

	vendor-specific-detailed-information	Displays detailed information specific to the internal RAID battery vendor.
`BMC Information`		Displays the BMC status of the node you are logged in to and the status of the connection with the other node. The BMC status is not displayed in the case of HDI Remote Server.

	`status`	Displays the BMC status of the node you are logged in to.
		
		`ok`
		    The status is normal.
		
		`Unknown!`
		    The information cannot be acquired.

	`connection`	Displays the status of the connection with the other node if a cluster configuration is used.
		
		`ok`
		    The connection is normal.
		
		`failed`
		    Communication with the BMC on the other node has failed.
		
		`none`
		    A cluster configuration has not been defined or information acquisition has failed.

`Network Interface`		Displays information about the network interface in the following format: *port-name port-status communication-speed media-type port-type* The port type is not displayed for data ports. A port whose information cannot be acquired is not displayed. If information cannot be acquired for any ports, a line of hyphens (-) is displayed.
	port-name	Displays the name of the port.

Item	Description

	`mng0`
	    Management port
	`hb0`
	    Heartbeat port
	`pm` *number*
	    Private maintenance port
	`eth` *number* or `xgbe` *number*
	    Data port

port-status	Displays the status of the port.
	`up`
	    The link is normal.
	`down`
	    The link is disconnected.

communication-speed	Displays the communication speed of the port in the following format:
	`linkspeed:`*communication-speed*
	The communication speed is displayed as follows:
	`10Base`
	    10 Mbps
	`100Base`
	    100 Mbps
	`1000Base`
	    1 Gbps
	`10000Base`
	    10 Gbps
	`Unknown!`
	    The communication speed is unknown.

media-type	Displays the media type of the port in the following format:
	`mediatype:` *media-type*
	The media type is displayed as follows:
	`Copper`
	    A metal cable can be used.
	`Fiber`
	    An optical cable can be used.

port-type	Displays the port type.
	`Management port`
	    Management port
	`Heartbeat port`
	    Heartbeat port
	`Private maintenance port`

Item	Description	
	Private maintenance port	
`FC Port Information`	FC port information is displayed in the following format:	
	`FC-port-name FC-port-status vendor-specific-detailed-information`	
	If the information cannot be acquired, a hyphen (-) is displayed for each item.	
	For a single-node configuration, this information is displayed if a storage system is connected.	
	FC-port-name	FC port names arranged in ascending order are displayed in the following format: `fc Hexadecimal-notation`
	FC-port-status	Displays the status of the FC port. `up` The link is normal. `down` The link is disconnected.
	vendor-specific-detailed-information	Host port WWN and communication speeds are displayed as information specific to HBA card vendors.

Return values

Table 2-263 Return values of the hwstatus command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`80`	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
`99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

Hitachi Data Ingestor CLI Administrator's Guide

ifadd (Add an interface)

Synopsis (for cluster configurations)

```
ifadd [-p {v4|v6}] -a [fixed-IP-address1:fixed-IP-address2]
    [-s [virtual-IP-address1]:[virtual-IP-address2]]
    [-S virtual-server-name=virtual-IP-address
    [,virtual-server-name=virtual-IP-address...]]
    -n netmask [-m MTU-value] interface
```

Synopsis (for single node configurations)

```
ifadd [-p {v4|v6}] -a IP-address
    -n netmask [-m MTU-value] interface
```

Synopsis (to reference the command syntax)

```
ifadd -h
```

Description

Adds an interface. Before executing this command, check the information in *Before managing an interface:* in Configuring the system on page 3-20.

You cannot specify a fixed IP address or virtual IP address from the networks below.

- 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`"
- The network of an IP address set in the private maintenance port

  You can use the `pmctl` command to check the network that contains the IP address set for the maintenance port.
- The network of an IP address set in the heartbeat port

  You can use the `clstatus` command to check the network that contains the IP address set for the heartbeat port.

If you use File Services Manager from the data port, do not set a tagged VLAN on the management port.

Options and arguments

`-a` *fixed-IP-address1* : *fixed-IP-address2*

The above syntax is for cluster configurations.

You can omit this option when adding an interface to a port other than `mng0`.

Specify the fixed IP address of the node to which you are logged in followed by a colon (`:`) and the fixed IP address of the other node in the cluster.

`-a` *IP-address*

The above syntax is for single-node configurations.

Specify the IP address of the node to which you are logged in.

`-m` *MTU-value*

Specify the MTU value of the interface. You can specify a value in the range from 1,280 to 9,216 for a GbE port, and in the range from 1,280 to 16,110 for a 10GbE port. However, depending on the hardware type and configuration, the maximum specifiable value might be 9,000 for a GbE port and 9,600 for a 10GbE port.

If you omit this option, `1,500` is set. However, if you omit this option when adding an address of a different protocol, the MTU value that has been set is used. The value you specify will be set in both the IPv4 and IPv6 environments. Note that the MTU value `mng0` cannot be added.

`-n` *netmask*

For IPv4, specify the netmask. The value you specify is used as the netmask for the fixed IP addresses and virtual IP addresses.

For IPv6, specify the prefix length. The value you specify is used as the prefix length for the fixed IP addresses and virtual IP addresses.

`-p {v4|v6}`

Specify the protocol version of the interface to be added. If you omit this option, `v4` or `v6` is automatically set according to the protocol version determined from the specified IP address.

`v4`

Specify this to use IPv4 IP addresses.

`v6`

Specify this to use IPv6 IP addresses.

`-s` [*virtual-IP-address1*] `:` [*virtual-IP-address2*]

Specify the virtual IP address for the resource group on the node to which you are logged in followed by a colon (`:`) and the virtual IP address for the resource group on the other node in the cluster.

If you omit this option or specify `-s :`, no virtual IP addresses for the resource group is set. This enables you to exclude those resource groups from the monitoring targets, preventing a failover when an error occurs.

`-S` *virtual-server-name = virtual-IP-address* [, *virtual-server-name = virtual-IP-address* ...]

This option is not supported.

interface

Specify the name of the port to which you want to add the interface.
You can specify the following port names. Specify an integer of 0 or more for *number*.

- `eth` *number*
- `agr` *number*
- `rdn` *number*

- ○ `xgbe` *number*
- ○ `mng0`[#]

This name can be added when IPv6 is used.

If a tagged VLAN is used, specify it in the format below. Note that the range of VLAN IDs you can specify is from 1 to 4094.

port-name.VLAN-ID

Return values

Table 2-264 Return values of the ifadd command

Return value	Description
`0`	Normal termination
`1, 2`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10, 11, 13, 14, 15, 66`[#]`, 67, 69, 70, 71`[#]`, 72`[#]`, 74, 75, 76, 77`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65, 66`[#]`, 68`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`66`[#]`, 71`[#]`, 72`[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`97, 98, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Examples

To add an interface to the data port `eth12` under the following conditions:

- ○ The fixed IP addresses are `172.19.23.31` and `172.19.23.32`.
- ○ The virtual IP addresses are `172.19.23.33` and `172.19.23.34`.
- ○ The netmask is `255.255.255.0`.
- ○ The MTU value is `9216`.

```
$ sudo ifadd -a 172.19.23.31:172.19.23.32 -s 172.19.23.33:172.19.23.34 -n
255.255.255.0 -m 9216 eth12
```

To add an interface that uses a tagged VLAN (VLAN ID: 1000) for the data port (`eth12`):

- ○ The fixed IP addresses are `172.20.23.3` and `172.20.23.4`.
- ○ The virtual IP addresses are `172.20.23.5` and `172.20.23.6`.
- ○ The netmask is `255.255.255.0`.

```
$ sudo ifadd -a 172.20.23.3:172.20.23.4 -s 172.20.23.5:172.20.23.6 -n
255.255.255.0 eth12.1000
```

To add an interface to the data port (`eth12`) by using IPv6 IP addresses:

- ○ The fixed IP addresses are `fd00::1:1` and `fd00::1:2`.
- ○ The virtual IP addresses are `fd00::1:3` and `fd00::1:4`.
- ○ The prefix length is `64`.

```
$ sudo ifadd -p v6 -a [fd00::1:1]:[fd00::1:2] -s [fd00::1:3]:[fd00::1:4] -
n 64 eth12
```

ifdel (Delete an interface)

Synopsis

```
ifdel [-p {v4|v6|all}] [-f] [-V] interface
ifdel --all [-f] [-V]
ifdel -h
```

Description

Deletes an interface.

Before executing this command, check the information in *Before managing an interface:* in Configuring the system on page 3-20.

Options and arguments

`--all`

Specify this to delete all interfaces except the one for the management port.

`-f`

Specify this to prevent the confirmation message from appearing.

`-p {v4|v6|all}`

Specify the protocol version of the interface to be deleted. If you omit this option, `v4` is set.

`v4`

Specify this to delete an interface configured for IPv4.

`v6`

Specify this to delete an interface configured for IPv6.

`all`

Specify this to delete interfaces configured for IPv4 and IPv6.

`-V`

Specify this to display the progress of the deletion processing.

interface

Specify the name of the port from which to delete the interface. You cannot delete the interface of the management port.

If a tagged VLAN is used, specify it in the following format:

port-name.VLAN-ID

Return values

Table 2-265 Return values of the ifdel command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
3, 10, 11, 15, 66[#], 69, 70, 71[#], 72[#], 74, 75	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#], 68	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71[#], 72[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Examples

To delete all interfaces except the interface of the management port:

```
$ sudo ifdel --all -V
KAQM05097-Q Do you want to delete all the interfaces? In a cluster
configuration, if there are no virtual IP addresses (service IP addresses)
set for the active resource group, the CIFS service will stop. Set a
virtual IP address, and then restart the CIFS service. (y/n)
```

To delete an interface configured with IPv6 IP addresses from the data port
(eth12):

```
$ sudo ifdel -p v6 eth12
KAQM05202-Q Do you want to delete the specified IP address of this
protocol version? In a cluster configuration, if there are no virtual IP
addresses (service IP addresses) set for the active resource group, the
CIFS service will stop. Set a virtual IP address, and then restart the
CIFS service. (y/n)
```

ifedit (Edit an interface)

Synopsis (for cluster configurations)

```
ifedit [-p {v4|v6}] [-a [fixed-IP-address1]:[fixed-IP-address2]]
    [-s [virtual-IP-address1]:[virtual-IP-address2]]
    [-S virtual-server-name=virtual-IP-address
    [,virtual-server-name=virtual-IP-address...]]
    [-n netmask] [-m MTU-value] interface
```

Synopsis (for single node configurations)

```
ifedit [-p {v4|v6}] [-a IP-address]
    [-n netmask] [-m MTU-value] interface
```

Synopsis (to reference the command syntax)

```
ifedit -h
```

Description

Changes an interface. Before executing this command, check the information
in *Before managing an interface:* in Configuring the system on page 3-20.

You cannot use this command to change the settings of interfaces configured
by using DHCP. To disable DHCP and manually set the IP address for an
interface, execute the dhcpset command with the --off option specified.

Before you can change the interface settings, the interface of the relevant
protocol version must have already been added.

You cannot specify a fixed IP address or virtual IP address from the networks
below.

- 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"

- The network of an IP address set in the private maintenance port

  You can use the `pmctl` command to check the network that contains the IP address set for the maintenance port.

- The network of an IP address set in the heartbeat port

  You can use the `clstatus` command to check the network that contains the IP address set for the heartbeat port.

When you change the network address of the management port in a cluster configuration, you must specify the same network address for the BMC port.

Hitachi AMS 2000 series and HUS 100 series controllers do not support tagged VLANs. If you configure a tagged VLAN on the management port, you will be unable to manage the storage system from the management server. When managing an HDI system from a data port, do not configure a tagged VLAN on the management port.

Releasing all the fixed and virtual IP addresses associated with an interface does not delete the interface itself. To delete an interface, use the `ifdel` command.

If you omit any of the following options, the current setting information applies.

Options and arguments

−a [*fixed-IP-address1*] : [*fixed-IP-address2*]

The above syntax is for cluster configurations.

To change fixed IP addresses, specify the fixed IP address of the node to which you are logged in followed by a colon (:) and the fixed IP address of the other node in the cluster.

If you specify −a: on its own without an IP address, the command releases the fixed IP addresses for both nodes. You cannot delete the IP address of one node but not the other.

−a *IP-address*

The above syntax is for single-node configurations.

To change an IP address, specify the IP address of the node to which you are logged in.

−m *MTU-value*

Specify the new MTU value of the interface. The value you specify will be set in both the IPv4 and IPv6 environments. Note that the MTU value of `mng0` cannot be changed.

−n *netmask*

For IPv4, specify a netmask. The value you specify is used as the netmask for the fixed IP addresses and virtual IP addresses.

For IPv6, specify a prefix length. The value you specify is used as the prefix length for the fixed IP addresses and virtual IP addresses.

−p {v4|v6}

Specify the protocol version of the interface to be changed. If you omit this option, the protocol version determined from the specified IP address is set. If a protocol version cannot be determined, `v4` is set.

`v4`

Specify this to use IPv4 IP addresses.

`v6`

Specify this to use IPv6 IP addresses.

`-s` [*virtual-IP-address1*] `:` [*virtual-IP-address2*]

To change virtual IP addresses, by using a colon (`:`) as a delimiter, specify the virtual IP address for the resource group on the node to which you are logged in followed by a colon (`:`) and the virtual IP address for the resource group on the other node in the cluster.

If you omit the IP addresses by specifying `-s :`, this command releases the virtual IP addresses for the resource groups on both nodes. If you omit the IP address specification for either node, the virtual IP address set for the resource group on the node for which you omitted the specification is deleted.

`-S` *virtual-server-name* = *virtual-IP-address* [, *virtual-server-name* = *virtual-IP-address* . . .]

This option is not supported.

interface

Specify the name of the port whose interface you want to change.

If a tagged VLAN is used, specify it in the format below. Note that the range of VLAN IDs you can specify is from 1 to 4094.

`port-name.VLAN-ID`

Return values

Table 2-266 Return values of the ifedit command

Return value	Description
0	Normal termination
1, 2	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 11, 12, 13, 15, 16, 66[#], 69, 70, 71[#], 72[#], 73[#], 74, 75, 76, 77	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#], 68	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
66[#], 71[#], 72[#], 73[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

    The command ended abnormally due to multiple causes.

Examples

To change the interface of the data port `eth12` under the following conditions:

- Change the fixed IP addresses to `172.19.23.31` and `172.19.23.32`.
- Change the virtual IP address to `172.19.23.33` and `172.19.23.34`.
- Change the netmask to `255.255.255.0`.
- Change the MTU value to `9216`.

```
$ sudo ifedit -a 172.19.23.31:172.19.23.32 -s 172.19.23.33:172.19.23.34 -n
255.255.255.0 -m 9216 eth12
```

To change the interface that uses a tagged VLAN (VLAN ID: 1000) for the data port (`eth12`):

- Change the fixed IP addresses to `172.20.23.3` and `172.20.23.4`.
- Clear the virtual IP address for the resource group on the node you are logged in to.
- Change the virtual IP address for the resource group on the other node to `172.20.23.6`.

```
$ sudo ifedit -a 172.20.23.3:172.20.23.4 -s :172.20.23.6 eth12.1000
```

To change an interface configured with IPv6 IP addresses for the data port (`eth12`):

- Change the fixed IP addresses to `fd00::1:5` and `fd00::1:6`.
- Change the virtual IP addresses to `fd00::1:7` and `fd00::1:8`.
- Change the prefix length to `64`.

```
$ sudo ifedit -p v6 -a [fd00::1:5]:[fd00::1:6] -s [fd00::1:7]:[fd00::1:8] -
n 64 eth12
```

iflist (List interface information)

Synopsis

```
iflist [-p {v4|v6}] [-c|--del delimiter]
iflist -v [-c|--del delimiter]
iflist [-p {v4|v6}] [-c|--del delimiter] interface
iflist -h
```

Description

Displays the interface information that is currently set.

If you do not specify an interface, the command displays all information about the interfaces in use.

If a virtual IP address has been added to the interface by using the `altipadd` command, a message is displayed at the end of the interface information.

Options and arguments

`-c`

Specify this to display the interface information separated with colons (:).

`--del` *delimiter*

Specify this to display the information separated with an alphanumeric character, symbol, or space, whichever is specified.

`-v`

Specify this to display all information about the interfaces in the cluster (including interfaces that are not in use). When this option is specified, the command also displays the information about the ports to which interfaces have not been added.

interface

To view information about a specific interface, specify the name of the port for which the interface is set.

If a tagged VLAN is used, specify it in the following format:

port-name.*VLAN-ID*

Displayed information

The following table lists the information displayed when this command is executed in a cluster configuration.

Table 2-267 Information displayed when the iflist command is executed in a cluster configuration

Item	Description
Interface	Displays information about the interface.

Item	Description
	If a tagged VLAN is used, the information is displayed in the following format: *port-name.VLAN-ID* For an interface that is not used, `Not used` is displayed.
node-number(host-name)	Displays information about the cluster node you are logged in to. This information is displayed in the following format: *node-number(host-name)*
`Fixed IP addr` [1]	Displays the fixed IP address of the node you are logged in to. A hyphen (-) is displayed if the node does not have a fixed IP address.
`Service IP addr` [1]	Displays the virtual IP address of the node you are logged in to. If no virtual IP address is set, a hyphen (-) is displayed.
`Netmask` [1]	Displays the netmask of the node you are logged in to when IPv4 is used.
`Prefix length` [1]	Displays the prefix length of the node you are logged in to when IPv6 is used.
node-number(host-name)	Displays information about the other node in the cluster. This information is displayed in the following format: *node-number(host-name)*
`Fixed IP addr` [1]	Displays the fixed IP address of the other node in the cluster.
`Service IP addr` [1]	Displays the virtual IP address of the other node in the cluster. If no virtual IP address is set, a hyphen (-) is displayed.
`Netmask` [1]	Displays the netmask of the other node in the cluster when IPv4 is used.
`Prefix length` [1]	Displays the prefix length for the other node in the cluster when IPv6 is used.
`MTU` [2]	Displays the MTU value.

Note:

If the -v option is specified, the command does not display information about a physical port on which link aggregation or link alternation is set.

The items for which information is set are displayed in the following order:

○ Interface information items set for IPv4 on the node you are logged in to

○ Interface information items set for IPv6 on the node you are logged in to

○ Interface information items set for IPv4 on the other node

○ Interface information items set for IPv6 on the other node

#1:

Command Reference

If this information cannot be acquired because of a problem, such as the OS not running or a communication error occurring, `Unknown` is displayed.

If the acquired information is invalid because of a problem such as an interface having been set up for one node only or an IP address whose network address is different from the other IP addresses in the same interface having been specified, `Invalid(`*invalid-value*`)` will be displayed.

#2:

If the MTU values in the cluster do not match, `Invalid(`*MTU-value-of-node-that-user-is-logged-in-to*`,`*MTU-value-of-other-node*`)` will be displayed. If an MTU value cannot be acquired because of a problem such as the OS on a node not running or a communication error occurring, `Unknown` will be displayed.

Example: `Invalid(1500,Unknown)`

If an MTU value cannot be acquired in other cases, `None` will be displayed.

Example: `Invalid(1500,None)`

The following table lists the information displayed when this command is executed in a single-node configuration.

Table 2-268 Information displayed when the iflist command is executed in a single-node configuration

Item	Description
Interface	Displays information about the interface.
	If DHCP is used, `(DHCP)` is displayed after the interface.
	If a tagged VLAN is used, the information is displayed in the following format:
	port-name.*VLAN-ID*
	For an interface that is not used, `Not used` is displayed.
IP address #	Displays the IP address.
Netmask #	For IPv4, the netmask appears.
Prefix length #	For IPv6, the prefix length appears.
MTU #	Displays the MTU value.

Note:

The items for which information is set are displayed in the following order:

○ Interface information items set for IPv4

○ Interface information items set for IPv6

#

If this information cannot be acquired because of a problem such as a communication error, `Unknown` is displayed. If the acquired information is invalid, `Invalid(None)` is displayed.

Return values

Table 2-269 Return values of the iflist command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70, 72[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
72[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
  The command ended abnormally due to multiple causes.

Example

To view the interfaces being used:

```
$ sudo iflist
Interface        : eth12.0001
node 0(D79RMPBX)
 [IPv4]
 Fixed IP addr   : 10.208.151.80
 Service IP addr : 10.208.151.81
 Netmask         : 255.255.255.0
 [IPv6]
 Fixed IP addr   : 2001:2c0:418:1::1
 Service IP addr : 2001:2c0:418:1::2
 Prefix length   : 64
node 1(DJ8RMPBX)
 [IPv4]
 Fixed IP addr   : 10.208.151.84
 Service IP addr : 10.208.151.85
 Netmask         : 255.255.255.0
 [IPv6]
 Fixed IP addr   : 2001:2c0:418:1::3
 Service IP addr : 2001:2c0:418:1::4
 Prefix length   : 64
MTU              : 9216

Interface        : mng0
node 0(D79RMPBX)
```

```
 [IPv4]
 Fixed IP addr   : 192.168.3.100
 Service IP addr : 192.168.3.101
 Netmask         : 255.255.0.0
 [IPv6]
 Fixed IP addr   : fdf1:afcb:44f9:1000::3:100
 Service IP addr : fdf1:afcb:44f9:1000::3:101
 Prefix length   : 64
node 1(DJ8RMPBX)
 [IPv4]
 Fixed IP addr   : 192.168.3.110
 Service IP addr : 192.168.3.111
 Netmask         : 255.255.0.0
 [IPv6]
 Fixed IP addr   : fdf1:afcb:44f9:1000::3:110
 Service IP addr : fdf1:afcb:44f9:1000::3:111
 Prefix length   : 64
MTU              : 1500
```

internalludelete (Delete a user disk from an internal hard disk)

Synopsis

```
internalludelete [-f] -n LUN-of-user-disk
internalludelete -h
```

Description

This command can be used in single-node configurations where a user disk has been created from an internal hard disk (excluding HDI Remote Server).

The command deletes a user disk and the associated mapping information from an internal hard disk.

Note that the OS disk and user disk must have been assigned to different RAID groups.

Options and arguments

-f

Specify this option to suppress the output of confirmation messages.

-n *LUN-of-user-disk*

Specify the LUN of the user disk to be deleted, as a hexadecimal value in the range from `00` to `FF`.

Note that the command will terminate normally even if the user disk specified in this option does not exist.

Return values

Table 2-270 Return values of the internalludelete command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review the command format and execute the `internalludelete` command again.
10, 80, 81, 82	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then execute the command again. If the error still occurs, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

internalraidlevelget (Display the RAID level of user disks created from internal hard disks)

Synopsis

```
internalraidlevelget [-h]
```

Description

This command can be used in single-node configurations where a user disk has been created from an internal hard disk (excluding HDI Remote Server).

The command displays the RAID level of a user disk created from an internal hard disk.

Note that the OS disk and user disk must have been assigned to different RAID groups.

Displayed information

The following table lists the information displayed when you execute the command.

Item	Description
RAID level	Displays the RAID level of the user disk created from the internal hard disk.

Return values

Table 2-272 Return values of the internalraidlevelget command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review the command format and execute it again.
10, 80	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The system might be busy or a temporary error might have occurred. Wait a while and then execute the command again. If the error still occurs, contact maintenance personnel.

internalraidlevelset (Set the RAID level of a user disk created from an internal hard disk)

Synopsis

```
internalraidlevelset RAID-level
internalraidlevelset -h
```

Description

This command can be used in single-node configurations where a user disk has been created from an internal hard disk (excluding HDI Remote Server).

The command sets the RAID level of a user disk created from an internal hard disk.

Note that the OS disk and user disk must have been assigned to different RAID groups.

Options and arguments

RAID-level

Specify the RAID level. You can specify `1`, `5`, `6`, or `10`.

Return values

Table 2-273 Return values of the internalraidlevelset command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review the command format and execute the `internalraidlevelset` command again.
10, 70, 80	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The system might be busy or a temporary error might have occurred. Wait a while and then execute the command again. If the error still occurs, contact maintenance personnel.

lulist (List available device files information)

Synopsis

```
lulist [-e] [-d] [-t] [-m] [-v]
lulist -h
```

Description

Lists information about device files that are not in use. The information appears in ascending order of the device file paths. No information appears for failed device files.

Options and arguments

`-d`

> If this option is specified, information about the default controller for the device file is displayed. A hyphen (`-`) is always displayed.

`-e`

> Specify this to append a hash mark (`#`) to the end of the name of the device file residing in an external storage system.

`-m`

> Specify this to view the model and serial number of the storage system where device files exist.

`-t`

> Specify this to view the target.

`-v`

> Specify this to view all device file information.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-274 Information displayed when executing the lulist command

Item	Description
device-file-path	The path of the device file is displayed in the following format: /dev/enas/lu*Hexadecimal-notation*# If you specified the `-e` or `-v` option, a hash mark (`#`) is displayed at the end of the path for a device file that is in an external storage system. # LUNs in the range from `00` to `FF` are displayed as a 2-digit number, and LUNs in the range from `0100` to `03FF` are displayed as a 4-digit number.

drive-type	Displays the drive type for the device file.
	
	`FC/SAS`
	
	This is displayed for an FC drive, an SAS drive, or an internal SAS 7.2K drive.
	
	`SAS7K`
	
	This is displayed for a SAS 7.2K drive.
	
	`SATA`
	
	This is displayed for a SATA drive.
	
	`SSD`
	
	This is displayed for a solid-state drive.
	
	`-`
	
	Displayed in either of the following cases:
	
	- This is displayed for a device file that is in an external storage system.
	
	- When a virtual LU in a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system is being used.
	
	- When a virtual LU that uses HUS100 series Dynamic Tiering is being used.

device-file-capacity	Displays the device file capacity in GB. The value is displayed to three decimal places.
default-controller	A hyphen (`-`) is displayed.

Item	Description
target	The target is displayed. If the target is an internal hard disk, a hyphen (-) is displayed.
storage-system-model	The model of the storage system containing the device file is displayed. If the device file is on an internal hard disk, a hyphen (-) is displayed.
storage-system-serial-number	The serial number of the storage system containing the device file is displayed. If the device file is on an internal hard disk, `INTERNAL` is displayed.

Dynamic Provisioning information	Dynamic Provisioning information is displayed.
	
	`DP`
	
	    This is displayed if the LU is a virtual LU.
	
	`-`
	
	    This is displayed if the LU is not a virtual LU.

DP pool ID	Displays the pool number to which the virtual LU was allocated by Dynamic Provisioning. If the virtual LU is not subject to Dynamic Provisioning, a hyphen (-) is displayed.

Return values

Table 2-275 Return values of the lulist command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`65, 66`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`80`	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

lumapadd (Assign user LUNs)

Synopsis

```
lumapadd -m model -s serial-number
    user-LUN=LDEV-number[ user-LUN=LDEV-number...]
lumapadd -h
```

Description

Assigns an LDEV number in the storage system to a user LUN.

Before executing this command, execute the `lumapctl` command so that LDEV numbers in the storage system are not automatically assigned to user LUNs (maintenance mode). In addition, after executing this command, set the normal operation mode by using the `lumapctl` command and execute the `lumaplist` command on the other node to make sure that the LDEV number is assigned correctly.

Options and arguments

-m *model*

Specify the model of the storage system.
You can specify the following models:

AMS

Specify this for the Hitachi AMS2000 series.

HUS

Specify this for the HUS100 series.

HUS_VM

Specify this for an HUS VM storage system.

USP_V

Specify this for a Universal Storage Platform V storage system.

USP_VM

Specify this for a Universal Storage Platform VM storage system.

VSP

Specify this for a Virtual Storage Platform storage system.

VSP_G1000

Specify this for a VSP G1000 storage system.

VSP_Gx00

Specify this for a VSP Fx00 model or VSP Gx00 model storage system.

-s *serial-number*

Specify the serial number of the storage system.

user-LUN = *LDEV-number* [*user-LUN* = *LDEV-number* ...]

Specify the assignment of a user LUN and an LDEV number. For the user LUN, specify a value in hexadecimal in the range from `00` to `FF` and from `0100` to `03FF`, and for the LDEV number, specify a value in the range from `0` to `65535`.

When specifying multiple assignments, use a space to separate them.

Return values

Table 2-276 Return values of the lumapadd command

Return value	Description
`0`	Normal termination
`1, 5, 6, 7, 8, 9`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10, 12, 13, 15, 70, 71`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To assign LDEV numbers to user LUNs:

- Assign LDEV number `56` whose model is `AMS` and serial number `85011261` to user LUN `13`.
- Assign LDEV number `57` whose model is `AMS` and serial number `85011261` to user LUN `14`.

```
$ sudo lumapadd -m AMS -s 85011261 13=56 14=57
```

lumapctl (Manage the assignment of user LUNs)

Synopsis

```
lumapctl -t m[aintenance] [--on|--off]
lumapctl -h
```

Description

Manages the assignment of user LUNs.

You can also use the command to view the current setting. When LDEV numbers in the storage system are not automatically assigned to user LUNs (maintenance mode), `On` is displayed. When these LDEV numbers are automatically assigned (normal operation mode), `Off` is displayed.

Options and arguments

`-t m[aintenance] [--on|--off]`

Specify whether to automatically assign LDEV numbers to user LUNs. When you want to view the status, execute the command with neither `--on` nor `--off` specified.

`--on`

Specify this to set the maintenance mode. In this mode, LDEV numbers in the storage system are not automatically assigned to user LUNs.

`--off`

Specify this to set the normal operation mode. In this mode, LDEV numbers in the storage system are automatically assigned to user LUNs.

Return values

Table 2-277 Return values of the lumapctl command

Return value	Description
0	Normal termination
1, 4	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To change the setting to prevent LDEV numbers in the storage system from being automatically assigned to user LUNs:

```
$ sudo lumapctl -t m --on
```

Hitachi Data Ingestor CLI Administrator's Guide

lumapdelete (Delete the assignment of user LUNs)

Synopsis

```
lumapdelete [-f] -n user-LUN[,user-LUN,...]
lumapdelete [-f] -m model -s serial-number -l LDEV-number
    [,LDEV-number...]
lumapdelete -h
```

Description

Deletes the assignment settings for LDEV numbers in the storage system and user LUNs.

Before executing this command, execute the `lumapctl` command so that LDEV numbers in the storage system are not automatically assigned to user LUNs (maintenance mode).

Options and arguments

`-f`

Specify this to prevent the confirmation message from appearing.

`-l` *LDEV-number* `[,` *LDEV-number* `...]`

Specify the LDEV number whose assignment you want to delete.
When specifying multiple LDEV numbers, use a comma (`,`) to separate them.

`-m` *model*

Specify the model of the storage system whose assignment you want to delete.
You can specify the following models:

`AMS`

Specify this for the Hitachi AMS2000 series.

`HUS`

Specify this for the HUS100 series.

`HUS_VM`

Specify this for an HUS VM storage system.

`USP_V`

Specify this for a Universal Storage Platform V storage system.

`USP_VM`

Specify this for a Universal Storage Platform VM storage system.

`VSP`

Specify this for a Virtual Storage Platform storage system.

`VSP_G1000`

Specify this for a VSP G1000 storage system.

```
VSP_Gx00
```
Specify this for a VSP Fx00 model or VSP Gx00 model storage system.

`-n` *user-LUN* `[,` *user-LUN* `, ...]`

Specify the user LUN whose assignment you want to delete. Specify a value in hexadecimal in the range from `00` to `FF` and from `0100` to `03FF`.

When specifying multiple user LUNs, use a comma (`,`) to separate them.

`-s` *serial-number*

Specify the serial number of the storage system whose assignment you want to delete.

Return values

Table 2-278 Return values of the lumapdelete command

Return value	Description
0	Normal termination
1, 2, 5, 6, 7, 8, 9	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 14, 70, 71	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To delete the assignments for user LUNs `01`, `02`, `03`, `04`, and `05`:

```
$ sudo lumapdelete -n 01,02,03,04,05
KAQM33009-Q Do you want to delete the specified user LU assignment
information? (y/n)
```

To delete the assignment of LDEV number `56` whose model is `AMS` and serial number is `85011261`:

```
$ sudo lumapdelete -m AMS -s 85011261 -l 56
KAQM33009-Q Do you want to delete the specified user LU assignment
information? (y/n)
```

lumaplist (Display the information of user LUNs)

Synopsis

```
lumaplist [-c] [-v] -n user-LUN[,user-LUN,...]
lumaplist [-c] [-v] -m model
    [-s serial-number [-l LDEV-number[,LDEV-number...]]]
lumaplist [-c] [-v] [-a]
lumaplist [-c] --allnode
lumaplist -h
```

Description

Displays information about the user LUNs.

The following processes are also executed:[#]

- If the user LUNs were added, the LDEV numbers on the storage system are automatically assigned to the user LUNs that were added.

- Assigned user LUNs that are not used and are unrecognized are automatically released.

[#]
> These processes are not executed if the `lumaplist` command was executed when the LDEV numbers on the storage system were set to not be automatically assigned to the user LUNs (maintenance mode).

Options and arguments

`-a`
> Specify this if you want to view the information for all user LUNs, regardless of whether they are assigned. If you omit this option, the information of all assigned user LUNs is displayed.

`--allnode`
> Specify this to display information about the user LUNs on both nodes.

`-c`
> Specify this to display the information separated with colons (:).

`-l LDEV-number [, LDEV-number ...]`
> Specify this to view the information for a specific LDEV number. Specify this option together with the `-m` and `-s` options.
>
> When specifying multiple LDEV numbers, use a comma (,) to separate them.

`-m model`
> Specify this option to view the information of a storage system of a specific model.
>
> You can specify the following models:
>
> `AMS`

Specify this for the Hitachi AMS2000 series.

HUS

Specify this for the HUS100 series.

HUS_VM

Specify this for an HUS VM storage system.

USP_V

Specify this for a Universal Storage Platform V storage system.

USP_VM

Specify this for a Universal Storage Platform VM storage system.

VSP

Specify this for a Virtual Storage Platform storage system.

VSP_G1000

Specify this for a VSP G1000 storage system.

VSP_Gx00

Specify this for a VSP Fx00 model or VSP Gx00 model storage system.

-n *user-LUN* [, *user-LUN* , ...]

Specify this to view information for a specific user LUN. Specify a value in hexadecimal in the range from 00 to FF and from 0100 to 03FF.

When specifying multiple user LUNs, use a comma (,) to separate them.

-s *serial-number*

Specify this to view the information of a storage system of a specific serial number. Specify this option together with the -m option.

-v

Specify this to display additional information about the user LU functions and status.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-279 Information displayed when executing the lumaplist command

Item	Description
LUN	Displays the user LUN in hexadecimal. LUNs in the range from 00 to FF are displayed as a 2-digit number, and LUNs in the range from 0100 to 03FF are displayed as a 4-digit number. A hash mark (#) is displayed at the end of the user LUN if a device file that is in an external storage system.

Item	Description
`Target`	Displays the target. Note that a hyphen (-) is displayed in the following cases: • When no LDEV number is assigned to the user LUN • When the target is an internal hard disk
`Model`	Displays the storage system model.
`serial`	Displays the serial number of the storage system. A hyphen (-) is displayed if the user LUN has not been assigned an LDEV number or the storage system is an internal hard disk.
`LDEV( hex)`	Displays the LDEV number of the device file. The value within the parentheses is displayed in hexadecimal format. A hyphen (-) is displayed if the user LUN has not been assigned an LDEV number or the storage system is an internal hard disk.

`type`	Displays the drive type for the device file.
	`FC/SAS`
	    This is displayed for an FC drive, an SAS drive, or an internal SAS 7.2K drive.
	`SAS7K`
	    This is displayed for a SAS 7.2K drive.
	`SATA`
	    This is displayed for a SATA drive.
	`SSD`
	    This is displayed for a solid-state drive.
	`-`
	    Displayed in either of the following cases:
	    - The drive is a device file on an external storage system.
	    - An LDEV number has not been assigned to the user LUN.
	    - When a virtual LU in a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system is being used.
	    - When a virtual LU that uses HUS100 series Dynamic Tiering is being used.
	    - The drive is an internal hard disk that has developed a fault.

`size`	Displays the size of the device file. A hyphen (-) is displayed when an error has occurred in the device file or when an LDEV number has not been assigned to the user LUN. The value is displayed to three decimal places.

`used function`	Displays the intended use of the device file. When the -v and -c options are specified, a colon (:) is replaced with a space.
	`Free`
	    The device file is not in use.
	`File:` *file-system-name*
	    The device file is used for the indicated file system.

Item	Description
	`ActMig:` *file-system-name*
	The device file is used for the indicated file system, which is being used by the function of Active File Migration.
	`ActMig(Work):` *file-system-name*
	The device file is used for the work space that is being used by the function of Active File Migration. *file-system-name* is the name of the setup source file system of the work space.
	`WORM:` *file-system-name*
	The device file is used for the WORM file system.
	`WORM,ActMig:` *file-system-name*
	The device file is used for the WORM file system of the work space, which is being used by the function of Active File Migration.
	`WORM,ActMig(Work):` *file-system-name*
	The device file is used for the WORM file system of the work space, which is being used by the function of Active File Migration. *file-system-name* is the name of the setup source file system of the work space.
	`VG:`*volume-group-name*
	This is displayed for device files used by a volume group in a single-node configuration.
	`Unknown`
	This is displayed when any of the following conditions are satisfied for the user LU:
	- The intended use of the device file has been changed during command execution.
	- Information about the device file could not be obtained because an error occurred.
	- Information could not be obtained for a volume group in a single node configuration.
	If `Unknown` is displayed, wait a while, and then try again. If `Unknown` is still displayed, check system messages and fix the problem. If a system message was not output, contact maintenance personnel.
`RG`	Displays the RAID group to which the device file belongs.
	If the RAID group associated with the internal hard disk is deleted, this item might display a different number than it did before due to the reallocation of RAID group numbers among existing RAID groups.
	If the user LU is a virtual LU, a device file that is in an external storage system, or an LU for which no LDEV number is assigned to the user LUN, a hyphen (–) is displayed.
`DP`	Virtual LU information is displayed.
	`DP`
	This is displayed if the user LU is a virtual LU.
	–

Item	Description
	This is displayed if the user LU is not a virtual LU or an LU for which no LDEV number is assigned to the user LUN.
`Used page`	The page size of the virtual LU is displayed. If the user LU is not a virtual LU or an LU for which no LDEV number is assigned to the user LUN, a hyphen (–) is displayed. Everything after the third decimal place is truncated. Executing a command such as the `fpstatus` and `fscreate` command might temporarily allocate space to a virtual LU. Therefore, the size might be displayed even if a virtual LU is not in use.
`Pool`	The number of the Pool to which the virtual LU belongs is displayed. If the user LU is not a virtual LU or an LU for which no LDEV number is assigned to the user LUN, a hyphen (–) is displayed.
`Free pool`	The amount of free space in the Pool is displayed. Note that a hyphen (–) is displayed in the following cases: • When the user LU is not a virtual LU • When no LDEV number is assigned to the user LUN • When a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system is being used Everything after the third decimal place is truncated.
`Total pool`	The total capacity of the Pool is displayed. Note that a hyphen (–) is displayed in the following cases: • When the user LU is not a virtual LU • When no LDEV number is assigned to the user LUN • When a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system is being used Everything after the third decimal place is truncated.
`Mismatch`	Whether both nodes use the same mapping is displayed for each user LUN. – The node mappings are the same. * The node mappings are different.

Return values

Table 2-280 Return values of the lumaplist command

Return value	Description
`0`	Normal termination

Return value	Description
1, 5, 6, 7	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
66, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

nasboot (Start the OS on the other node in the cluster)

Synopsis

```
nasboot [-h]
```

Description

Sends a power-on request from the node to which you are logged in to the hardware on the other node in the cluster in order to start the OS on the other node.

Notes:

- Because the command terminates normally at the moment the power-on request is sent, use the `peerstatus` command or the GUI to confirm that the OS on the other node in the cluster has started normally.

- If you are using the encryption functionality, and system settings are saved in the HCP system, before starting the OS, check that the HCP system is running normally and that the HDI and HCP systems can communicate normally.

Return values

Table 2-281 Return values of the nasboot command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.

Return value	Description
`10, 13, 66, 70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

nasipneigh (Check that IP addresses and MAC addresses correspond)

Synopsis

```
nasipneigh [-4] [-6]
```

Description

Checks that IP addresses and MAC addresses correspond.

Notes:

- Multiple processes cannot execute the `nasipneigh` command concurrently. If the `nasipneigh` command is executed concurrently by multiple processes, an exclusive control error occurs and `failed to lock` is displayed. If you want to execute the `nasipneigh` command, execute the command after making sure that the process executing the `nasipneigh` command has ended. If no process is executing the `nasipneigh` command but an exclusive control error occurs, execute the `eraselog` command and then execute the `nasipneigh` command.

- Information may not appear immediately due to internal buffering.

- Check the information for the interface name followed by `-br`.

Options and arguments

`-4`

    Specify this option to check that IPv4 IP addresses and MAC addresses correspond. If you specify this option together with the `-6` option, the last specified option takes effect.

`-6`

    Specify this option to check that IPv6 IP addresses and MAC addresses correspond. If you omit this option, `-4` is set. If you specify this option together with the `-4` option, the last specified option takes effect.

Return values

Table 2-282 Return values of the nasipneigh command

Return value	Description
0	Normal termination
1[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
1[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

nasnetstat (Display the network setting information)

Synopsis

```
nasnetstat [-r|-g|-i|-s|-M] [-v] [-n] [--numeric-hosts]
    [--numeric-ports] [--numeric-users]
    [--protocol=family[,family...]]
    [-4] [-6] [-c] [-e [-e]] [-o] [-p] [-l] [-a] [-F] [-C]
```

Description

Displays the network information set in the GUI. The displayed information is the same as that displayed by the `netstat` command.

By executing this command, you can check whether the network settings are set correctly in the OS on a node.

The displayed information is added to the beginning of the log file and stored. When the log file exceeds 1 MB, information equivalent to the amount by which the maximum size was exceeded is deleted from the end of the log file. You can obtain the log file by downloading all the log data from the **List of RAS Information** page (for `Batch-download`) of the Check for Errors dialog box. For details on downloading all log data, see the *Troubleshooting Guide*.

For a system that uses tagged VLANs, the tagged VLAN interface names are displayed in the following format by using the `nasnetstat` command:

port-name.*VLAN ID*

For example, if the name of the port for which a tagged VLAN is set is `eth12` and the VLAN ID is `10`, the tagged VLAN interface name that will be displayed is `eth12.0010`.

Notes:

- Multiple processes cannot execute the `nasnetstat` command concurrently. If the `nasnetstat` command is executed concurrently by multiple processes, an exclusive control error occurs and `failed to lock` is displayed. If you want to execute the `nasnetstat` command, execute the command after making sure that the process executing the `nasnetstat` command has ended. If no process is executing the `nasnetstat` command but an exclusive control error occurs, execute the `eraselog` command and then execute the `nasnetstat` command.

- Information may not appear immediately due to internal buffering.

- If command processing does not complete within 30 seconds, a timeout occurs and processing is canceled. If a timeout occurs, re-execute the command with the `-n` option specified.

- When you execute the command with the `-r`, `-g`, or `-i` option specified, check the information for the interface name followed by `-br`.

Options and arguments

`-4`

Specify this to use IPv4 IP addresses.

If you specify this option together with the `-6` option, both options take effect. Note, however, that if you specify the `-r` option with these options, the routing table information will be displayed for the specified number of times in the order in which the `-4` and `-6` options were specified.

If you specify neither the `-4` nor the `-6` option, IPv4 and IPv6 protocols take effect. Note, however, that if you specify the `-r` option without specifying these options, IPv4 takes effect.

`-6`

Specify this to use IPv6 IP addresses.

If you specify this option together with the `-4` option, both options take effect. Note, however, that if you specify the `-r` option with these options, the routing table information will be displayed for the specified number of times in the order in which the `-4` and `-6` options were specified.

If you specify neither the `-4` nor the `-6` option, IPv4 and IPv6 protocols take effect. Note, however, that if you specify the `-r` option without specifying these options, IPv4 takes effect.

`-a`

Specify this option to view all the sockets in use regardless of their connection status.

`-c`

Specify this option to refresh the displayed information at one-second intervals.

`-C`

Specify this option to view routing information in the routing cache.

`-e [-e]`

Specify this option to view detailed information. Specify the option twice to obtain even more detailed information.

`-F`

Specify this option to view routing information in the FIB.

`-g`

Specify this option to view information about IPv4 and IPv6 multicast group membership.

`-i`

Specify this option to view information about all network interfaces.

`-l`

Specify this option to view only the sockets that are waiting for connections.

`-M`

Specify this option to view information about a masqueraded network.

`-n`

Specify this option to view numerical addresses without resolving host names, port names, or user names.

`--numeric-hosts`

Specify this option to view hosts by IP address, not host name.

`--numeric-ports`

Specify this option to view ports by port number, not port name.

`--numeric-users`

Specify this option to view users by user ID, not user name.

`-o`

Specify this option to view information about the networking timer.

`-p`

Specify this option to view the name and PID of the program that each socket belongs to.

`--protocol=` *family* `[,` *family* `...]`

Specify this option to view the connection status of a specified address family. In *family*, specify one of the following keywords: `inet`, `unix`, `ipx`, `ax25`, `netrom`, or `ddp`. `inet` includes the protocol sockets (`raw`, `udp`, and `tcp`).

`-r`

Specify this option to view the routing table.

`-s`

Specify this option to view statistical information for each protocol.

`-v`

Specify this option to view information in detail mode.

Return values

Table 2-283 Return values of the nasnetstat command

Return value	Description
0	Normal termination
1[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
1[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

#
The command ended abnormally due to multiple causes.

nasping (Display the connection to a specified host)

Synopsis

```
nasping [-4] [-6] [-L] [-R] [-d] [-n] [-q] [-r] [-v]
    [-c count] [-p pattern] [-s packetsize] [-t ttl]
    [-I interface-address] host
```

Description

Displays the connection status of the specified host. The displayed information is the same as that displayed by the `ping` command.

The displayed information is added to the beginning of the log file and stored. When the log file exceeds 1 MB, information equivalent to the amount by which the maximum size was exceeded is deleted from the end of the log file. The packet dump file is also output as a log file at the same time. You can obtain the log file by downloading all the log data from the **List of RAS Information** page (for `Batch-download`) of the Check for Errors dialog box. For details on downloading all log data, see the *Troubleshooting Guide*.

Notes:

- Multiple processes cannot execute the `nasping` command concurrently. If the `nasping` command is executed concurrently by multiple processes, an exclusive control error occurs and `failed to lock` is displayed. If you want to execute the `nasping` command, execute the command after making sure that the process executing the `nasping` command has ended. If an exclusive control error occurs while no other processes are

executing the `nasping` command, execute the `eraselog` command, and then execute the `nasping` command.

- Information may not appear immediately due to internal buffering.
- When you execute the command with the `-I` option specified, check the information for the interface name followed by `-br`.

Options and arguments

`-4`

Specify this option to use IPv4 IP addresses. If you specify this option together with the `-6` option, the last specified option takes effect.

`-6`

Specify this option to use IPv6 IP addresses. If you omit this option, `-4` is assumed. If you specify this option together with the `-4` option, the last specified option takes effect.

`-c` *count*

Specify the number of packets to be sent. The maximum number of send packets is 10. If you omit this option, this option is set to 10.

`-d`

Specify this option to set the debugging option to the socket to be used.

`-I` *interface-address*

Specify the IP address of the interface that sends packets.

`-L`

Specify this option to control a loopback for multicast packets.

`-n`

Specify this option to output the IP address of the host without converting to a host name.

`-p` *pattern*

Specify a pattern for filling the ping packet to be sent. You can specify a hexadecimal value consisting of a maximum of 16 bytes. You can use this option for diagnosing data-dependent network problems. For example, if you specify `-p ff`, the packet will be filled entirely with 1s.

`-q`

Specify this option to view only the statistical information about the starting and ending time for sending.

`-r`

Specify this option to send packets directly to the host by ignoring the routing settings.

`-R`

Specify this option to view the path from the node to the host.

`-s` *packetsize*

Specify the byte size of the data to be sent. When you omit this option, the default is 56.

-t *ttl*

Specify this option to set the keep-alive period for packets.

-v

Specify this option to view detailed information.

host

Specify the target host name or IP address.

Return values

Table 2-284 Return values of the nasping command

Return value	Description
0	Normal termination
1[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
1[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

nasreboot (Restart the OS on a node)

Synopsis

```
nasreboot [-f] [-q] [--force]
nasreboot -h
```

Description

Restarts the OS on the node to which you are logged in.

If you want to restart the OS, the status of the node to which you are logged in must be INACTIVE or UNKNOWN.

Notes:

- In a cluster configuration, if the nasshutdown, nasreboot, ndstop, or rgmove commands are executed for a node in the same cluster while the this command is processing, the processing might not finish. Confirm from the other node that the status of the node to which the this

command is executed is `INACTIVE`, and then execute the `nasshutdown`, `nasreboot`, `ndstop`, or `rgmove` commands.

- If you are using the encryption functionality, and system settings are saved in the HCP system, before restarting the OS, check that the HCP system is running normally and that the HDI and HCP systems can communicate normally.

Options and arguments

`-f`

Specify this to prevent the confirmation message from appearing.

`--force`

For a cluster configuration, specify this to forcibly restart the OS on a node. Note, however, that you cannot use this option when the status of the node to which you are logged in is `UP` and the status of the other node is not `UP`.

For a single-node configuration, this option is not applicable and will be ignored.

`-q`

Specify this to suppress the output of messages to the standard output and standard error output.

Return values

Table 2-285 Return values of the nasreboot command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 11, 12, 13	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

nasshutdown (Stop the OS on a node)

Synopsis

```
nasshutdown [-f] [-q] [--force]
nasshutdown -h
```

Description

Stops the OS on the node to which you are logged in.

To stop the OS on a node in a cluster configuration, the status of the node to which you are logged in must be `INACTIVE` or `UNKNOWN`.

Note: In a cluster configuration, if the `nasshutdown`, `nasreboot`, `ndstop`, or `rgmove` commands are executed for a node in the same cluster while the this command is processing, the processing might not finish. Confirm from the other node that the status of the node to which the this command is executed is `INACTIVE`, and then execute the `nasshutdown`, `nasreboot`, `ndstop`, or `rgmove` commands.

Options and arguments

`-f`

Specify this to prevent the confirmation message from appearing.

`--force`

For a cluster configuration, specify this to forcibly stop the OS on a node. Note, however, that you cannot use this option when the status of the node to which you are logged in is `UP` and the status of the other node in the cluster is not `UP`.

For a single-node configuration, this option is not applicable and will be ignored.

`-q`

Specify this to suppress the output of messages to the standard output and standard error output.

Return values

Table 2-286 Return values of the nasshutdown command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 11, 12, 13	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If

Return value	Description
	this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

nastraceroute (Display the path that leads to the specified host)

Synopsis

```
nastraceroute [-4] [-6] [-d] [-F] [-I] [-r] [-n]
    [-g gateway[,gateway]...] [-i iface] [-f first-ttl]
    [-m max-ttl] [-p port] [-q nqueries] [-s src-addr] [-t tos]
    [-w waittime] host [packet-length]
```

Description

Displays the path that leads to the specified host. The displayed information is the same as that displayed by the `traceroute` command.

The displayed information is added to the beginning of the log file and stored. When the log file exceeds 1 MB, information equivalent to the amount by which the maximum size was exceeded is deleted from the end of the log file. The packet dump file is also output as a log file at the same time. You can obtain the log file by downloading all the log data from the **List of RAS Information** page (for `Batch-download`) of the Check for Errors dialog box. For details on downloading all log data, see the *Troubleshooting Guide*.

Notes:

- Multiple processes cannot execute the `nastraceroute` command concurrently. If the `nastraceroute` command is executed concurrently by multiple processes, an exclusive control error occurs and `failed to lock` is displayed. If you want to execute the `nastraceroute` command, execute the command after making sure that the process executing the `nastraceroute` command has ended. If no process is executing the `nastraceroute` command but an exclusive control error occurs, execute the `eraselog` command and then execute the `nastraceroute` command.

- Information may not appear immediately due to internal buffering.

- If command processing does not complete within 30 seconds, a timeout occurs and processing is canceled. If a timeout occurs, re-execute the command with the `-n` option specified.

Options and arguments

`-4`

Specify this to use IPv4 IP addresses. If you specify this option together with the `-6` option, the last specified option takes effect.

`-6`

Specify this to use IPv6 IP addresses. If you omit this option, `-4` is set. If you specify this option together with the `-4` option, the last specified option takes effect.

`-d`

Specify this option to execute the command in debug mode.

`-f` *first-ttl*

Specify the initial value for TTL to be used. From the hop (TTL) specified in this option, the network information is displayed.

`-F`

Specify this option to prohibit packet fragmentation.

`-g` *gateway* [, *gateway*]...

Specify the IP addresses of the gateways (routers) to be passed through. You can specify a maximum of eight IP addresses.

`-i` *iface*

Specify this if you want to use the specified interface (network card name) to execute this command.

`-I`

Specify this if you want to use ICMP Echo Request. If you omit this option, UDP packets are used.

`-m` *max-ttl*

Specify the maximum value of TTL to be used. The network information up to the hop count (TTL) specified in this option is displayed.

`-n`

Specify this option to view IP addresses only, without performing name resolution.

`-p` *port*

Specify this if you want to set the port number for a UDP packet to be used. Specify this only when a UDP packet is used.

`-q` *nqueries*

Specify the retry count for one gateway. If you omit this option, this option is set to 3.

`-r`

Specify this if you want to ignore the routing table and send packets directly to the specified host.

`-s` *src-addr*

Specify the source address. Execution will be from this specified IP address.

−t *tos*

Specify the packet TOS.

−w *waittime*

Specify the timeout value (in units of seconds). If you omit this option, this option is set to 5.

host

Specify the target host name or IP address.

packet-length

Specify the size of packets to be used for path searches (units: bytes).

Return values

Table 2-287 Return values of the nastraceroute command

Return value	Description
0	Normal termination
1[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
1[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

ndmpconfig (Display or modify NDMP server configuration information)

Synopsis
```
ndmpconfig [-l server_timeout] [-nomsg]
ndmpconfig -m server_timeout timeout-value [-nomsg]
ndmpconfig -h
```

Description

The ndmpconfig command displays or modifies the timeout information that is set for the NDMP server.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

The timeout value for the NDMP server is initially set to 480 minutes. You can change this value as needed to accommodate the actual backup operation.

When you change the configuration information of the NDMP server on a node, set the same timeout value for both of the nodes in the cluster. If different timeout values are set for the nodes while processing for a backup or restore operation is being performed, data transmission cannot be completed and the processing might terminate with an error.

Also, do not change the configuration information while performing a backup or restore operation. The NDMP server will automatically restart when you change the configuration information while the server is running. After executing the command, check the operating status of the NDMP server.

If an option is omitted, the command is executed as if `-l server_timeout` were specified.

Options and arguments

`-l server_timeout`

Specify this option to view the timeout information that is set for the NDMP server.

`-m server_timeout` *timeout-value*

Specify this option to modify the NDMP server timeout information. Specify a value from 5 to 1,440 for the timeout value (in minutes).

If you use a tape device that is connected to a node via a SAN, specify `15` minutes or more for the timeout value.

Displayed information

The information that is displayed when this command is executed is shown in the table below.

Table 2-288 Information displayed when executing the ndmpconfig command (when the -l option is specified)

Item	Description
server_timeout	Displays the timeout value that is set for the NDMP server (in minutes).

Return values

Table 2-289 Return values of the ndmpconfig command

Return value	Description
0	Normal termination

Return value	Description
1, 2, 3, 4, 5, 16, 21	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
6, 8, 12, 14, 20, 22, 23, 24, 25, 31, 32	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
11, 15	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
13	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To modify the timeout information that has been set for the NDMP server:

```
$ sudo ndmpconfig -m server_timeout 1440
Aug 14 12:00:18 KAQB11500-I ndmpconfig command execution has started.
Aug 14 12:00:24 KAQB11705-W Items are applied only to the logged-in node.
If necessary, log in to each node on the cluster and check each setup.
Aug 14 12:00:24 KAQB11501-I ndmpconfig command has finished.
```

ndmpcontrol (Control the NDMP server)

Synopsis

```
ndmpcontrol [-l] [-nomsg]
ndmpcontrol [-s|-r|-q|-f] [-nomsg]
ndmpcontrol -h
```

Description

The ndmpcontrol command is used to display the operating status of the NDMP server on the node that you are logged in to, and to control the NDMP server.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

The options that you can specify in this command depend on the operating status of the NDMP server and on the processing status of the backup or restore operation when the command is specified. Therefore, we recommend that you specify the -l option to check the available command options before you attempt to start or stop the NDMP server.

If an option is omitted, the command is executed as if -l were specified.

Options and arguments

-f

Specify this option to perform a forced stop of the NDMP server.

If you perform a forced stop of the NDMP server while it is connected to a backup server or media server, a backup or restore operation will terminate with an error.

Check the status of the connection to an external server before you perform a forced stop of the NDMP server.

-l

Specify this option to check the operating status of the NDMP server or the available command options.

You can use this option regardless of the operating status of the NDMP server or the processing status of the backup or restore operation.

-q

Specify this option to stop the NDMP server.

-r

Specify this option to restart the NDMP server.

-s

Specify this option to start the NDMP server.

Displayed information

The information that is displayed when this command is executed is shown in the table below.

Table 2-290 Information displayed when executing the ndmpcontrol command (when the -l option is specified)

Item	Description

NDMPsvrstatus	Displays the NDMP server operating status:
	running
	    The NDMP server is running.
	stopped
	    The NDMP server has stopped.

allowrequest #	Displays currently available options:
	L
	    The -l option can be specified.
	S
	    The -s option can be specified.
	R
	    The -r option can be specified.

Item	Description
	Q The `-q` option can be specified. F The `-f` option can be specified. H The `-h` option can be specified.
`pid`	Displays the process ID of the NDMP server. The process ID is shown as a whole decimal number from 1 to 99999. If the NDMP server has stopped, no ID is displayed.

`connectstatus`	Displays the connection status between the NDMP server and external servers (backup servers, media servers, or NDMP servers for another node):
	
	`connected`
	
	    The NDMP server and external servers are connected.
	
	`disconnected`
	
	    The NDMP server and external servers are disconnected.

\#

When multiple options can be specified in the command, the options are delimited with commas.

Return values

Table 2-291 Return values of the ndmpcontrol command

Return value	Description
0	Normal termination
1, 2, 21	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
6, 8, 12, 13[#], 14, 20, 22, 23, 24, 25	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
11, 15	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
13[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Examples

To start the NDMP server:

```
$ sudo ndmpcontrol -s
Aug 14 12:17:04 KAQB11500-I ndmpcontrol command execution has started.
Aug 14 12:17:06 KAQB11501-I ndmpcontrol command has finished.
```

To restart the NDMP server:

```
$ sudo ndmpcontrol -r
Aug 14 12:17:21 KAQB11500-I ndmpcontrol command execution has started.
Aug 14 12:17:25 KAQB11501-I ndmpcontrol command has finished.
```

To stop the NDMP server:

```
$ sudo ndmpcontrol -q
Aug 14 12:16:41 KAQB11500-I ndmpcontrol command execution has started.
Aug 14 12:16:43 KAQB11501-I ndmpcontrol command has finished.
```

Notes:

- The NDMP server might take a long time to start or stop even if the command completes successfully. After executing the `ndmpcontrol` command, run the `ndmpcontrol -l` command to check the NDMP server's operating status.
- If `stopped` is displayed under `NDMPsvrstatus` or if `connected` is displayed under `connectstatus`, the connection to the NDMP server will be automatically severed. After executing the command, use the `ndmpcontrol -l` command to check the connection status.
- If you restart the OS while the NDMP server is running, the NDMP server will restart automatically.

ndmpfsconfig (Change the conditions for interrupting an offline backup)

Synopsis

```
ndmpfsconfig -a -p accurate-check file-system-name [-nomsg]
ndmpfsconfig -d -p accurate-check file-system-name [-nomsg]
ndmpfsconfig [-l] [file-system-name] [-nomsg]
ndmpfsconfig -h
```

Description

The `ndmpfsconfig` command changes the setting of whether to interrupt offline backup processing when a file is modified or deleted during an offline backup.

If all options are omitted, the command is executed assuming that the `-l` option is specified.

You can change or view the conditions for interrupting an offline backup for file systems mounted on the local node. You cannot change the conditions for interrupting an offline backup for file systems that are not mounted on the local node or file systems that are on the other node.

Options and arguments

`-a`

Specify this option to interrupt offline backup processing when a file is modified or deleted during the offline backup. Specify this option together with the `-p accurate-check` option.

`-d`

Specify this option to continue offline backup processing when a file is modified or deleted during the offline backup. Specify this option together with the `-p accurate-check` option.

`-l`

Specify this option to display the name of the file system for which the settings for the conditions for interrupting an offline backup are to be changed and the current conditions set for the file system.

If you specify only the `-l` option, information about all file systems on the node on which the command is being executed. If you specify the file system name for the `-l` option, only information about the specified file system is displayed.

If you specify only the `-l` option when there is no file system, the command terminates normally without displaying anything.

`-p accurate-check`

Specify this option to change the conditions for interrupting an offline backup. Specify the `-a` or `-d` option together with this option to specify whether to interrupt offline backup processing when a file is modified or deleted during the backup.

If this option is omitted, the offline backup is set to continue.

file-system-name

Specify the name of the file system for which the conditions for interrupting an offline backup are to be changed. Use no more than 16 characters. You can use alphanumeric characters and underscores (_).

If you execute the command by specifying the `-l` option but not specifying a file system name, information about all the registered file systems is displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-292 Information displayed when executing the ndmpfsconfig command (when the -l option is specified)

Item	Description
`File system`	Displays the name of the file system for which the setting for the conditions for interrupting an offline backup are to be changed.

`Improved backup data accuracy check`	Displays the settings for the conditions for interrupting an offline backup.
	
	`On`
	
	The settings are specified so that offline backup processing is to be interrupted.
	
	`Off`
	
	The settings are specified so that offline backup processing is to continue.

Return values

Table 2-293 Return values of the ndmpfsconfig command

Return value	Description
`0`	Normal termination
`1, 2, 4`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10, 11, 70, 71`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65, 67, 68, 97, 99`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Examples

To specify the settings so that backup processing is interrupted when a file is updated during an offline backup of the file system (`FS1`) (when enhancing the accuracy check of the offline backup):

```
$ sudo ndmpfsconfig -a -p accurate-check FS1
Mar  8 09:19:30 KAQB11500-I ndmpfsconfig command execution has started.
Mar  8 09:19:31 KAQB11501-I ndmpfsconfig command has finished.
```

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

To specify the settings so that backup processing continues even if a file is updated during an offline backup of the file system (`FS1`) (when not enhancing the accuracy check of the offline backup):

```
$ sudo ndmpfsconfig -d -p accurate-check FS1
Mar  8 09:22:58 KAQB11500-I ndmpfsconfig command execution has started.
Mar  8 09:22:59 KAQB11501-I ndmpfsconfig command has finished.
```

To display a list of the conditions for interrupting an offline backup that are set for all the registered file systems:

```
$ sudo ndmpfsconfig -l
Mar  8 09:36:11 KAQB11500-I ndmpfsconfig command execution has started.
The number of file systems(1)
 File system                        : FS1
 Improved backup data accuracy check : On
The number of file systems(2)
 File system                        : FS2
 Improved backup data accuracy check : Off
Mar  8 09:36:12 KAQB11501-I ndmpfsconfig command has finished.
```

Notes:

- You cannot interrupt the command processing by pressing **Ctrl** + **C** because the `ndmpfsconfig` command is executed after disabling `SIGHUP`, `SIGINT`, `SIGQUIT`, and `SIGTERM`.
- If you perform the operations below for a file system, the settings for the conditions are reset to the default. You will need to set the conditions for interrupting an offline backup again.

  - Use the `fsimport` command to connect the file system that was disconnected from a node by using the `fsexport` command to a node.
  - Use the `horcimport` or `horcvmimport` command to connect the copy-destination file system that was disconnected from a node by using the `horcexport` command to a node.

ndmppasswd (Change the NDMP server password)

Synopsis

```
ndmppasswd
    [user-ID old-password new-password confirm-password] [-nomsg]
ndmppasswd -h
```

Description

The `ndmppasswd` command changes the password used by a backup server to connect to an NDMP server.

After you install the system for the first time, you must change the password of the NDMP server.

When you change the password of the NDMP server on a node, specify the same password for both of the nodes in the cluster. If you set different passwords on the nodes, an authentication error might occur during a backup or restore operation.

If you specify the command without specifying any argument, you can change the password interactively. The entered password will not be shown, eliminating any risk of discovery by third parties. For security reasons, we recommend the interactive method.

After changing the password, use the backup management software to set up the access permissions for the NDMP server again.

The following table lists the information to be specified when changing an NDMP server password interactively.

Table 2-294 Information to be specified when changing the NDMP server password interactively

Item	Description
userid	Enter the user name (root) for connecting to the NDMP server.
oldpasswd	Enter the current password.
newpasswd	Enter the new password.
	Enter from 1 to 32 characters. You can use alphanumeric characters and underscores (_).
	You cannot enter a string that is the same as the string you entered in either userid or oldpasswd.
	In newpasswd, enter a string that a third party will not easily guess.
confirmpasswd	Re-enter the new password.

Options and arguments

-nomsg
    Specify this option to suppress the output of messages to the standard output and standard error output. When the ndmppasswd command is executed interactively, this option cannot be specified.

user-ID
    Specify the user name (root) for connecting to the NDMP server.

old-password
    Specify the current password.

new-password
    Specify the new password. You must enter the password again in *confirm-password* to confirm.
    Enter from 1 to 32 characters. You can use alphanumeric characters and underscores (_). You cannot enter a string that is the same as the string

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

you entered in *user-ID* or *old-password*. Enter a new password that a third party will not easily guess.

Return values

Table 2-295 Return values of the ndmppasswd command

Return value	Description
0	Normal termination
1, 2, 3, 4	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
6, 8, 12, 13, 14, 20, 26	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
11, 15, 21, 23, 24, 25	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.

Example

To change the NDMP server password interactively:

```
$ sudo ndmppasswd
Aug 14 12:18:39 KAQB11502-Q Enter the value of the displayed parameter
name, and then press 'Enter'.
userid=root
oldpasswd=
newpasswd=
confirmpasswd=
Aug 14 12:18:47 KAQB11500-I ndmppasswd command execution has started.
Aug 14 12:18:47 KAQB11705-W Items are applied only to the logged-in node.
If necessary, log in to each node on the cluster and check each setup.
Aug 14 12:18:47 KAQB11501-I ndmppasswd command has finished.
```

ndstart (Start a node)

Synopsis

```
ndstart [--] node-name
ndstart -h
```

Description

Starts a specified node.

You can execute this command when the node is in INACTIVE state.

If you start the node with the resource group status in the `Online Ready/No error` state, the resource group also starts automatically. After the `ndstart` command processing has been completed, it might take a while until resource group-related operations can be performed (the state of the resource group has changed to `Online/No error`).

Options and arguments

node-name
    Specify the name of the node you want to start.

Return values

Table 2-296 Return values of the ndstart command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 21, 28, 29, 66, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80, 81	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

ndstatus (Display node status)

Synopsis

```
ndstatus [-c] [--] [node-name]
ndstatus -h
```

Description

Displays the status of a node.

Options and arguments

`-c`

Specify this to display node status information separated with colons (`:`).
When the `-c` option is specified, any colon (`:`) contained in the node
names is replaced with a hash mark (`#`).

node-name

To view the status of a particular node in the cluster, specify the node
name.

Displayed information

The following table lists the information displayed when you execute the
command.

Table 2-297 Information displayed when executing the ndstatus command

Item	Description
`--Node Status--`	The node information is displayed.
	If you do not specify a node name, the command displays the status of the node to which you are logged in and the status of the other node in the cluster, in that order.
node-number , *host-name*	The node information is displayed in the following format:
	`node-number(host-name)`
`Node name`	Name of the node is displayed.
`Node status`	Status of the node is displayed.[#1]
	`UP`
	The node is running normally.
	`INACTIVE`
	The node is stopped.
	`DOWN`
	The node ended abnormally and has shut down.
	`UNKNOWN` [#2#3]
	The status cannot be determined.

Note:

If you execute the `ndstatus` command immediately after executing the
`clstart` command or the `ndstart` command, the command might remain
in the processing status for some time.

#1:

If an error occurs in the system, the status of nodes may not be
displayed. In this case, collect error information and contact maintenance
personnel. For details on collecting error information, see the
Troubleshooting Guide.

#2:

If you execute the `ndstatus` command while you are logged in to a stopped node, the other node in the cluster is shown as having UNKNOWN status, regardless of its actual status. To check the status of the other node and the resource group, log in to the active node (the other node), and then execute the `clstatus` command.

#3:

UNKNOWN is also displayed when a cluster starts up. Note that, when a cluster starts up, UNKNOWN is displayed until both OSs on the nodes making up the cluster complete startup (for up to 10 minutes).

Return values

Table 2-298 Return values of the ndstatus command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 21, 66, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

ndstop (Stop a node)

Synopsis

```
ndstop [-f] [-y] [--] node-name
ndstop -h
```

Description

Stops a specified node.

You can execute this command when the status of the node and resource group is as follows:

- The node to be stopped is in UP state.

- The status of the resource group on the node to be stopped is `Online/No error`, `Offline/No error`, or `Online Maintenance/No error`.

Note: If the `nasshutdown` or `nasreboot` commands are executed for a node in the same cluster while the this command is processing, the processing might not finish. Confirm from the other node that the status of the node to be stopped is `INACTIVE`, and then execute the `nasshutdown` or `nasreboot` commands.

Options and arguments

`-f`

Specify this option if you want to forcibly stop the specified node. If an error occurs during node startup or stop operation and prevents processing from continuing, you can forcibly stop the node by executing this command with the `-f` option specified.

node-name

Specify the name of the node you want to stop or forcibly stop.

Return values

Table 2-299 Return values of the ndstop command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10, 21, 27, 66, 70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

nfsbackup (Back up NFS share information)

Synopsis

```
nfsbackup file-system-name information-definition-file-name
nfsbackup -h
```

Description

Backs up the NFS share information for the specified file system. The backed-up NFS share information can be restored by using the `nfsrestore` command.

The resource group to which the specified file system belongs must be properly running on the node where the command is executed. NFS share information can be backed up even if the resource group is in the failover status. However, the information definition file will be created on the failover-destination node, where the command is executed.

Options and arguments

file-system-name

> Specify the name of the file system whose NFS share information you want to back up.

information-definition-file-name

> Specify the name of the information definition file to which the NFS share information is backed up.
>
> Specify the name of the information definition file using no more than 255 characters. You can use alphanumeric characters, hyphens (-), and underscores (_). Note that hyphens cannot be used as the first character of the file name. You can also use periods (.), except at the beginning or end of the character string.
>
> The information definition file will be output immediately under the SSH account home directory (`/home/nasroot`). The file cannot have the same name as an existing file in the `/home/nasroot` directory.
>
> Notes:
>
>> - Do not edit the contents of the information definition file. If the information definition file is edited, restoration of the backup of the CIFS share information might not be possible.
>>
>> - You can use the `scp` command or some other secure transfer tools to send and save the information definition file onto a remote host.

Return values

Table 2-300 Return values of the nfsbackup command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 66[#], 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If

Return value	Description
	this error occurs repeatedly, contact maintenance personnel.
65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
: The command ended abnormally due to multiple causes.

nfscacheflush (Flush NFS caches)

Synopsis

```
nfscacheflush [cache-name[,cache-name...]]
nfscacheflush -h
```

Description

Flushes the NFSv4 client caches, which are used for converting user names to user IDs and group names to group IDs, or flushes Kerberos authentication caches. Sometimes, the cached client information differs from the current client information because of changes to the NFSv4 domain or user information. If this occurs while the cache is still active and if you want to access the NFS share, you must execute this command. In addition, if Kerberos authentication fails, you must execute this command. This is necessary because, if the failure result remains in the enabled cache, the Kerberos authentication will continue to fail.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Note:
: While this command is being executed, NFS clients might not be able to access the NFS share. Notify the administrator of the NFS client host that the NFS share will be inaccessible until the process is completed. In addition, after completion of the processing, notify the users who were accessing the NFS share from NFS clients to execute the `kdestroy` and `kinit` commands so that they will be able to resume access.

Options and arguments

cache-name [, *cache-name* ...]
: Specify the type of the cache to be flushed by using a cache name that has been assigned to the cache type. If you omit this option, the

command performs processing in the same way as when all cache names are specified.

You can specify the following cache names:

nfs4name

Specify this to flush the cache that is being used to convert NFSv4 client user/group names to user/group IDs.

rpcsec

Specify this to flush a cache used for Kerberos authentication.

Return values

Table 2-301 Return values of the nfscacheflush command

Return value	Description
0	Normal termination
1	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
2	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
3	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To flush a cache used for Kerberos authentication:

```
$ sudo nfscacheflush rpcsec
```

nfscreate (Create an NFS share)

Synopsis

```
nfscreate -d shared-directory
    -H host[:[{ro|rw_sync|rw_sync_opt}]:[{everyone|root_only|none}]
    [:[security-flavor[.security-flavor...]]]]][,host...]
    [-p {ro|rw_sync|rw_sync_opt}] [-a {everyone|root_only|none}]
    [-u UID] [-g GID] [-t {perform|do_not_perform}]
    [-s {perform|do_not_perform}] [-l {perform|do_not_perform}]
    [-m maximum-transfer-length]
    [-S security-flavor[{.|,}security-flavor...]]
nfscreate -h
```

security-flavor:
```
{sys|krb5|krb5i|krb5p|default}
```

Description

Creates an NFS share using the specified attributes.

To make a directory public with different attributes on multiple hosts, execute this command on each target host. However, for attributes set by the following options, the attribute you specify the last time you execute this command will apply to all target hosts where the directory is made public. (When an option is omitted, the existing setting is inherited. When an option is specified, the specified setting becomes effective.)

- `-u` option
- `-g` option
- `-t` option
- `-s` option
- `-l` option
- `-m` option

Note that you can use this command to set access permissions, anonymous user mapping, and security flavors by host, as well as for individual NFS shares. If you specify both a setting applicable to the NFS share (the `-p` option, `-a` option, or `-S` option) and a setting applicable to the host (the `-H` option), the setting applicable to the host takes effect.

Notes:

- This command cannot be used for home-directory-roaming file systems.
- For a file system linked to the HCP system at the share level, an NFS share cannot be created at the mount point.

  This command cannot be used for home-directory-roaming file systems.

- If `ro` or `none` is specified for the owner, none of users, including the owner, can write to new files.

- In an Advanced-ACL-type file system, the following access permissions must be specified for all users and groups depending on the owner group specification:

  - If you specify `ro` for the owner group, specify `ro` or `none` for all users and groups. If you specify `rw`, users belonging to the owner group (including the owner) will no longer be able to write to new files.

  - If you specify `none` for the owner group, specify `none` for all users and groups. If you specify `rw`, users belonging to the owner group (including the owner) will no longer be able to read or write to new files, and if you specify `ro`, they will no longer be able to read new files.

Options and arguments

`-a {everyone|root_only|none}`

Specify whether to map the user as an anonymous user when an NFS client accesses the NFS share. If you omit this option, `root_only` applies.

`everyone`

Specify this when you map all users as anonymous users.

`root_only`

Specify this when you map only the root user as an anonymous user.

`none`

Specify this when you do not want to map users as anonymous users.

`-d` *shared-directory*

Specify the absolute path of the directory in which you want to create an NFS share, using no more than 63 characters beginning with `/mnt/`.

For a read-write-content-sharing file system, you must specify the mount point as a shared directory.

You can specify alphanumeric characters, hyphens (-), periods (.), forward slashes (/), and underscores (_). You cannot specify multibyte characters. In addition, you cannot specify a path that includes a symbolic link. Note that `.conflict`, `.conflict_longpath`, `.snaps` , `.history`, and `.lost+found` cannot be specified for a directory name. Also, `.arc`, `.system_gi`, `.system_reorganize`, or `lost+found` cannot be specified for the name of a directory immediately under the file system.

`-g` *GID*

Specify the group ID to be used in an anonymous user access. Specify a value within the range from 0 to 65535. If you omit this option, it defaults to 65534.

`-H` *host* `[:[{ro|rw_sync|rw_sync_opt}]:[{everyone|root_only|none}][:[` *security-flavor* `[.` *security-flavor* `...]]]][,` *host* `...]`

Specify the NFS share public destination.

You can also specify the access permissions, users to be mapped as anonymous users, and security flavors by host. If you omit this option, the settings for individual NFS shares are applied.

When you specify multiple destinations, use a comma (,) to separate them.

host

Specify a string of no more than 255 characters

When specifying a host alias, you also need to specify an official host name of 255 characters or less.

Specify a host name beginning with an alphabetic character and consisting of alphanumeric characters, hyphens (-), and underscores (_).

In addition to the host name and IP address, you can specify the destinations in the following formats:

Netgroup

Specify an NIS netgroup.

IP network

For IPv4, specify the IP address and netmask. Specify the netmask as a decimal value separated by periods (.), or as the bit count indicating the mask length.

For IPv6, specify the IP address and prefix length.

Wildcard

When you specify all hosts, you can use an asterisk (*) as the wildcard.

DNS domain

Specify the name of the DNS domains to which the NFS client belongs, starting with a period (.).

If the NFS client machine contains multiple network interfaces that are used to communicate with the HDI system, specify the host by using one of the following methods:

- Specify an asterisk (*) as the wildcard

- Specify all the IP addresses of network interfaces used by the NFS clients

- Specify all the host names of network interfaces used by the NFS clients

- Specify all the IP networks including the IP addresses of network interfaces used by the NFS clients

- Specify all the netgroups including the host names that support network interfaces used by the NFS clients

- Specify all the DNS domains including the host that support network interfaces used by the NFS clients

If you specify both an IP address and a host name for the same host, the host name setting will take effect.

The length of each host name or network name (input length + 5 bytes) must be less than 1,258 bytes. If an NFS share has already been created for the shared directory specified in the `-d` option, the hosts on which that NFS share is made public must also be included in the calculation.

To check the length of the host names or network names on which the existing NFS share was made public, execute the `nfslist` command with the `-d` option specified. To calculate the total size, add 5 bytes to each of the lengths output to `Public destination host/network`.

For the shared directory, if you specify multiple hosts in the form of ranges in different formats, each range will be checked to see whether it includes an NFS client. The ranges will be checked in the following order of priority: host name, IP network or IP address, net group, DNS domain, and wildcards. Specified options (such as access permissions, users to be mapped as anonymous users, and security flavors) are applied to the NFS client in the range of the highest priority.

Example:

```
*:ro:root_only
172.16.0.0/16:rw_sync:none
```

In this example, the IP network (`172.16.0.0/16`) is prioritized over the wildcard (`*`). Therefore, the option for the IP network (`rw_sync`) is applied to the NFS client in the IP network `172.16.0.0/16`, whereas the option `ro` is applied to NFS clients outside of the IP network `172.16.0.0/16`.

If you specify multiple hosts in the form of ranges in the same format but with different options (such as access permissions, users to be mapped as anonymous users, and security flavors), the options are given priority in the order in which they are specified.

Example:

```
172.16.0.0/16:ro:root_only
172.16.0.0/17:rw_sync:none
```

In this example, hosts are specified in the same format, so the option specified first (`ro`) is applied. Note that, while the `nfscreate` command is still running, checking might not be performed in the order described above.

`ro|rw_sync|rw_sync_opt`

Specify access permissions for the public destination. If this specification is omitted, `rw_sync` is set by default.

`ro`

Specify this to permit the NFS share to be read-only.

`rw_sync`

Specify this to permit read and write operations on the NFS share, and to set synchronous writing without optimization.

`rw_sync_opt`

Specify this to permit read and write operations on the NFS share, and to set synchronous writing with optimization.

`everyone|root_only|none`

Specify the users to be mapped as anonymous users. If this specification is omitted, `root_only` is set by default.

`everyone`

Specify this to map all users as anonymous users.

`root_only`

Specify this to map only the root user as an anonymous user.

`none`

Specify this when you do not want to map users as anonymous users.

security-flavor

Specify security flavors. To specify multiple security flavors, use a period (`.`) to separate them. If this specification is omitted, `default` is set by default.

You can specify the following as security flavors:

sys

Specify this to apply UNIX (AUTH_SYS) authentication.

krb5

Specify this to apply Kerberos authentication.

krb5i

Specify this to apply the data integrity function as well as Kerberos authentication.

krb5p

Specify this to apply the data integrity and privacy functions as well as Kerberos authentication.

default

Specify this to apply the security flavor settings specified in the **NFS Service Management** page of the GUI. The settings at the moment that the command was executed are applied. `default` cannot be specified together with other *security-flavor* values.

-l {perform|do_not_perform}

Specify whether to check permissions (authorize) for a lock request. If you omit this option, it defaults to `do_not_perform`.

If you use a machine that does not send authentication information for a lock request (the machine OS is HP-UX or a machine on which the `rpcinfo -p` command displays `100020` in `program`) or that might send authentication information of a user other than the user who requests a lock (the machine OS is AIX), as an NFS client, specify `do_not_perform`. If you specify `perform`, the lock might not be obtained (an ENOLCK error might occur) unless anonymous users of the HDI system have the read permission (`r`) for all directories from the parent directory of the file to be locked to the NFS mounted directory.

perform

Specify this to check permissions for each lock request. If anonymous mapping is not set for the user who locked the file, permissions for that user are checked. If anonymous mapping is set for the user, permissions for the anonymous user in the HDI system are checked. The owner of the locked files can lock them without permissions. Also, if the user has the read permission, they can write-lock the files.

do_not_perform

Specify this if you do not want to check permissions for each lock request. Permissions for an anonymous user in the HDI system are checked.

-m *maximum-transfer-length*

Specify the maximum transfer length for the NFS share (unit: KB). Specify a value within the range from 4 to 1,024.

This option is valid only when the NFSv2 or NFSv3 protocol is used.

-p {ro|rw_sync|rw_sync_opt}

Specify access permissions for the NFS share. If you omit this option, it defaults to `rw_sync`.

When you permit writing, specify whether to optimize synchronous writing as well. Optimization of synchronous writing is a function that slightly delays a disk drive update by a write request, when the write request has been received from an NFS client while another relevant write request is being performed (or is about to be performed). Optimization can improve performance because the disk drive is updated by multiple write requests in one operation. If multiple data-write requests that are relatively unrelated are made, optimizing synchronous writing might actually lower performance. In this situation, specify synchronous writing without optimization (`rw_sync`).

`ro`

Specify this to permit the NFS share to be read-only.

`rw_sync`

Specify this to permit read and write operations on the NFS share, and to set synchronous writing without optimization.

`rw_sync_opt`

Specify this to permit read and write operations on the NFS share, and to set synchronous writing with optimization.

`-s {perform|do_not_perform}`

Specify whether to check if the user has the execute permission (`x`) for all directories (subtrees) from the shared directory to the directory in which the file or directory to be accessed exists, as well as checking the access permission for the file or directory to be accessed. If you omit this option, it defaults to `do_not_perform`.

If you use a machine that does not send authentication information for a lock request (the machine OS is HP-UX or a machine on which the `rpcinfo -p` command displays `100020` in `program`) or that might send authentication information of a user other than the user who requests a lock (the machine OS is AIX), as an NFS client, specify `do_not_perform`. If you specify `perform`, the lock might not be obtained (an ENOLCK error might occur) unless anonymous users of the HDI system have the execute permission (`x`) for all directories from the parent directory of the file to be locked to the NFS mounted directory.

`perform`

Specify this if you want to perform a subtree check.

`do_not_perform`

Specify this if you do not want to perform a subtree check.

`-S` *security-flavor* `[{.|,}` *security-flavor* `...]`

Specify this to set a security flavor for individual NFS shares. To specify multiple security flavors, use a comma (`,`) or period (`.`) to separate them.

You can specify the following as security flavors:

`sys`

Specify this to apply UNIX (AUTH_SYS) authentication.

krb5

Specify this to apply Kerberos authentication.

krb5i

Specify this to apply the data integrity function as well as Kerberos authentication.

krb5p

Specify this to apply the data integrity and privacy functions as well as Kerberos authentication.

default

Specify this to apply the security flavor settings specified in the NFS Service Management page of the GUI. The settings at the moment that the command was executed are applied. default cannot be specified together with other *security-flavor* values.

-t {perform|do_not_perform}

Specify whether to accept only the requests from an Internet port whose port number is lower than 1024. To make the file system open to machines that use an Internet port assigned 1024 or higher, specify do_not_perform. If you omit this option, it defaults to do_not_perform.

perform

Specify this to limit transmission ports.

do_not_perform

Specify this if you do not want to limit transmission ports.

In AIX, an Internet port whose port number is 1024 or higher is used by default. If you use AIX for the NFS client host and choose to use the default Internet port setting, specify do_not_perform. In HP-UX, an Internet port whose port number is 1024 or higher is used for file locking. If you use HP-UX for the NFS client host, specify do_not_perform.

-u *UID*

Specify the user ID to be used in an anonymous user access. Specify a value within the range from 0 to 65535. If you omit this option, it defaults to 65534.

Return values

Table 2-302 Return values of the nfscreate command

Return value	Description
0	Normal termination
1, 10#	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.

Return value	Description
10[#], 66[#], 70, 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.
99[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

#

    The command ended abnormally due to multiple causes.

Examples

To create an NFS share according to the following conditions:

- The shared directory is `/mnt/FS1/dir_case1`.
- The public destination hosts are specified for `host1`, `host2`, `host3`, and `host4`.
- UNIX (AUTH_SYS) authentication is the security flavor for all of the individual public destination hosts.

```
$ sudo nfscreate -d /mnt/FS1/dir_case1 -H host1,host2,host3,host4 -S sys
```

To create an NFS share according to the following conditions:

- The shared directory is `/mnt/FS1/dir_case1`.
- Specify the public destination hosts to all hosts.
- Kerberos authentication is the security flavor.
- The data integrity and privacy functions are not being used.

```
$ sudo nfscreate -d /mnt/FS1/dir_case1 -H "*" -S krb5
```

To create an NFS share according to the following conditions:

- The shared directory is `/mnt/FS1/dir_case1`.
- Specify the public destination hosts to all hosts.
- Execute the following command from a remote host[#]:

```
$ ssh -2 nasroot@fshost01 sudo nfscreate -d /mnt/FS1/dir_case1 -H "\*"
```

#

When you specify a wildcard, use an escape character corresponding to your remote host environment.

nfsdelete (Delete NFS shares)

Synopsis

```
nfsdelete -d shared-directory {-a|-H host[,host...]}
nfsdelete -h
```

Description

Deletes an NFS share.

Options and arguments

-a

Specify this option to delete all NFS shares in the shared directory specified in the -d option.

-d *shared-directory*

Specify the absolute path beginning with /mnt/ of the directory from which NFS shares are to be deleted.

-H *host* [, *host* ...]

Specify the public destination hosts whose access to the NFS shares is to be set to unavailable.

When you specify multiple public destinations, use a comma (,) to separate them.

Return values

Table 2-303 Return values of the nfsdelete command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 66#, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If

Return value	Description
	this error occurs repeatedly, contact maintenance personnel.
65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

nfsedit (Edit NFS share information)

Synopsis

```
nfsedit -d shared-directory
    -H host[:[{ro|rw_sync|rw_sync_opt}]]:[{everyone|root_only|none}]
    [:[security-flavor[.security-flavor...]]]][,host...]
    [-p {ro|rw_sync|rw_sync_opt}] [-a {everyone|root_only|none}]
    [-u UID] [-g GID] [-t {perform|do_not_perform}]
    [-s {perform|do_not_perform}] [-l {perform|do_not_perform}]
    [-m maximum-transfer-length]
    [-S security-flavor[{.|,}security-flavor...]]
nfsedit -h
```

security-flavor:

```
{sys|krb5|krb5i|krb5p|default}
```

Description

Edits NFS share information according to the specified attributes.

However, for attributes set by the following options, the attribute you specify the last time you execute this command will apply to all target hosts where the directory is made public.

- -u option
- -g option
- -t option
- -s option
- -l option
- -m option

If you omit any of the following options, the current setting information applies.

Note that you can use this command to set access permissions, anonymous user mapping, and security flavors by host, as well as for individual NFS

shares. If you specify both a setting applicable to the NFS share (the `-p` option, `-a` option, or `-S` option) and a setting applicable to the host (the `-H` option), the setting applicable to the host takes effect.

Options and arguments

`-a {everyone|root_only|none}`

Specify whether to map the user as an anonymous user when an NFS client accesses the NFS share.

`everyone`

Specify this when you map all users as anonymous users.

`root_only`

Specify this when you map only the root user as an anonymous user.

`none`

Specify this when you do not want to map users as anonymous users.

`-d` *shared-directory*

Specify the absolute path beginning with `/mnt/` of the directory of the NFS share whose attributes are to be changed.

`-g` *GID*

Specify the group ID to be used in an anonymous user access. Specify a value within the range from 0 to 65535.

`-H` *host* `[:[{ro|rw_sync|rw_sync_opt}]:[{everyone|root_only|none}][:[` *security-flavor* `[.` *security-flavor* `...]]]][,` *host* `...]`

Specify the public destination hosts set for the target NFS share.

You can also specify the access permissions, users to be mapped as anonymous users, and security flavors by host. If you omit this option, the settings for individual NFS shares are applied.

When you specify multiple destinations, use a comma (,) to separate them.

host

Specify the public destination for which NFS share information is to be edited.

`ro|rw_sync|rw_sync_opt`

Specify this option to change the access permissions that are set for each public destination. If you omit this option, the current setting information applies.

`ro`

Specify this to permit the NFS share to be read-only.

`rw_sync`

Specify this to permit read and write operations on the NFS share, and to set synchronous writing without optimization.

`rw_sync_opt`

Specify this to permit read and write operations on the NFS share, and to set synchronous writing with optimization.

`everyone|root_only|none`

Specify this option to change the users who, for each public destination, are to be mapped as anonymous users. If you omit this option, the current setting information applies.

`everyone`

Specify this to map all users as anonymous users.

`root_only`

Specify this to map only the root user as an anonymous user.

`none`

Specify this when you do not want to map users as anonymous users.

security-flavor

Specify security flavors. To specify multiple security flavors, use a period (`.`) to separate them.

You can specify the following as security flavors:

`sys`

Specify this to apply UNIX (AUTH_SYS) authentication.

`krb5`

Specify this to apply Kerberos authentication.

`krb5i`

Specify this to apply the data integrity function as well as Kerberos authentication.

`krb5p`

Specify this to apply the data integrity and privacy functions as well as Kerberos authentication.

`default`

Specify this to apply the security flavor settings specified in the **NFS Service Management** page of the GUI. The settings at the moment that the command was executed are applied. `default` cannot be specified together with other *security-flavor* values.

`-l {perform|do_not_perform}`

Specify whether to check permissions (authorize) for a lock request.

If you use a machine that does not send authentication information for a lock request (the machine OS is HP-UX or a machine on which the `rpcinfo -p` command displays `100020` in `program`) or that might send authentication information of a user other than the user who requests a lock (the machine OS is AIX), as an NFS client, specify `do_not_perform`. If you specify `perform`, the lock might not be obtained (an ENOLCK error might occur) unless anonymous users of the HDI system have the read permission (`r`) for all directories from the parent directory of the file to be locked to the NFS mounted directory.

`perform`

Specify this to check permissions for each lock request. If anonymous mapping is not set for the user who locked the file, permissions for that user are checked. If anonymous mapping is set for the user, permissions for the anonymous user in the HDI system are checked. The owner of the locked files can lock them without permissions. Also, if the user has the read permission, they can write-lock the files.

do_not_perform

Specify this if you do not want to check permissions for each lock request. Permissions for an anonymous user in the HDI system are checked.

-m *maximum-transfer-length*

Specify the maximum transfer length for the NFS share (unit: KB). Specify a value within the range from 4 to 1,024. Before changing the maximum transfer length, you need to ask the administrator of the NFS client host to unmount the file system from the NFS client side.

This option is valid only when the NFSv2 or NFSv3 protocol is used.

-p {ro|rw_sync|rw_sync_opt}

Specify access permissions for the NFS share.

When you permit writing, specify whether to optimize synchronous writing as well. Optimization of synchronous writing is a function that slightly delays a disk drive update by a write request, when the write request has been received from an NFS client while another relevant write request is currently being performed (or is about to be performed). Optimization can improve performance because the disk drive is updated by multiple write requests in one operation. If multiple data-write requests that are relatively unrelated are made, optimizing synchronous writing might actually lower performance. In this situation, specify synchronous writing without optimization (rw_sync).

ro

Specify this to permit the NFS share to be read-only.

rw_sync

Specify this to permit read and write operations on the NFS share, and to set synchronous writing without optimization.

rw_sync_opt

Specify this to permit read and write operations on the NFS share, and to set synchronous writing with optimization.

-s {perform|do_not_perform}

Specify whether to check if the user has the execute permission (x) for all directories (subtrees) from the shared directory to the directory in which the file or directory to be accessed exists, as well as checking the access permission for the file or directory to be accessed.

If you use a machine that does not send authentication information for a lock request (the machine OS is HP-UX or a machine on which the rpcinfo -p command displays 100020 in program) or that might send

authentication information of a user other than the user who requests a lock (the machine OS is AIX), as an NFS client, specify `do_not_perform`. If you specify `perform`, the lock might not be obtained (an ENOLCK error might occur) unless anonymous users of the HDI system have the execute permission (`x`) for all directories from the parent directory of the file to be locked to the NFS mounted directory.

`perform`

    Specify this if you want to perform a subtree check.

`do_not_perform`

    Specify this if you do not want to perform a subtree check.

`-S` *security-flavor* `[{.|,}` *security-flavor* `...]`

Specify this to set a security flavor for individual NFS shares. To specify multiple security flavors, use a comma (`,`) or period (`.`) to separate them.

You can specify the following as security flavors:

`sys`

    Specify this to apply UNIX (AUTH_SYS) authentication.

`krb5`

    Specify this to apply Kerberos authentication.

`krb5i`

    Specify this to apply the data integrity function as well as Kerberos authentication.

`krb5p`

    Specify this to apply the data integrity and privacy functions as well as Kerberos authentication.

`default`

    Specify this to apply the security flavor settings specified in the **NFS Service Management** page of the GUI. The settings at the moment that the command was executed are applied. `default` cannot be specified together with other *security-flavor* values.

`-t {perform|do_not_perform}`

Specify whether to accept only the requests from an Internet port lower than 1024. To make the file system open to machines that use an Internet port assigned 1024 or higher, specify `do_not_perform`.

`perform`

    Specify this to limit transmission ports.

`do_not_perform`

    Specify this if you do not want to limit transmission ports.

In AIX, an Internet port whose port number is 1024 or higher is used by default. If you use AIX for the NFS client host and choose to use the default Internet port setting, specify `do_not_perform`. In HP-UX, an

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

Internet port whose port number is 1024 or higher is used for file locking. If you use HP-UX for the NFS client host, specify `do_not_perform`.

`-u` *UID*

Specify the user ID to be used in an anonymous user access. Specify a value within the range from 0 to 65535.

Return values

Table 2-304 Return values of the nfsedit command

Return value	Description
0	Normal termination
1, 10#	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10#, 66#, 70, 99#	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66#	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99#	The error cannot be handled by the system administrator. Contact maintenance personnel.
99#	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Examples

To change information about the NFS shares in the directory `mnt/FS1/dir_case1` according to the following conditions:

- An NFS share with the write permission set has been created and made public on `host1`.
- Change the settings to be read-only.

```
$ sudo nfsedit -d /mnt/FS1/dir_case1 -H host1 -p ro
```

To change information about the NFS shares in the directory `mnt/FS1/dir_case1` according to the following conditions:

- host1, host2, host3, and host4 have been specified as the public destination hosts.
- Change the security flavor for all of the individual public destination hosts to UNIX (AUTH_SYS) authentication.

```
$ sudo nfsedit -d /mnt/FS1/dir_case1 -H host1,host2,host3,host4 -S sys
```

nfskeytabadd (Add a keytab file for Kerberos authentication)

Synopsis

```
nfskeytabadd -i keytab-file-name [-q]
nfskeytabadd -h
```

Description

Adds a keytab file for Kerberos authentication to the keytab files being managed by nodes.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

The following conditions must be met before you can use this command:

- The keytab file for Kerberos authentication has been created on the NFS client computer or KDC server.
- The keytab file has been transferred to the SSH account home directory (/home/nasroot) by using the scp command or other secure transfer tool.

Options and arguments

-i *keytab-file-name*

Specify the name including the absolute path beginning with /mnt/ of the keytab file for Kerberos authentication. Note that you cannot specify a keytab file name that includes double quotation marks ("), colons (:), and spaces. If the contents of the keytab file are properly added, the specified keytab file is deleted.

-q

Specify this to prevent the confirmation message from appearing.

Return values

Table 2-305 Return values of the nfskeytabadd command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
70[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
70[#], 71	The error cannot be handled by the system administrator. Contact maintenance personnel.
72	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Example

To add a keytab file for Kerberos authentication (keytab file name: `/home/nasroot/nfs.keytab`):

```
$ sudo nfskeytabadd -i /home/nasroot/nfs.keytab
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
----
--------------------------------------------------------------------------
   3 nfs/node0.ad2003.skyu1.local@AD2003.SKYU1.LOCAL
   3 nfs/node1.ad2003.skyu1.local@AD2003.SKYU1.LOCAL
```

nfskeytabdel (Delete principal information from the keytab file for Kerberos authentication)

Synopsis

```
nfskeytabdel [-y] -s slot-number
nfskeytabdel -h
```

Description

Deletes principal information from the keytab file for Kerberos authentication.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Options and arguments

-s *slot-number*

Specify the slot number of principal information to be deleted.

Return values

Table 2-306 Return values of the nfskeytabdel command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
70, 71	The error cannot be handled by the system administrator. Contact maintenance personnel.
72	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Example

To delete principal information from the keytab file (slot number: 2):

```
$ sudo nfskeytabdel -s 2
KAQG20329-Q Do you want to delete an entry for slot 2 ? (y/n)
```

nfskeytablist (List the contents of the keytab file for Kerberos authentication)

Synopsis

```
nfskeytablist [-h]
```

Description

Lists the contents of the keytab file for Kerberos authentication in ascending order of slot number.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-307 Information displayed when executing the nfskeytablist command

Item	Description
slot	Slot number
KVNO	Key version number
Principal	Principal information

Return values

Table 2-308 Return values of the nfskeytablist command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
70	The error cannot be handled by the system administrator. Contact maintenance personnel.

nfslist (List NFS share information)

Synopsis

```
nfslist [-d shared-directory] [{-c|--del delimiter}]
    [-O extended-options]
nfslist -h
```

extended-options:
```
    value[,value...]
```

Description

Lists information about the NFS shares on the node to which you are logged in. Information is listed for each NFS share in ascending order of the shared directory paths. When multiple NFS shares have been created in one directory, the information appears in ascending order of the public destination hosts.

> *Note:*
> If the host name or network group name specified for the public destination of the NFS share cannot be resolved, it might take a while for the command processing to finish.

Options and arguments

`-c`

Specify this to display NFS share information separated with colons (`:`).

`-d` *shared-directory*

Specify the absolute path beginning with `/mnt/` of the target directory if you want to view the settings for a specific NFS share. If you omit this option, the command displays information about all NFS shares on the node.

`--del` *delimiter*

Specify this to display the information separated with an alphanumeric character, symbol, or space, whichever is specified.

`-O` *extended-options*

Specify which optional information to be displayed. If this option is omitted, optional information is not displayed.
You can specify the following values:

`m`

Specify this to view information about the `Maximum rwsize(KB)`.

`n`

Specify this to view information about the `Host/network name resolution`.

`s`

Specify this to view information about security flavors.

`all`

Specify this to view all optional information.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-309 Information displayed when executing the nfslist command

Item	Description
`Shared directory`	Displays the absolute path for the directory of the created NFS shares.
`Public destination host/network`	Displays the name of a host or network on which the NFS share is made public.

`Permission mode / Synchronous writing`	Displays information about the access permission for the NFS share and the synchronous write mode.
	
	`ro`
	
	    The NFS share is read-only.
	
	`rw_sync`

Item	Description
	Read and write operations are permitted on the NFS share, and synchronous writing without optimization is set. `rw_sync_opt` Read and write operations are permitted on the NFS share, and synchronous writing with optimization is set.

`Anonymous mapping`	Displays users who are mapped as anonymous users.
	
	`everyone`
	
	All users are mapped as anonymous users.
	
	`root_only`
	
	Only the root user is mapped as an anonymous user.
	
	`none`
	
	Users are not mapped as anonymous users.

`Anonymous UID`	Displays the user ID to be used when accessing the NFS share as an anonymous user.
`Anonymous GID`	Displays the group ID to be used when accessing the NFS share as an anonymous user.

`Transmission port restriction`	Displays whether the only accepted requests are those from an Internet port whose port number is lower than 1024.
	
	`perform`
	
	Transmission ports are restricted.
	
	`do_not_perform`
	
	No restriction on transmission ports.

`Subtree check`	Displays whether the system (in addition to checking the access permission for the file or directory to be accessed) also checks that the user has the execute permission (`x`) for all directories (subtrees) from the shared directory to the directory in which the file or directory to be accessed exists.
	
	`perform`
	
	A subtree check is performed.
	
	`do_not_perform`
	
	A subtree check is not performed.

`Access check with lock request`	Displays whether there is a check of permissions (authorize) for a lock request.
	
	`perform`
	
	Permissions are checked for a lock request.
	
	`do_not_perform`
	
	Permissions are not checked for a lock request.

`Maximum rwsize(KB)`	Displays the maximum transfer length for the NFS share. When no maximum transfer length is set, `--` is displayed. This information appears only when `m` or `all` is specified in the `-o` option.

Item	Description

Host/network name resolution	Displays whether the host name specified as the NFS share public destination can be resolved. This information appears only when `n` or `all` is specified in the `-O` option.
	
	 OK
	
	    Displayed when the name can be resolved.
	
	 NG(*host-name*)
	
	    Displayed when the name cannot be resolved. If multiple host names cannot be resolved, they are displayed and separated by a comma (,). For an NFS share in which you have specified a network group as the public destination, only `NG` will be displayed when the list of host names cannot be acquired.
	
	 --
	
	    Displayed when an IP address is specified, an asterisk is specified as a wildcard, or a DNS domain is specified.

Security flavor	Displays the security flavor set for the public destination of the NFS share. If multiple destinations have been set, each security flavor is separated by a comma (,). This information appears only when `s` or `all` is specified in the `-O` option.

Return values

Table 2-310 Return values of the nfslist command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

nfslocksclear (Delete file lock information for an NFS client host)

Synopsis

```
nfslocksclear [-F] host-name [host-name...]
```

Description

Deletes the file lock information remaining in the OS on a node after an error occurs on the NFS client host or network.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Delete the file lock information for an NFS client host in the following cases:

* When an NFS client machine that has obtained the file lock terminates abnormally while holding the file lock, and that machine cannot restart for some reason.

* When the NFS client host is in a cluster configuration and the jobs running on the NFS client machine that terminated abnormally are taken over by another NFS client machine

> *Notes:*
>
> - When a file lock is obtained normally by an NFS client, if the NFS file lock information is deleted on the HDI system, exclusive control over the file will be lost, leaving the file vulnerable to damage.
>
> - After deleting the file lock information that has remained in the OS on a node because of a network error occurring while an NFS client host was normally operating, restart the NFS client host before reconnecting the client to the network.

Options and arguments

-F

Specify this to prevent the confirmation message from appearing.

host-name [*host-name* ...]

Specify the host names of the NFS client hosts of which to delete the file lock information. Separate multiple host system names with spaces. Specify a host name beginning with an alphabetic character and consisting of halfwidth alphanumeric characters, hyphens (-), and underscores (_).

Return values

Table 2-311 Return values of the nfslocksclear command

Return value	Description
0	Normal termination

Return value	Description
1#	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
1#	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

nfslockslist (List file lock information for an NFS client host)

Synopsis

```
nfslockslist [-a]
    [-f target-file-name|-i [major-number:minor-number:]inode-number]
    [-p process-ID] [-t time-passed] [host-name [host-name...]]
nfslockslist -h
```

Description

Lists the file lock information for an NFS client host on the OS on a node. Note that information about share reservation locking cannot be displayed in an NFSv4 environment.

If you omit all of the options and arguments, the file lock information for the obtained file locks is only displayed.

This command shows no file lock information for an NFS client host while one of the following conditions persists. Re-execute the command after resolving the problem.

- During failover.
- During failback.
- Immediately after failback.
- Immediately after the OS is started on a node.
- While NFS service is stopped.

If you suspend processing of the command for a long time by using a signal such as the SIGSTOP signal, performance of the HDI system might be affected.

Options and arguments

-a

Specify this to view all the file lock information for the obtained file locks and the file locks waiting to be obtained.

-f *target-file-name*

Specify the file name including the absolute path beginning with `/mnt/` if you only want to view the file lock information for a particular file.

-i [*major-number* : *minor-number* :] *inode-number*

Specify the major number, minor number, and inode number for a particular file if you only want to view the file lock information for that file.

Execution of this command with this option specified terminates normally, even if the specified file does not exist.

-p *process-ID*

Specify the process ID if you only want to view the file lock information about a particular process.

-t *time-passed*

Specify this if you only want to view the file lock information regarding file locks that have passed a certain period of time after they are obtained or are waiting to be obtained (units: seconds). Specify an integer of `0` or more for the argument.

host-name [*host-name* ...]

Specify the IP address or the host name if you only want to view the file lock information about a particular NFS client host. Separate multiple host names with spaces. Specify a host name beginning with an alphabetic character and consisting of halfwidth alphanumeric characters, hyphens (-), and underscores (_).

Displayed information

Displayed in the following format:

```
number#1: major-number:minor-number:inode-number path#2 POSIX  ADVISORY WRITE-
or-READ starting-offset-of-file-lock ending-offset-of-file-lock process-ID#3
host-name-or-IP-address#4 date-and-time-at-which-the-file-lock-was-obtained-or-
date-and-time-from-which-the-file-lock-waiting-to-be-obtained-starts#5
```

#1:

If the file lock information you are viewing is about a file lock that is waiting to be obtained, `->` is displayed following the number.

#2:

- When the NFS client host has obtained a file lock, if that file is deleted from that client host, the file name is displayed beginning with a period (.).

- When the NFS client host has obtained a file lock, if that file is deleted from another client, `(deleted)` is displayed at the end of the path.

(deleted) is displayed at the end of the path even after the resource group is failed over or failed back, or the OS restarts on a node.

- ○ Before and after the NFS client host obtains a file lock, if that file is moved to another directory, the path is not displayed correctly and (moved) is displayed at the end of the path.

#3:

- ○ If the NFS client host uses Linux kernel 2.6.9 or later, a unique ID that identifies file lock information is displayed instead of the process ID.

  For details on how to identify the process ID from a unique ID, see .

- ○ If the NFS client host uses the NFSv4 protocol, the nfsd process ID is displayed.

#4:

If a machine that is not an NFS client host obtains a file lock, a hyphen (-) is displayed.

#5:

The displayed date and time are updated in the following cases:

- ○ Failover occurs.
- ○ Failback occurs.
- ○ The OS on a node is restarted.
- ○ NFS service is restarted.

Return values

Table 2-312 Return values of the nfslockslist command

Return value	Description
0	Normal termination
1, 3	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
2	The error cannot be handled by the system administrator. Contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.

Example

To view a large amount of file lock information or execute the grep command on the remote host to narrow down the file lock information:

```
$ ssh -2 nasroot@fshost01 'sudo nfslockslist' > lockslist.txt
$ grep file lockslist.txt
20: 254:5:137 /mnt/nfs/file2413 POSIX  ADVISORY  WRITE 0 13 22400
ClientHost1 2009/12/18 10:14:20
21: 254:5:136 /mnt/nfs/file124 POSIX  ADVISORY  WRITE 0 13 15466
ClientHost5 2009/12/18 10:12:48
```

nfsoptlist (Display the NFS environment settings)

Synopsis

```
nfsoptlist [keyword]
nfsoptlist -h
```

Description

Displays the NFS environment information set in the OS on a node.

Options and arguments

keyword

Specify a keyword. If you omit this option, the command displays information about all keywords.

You can specify the following:

disable_mountd_reply_dumplist

Specify this option if you want to see whether the list of NFS shares mounted by the requesting client is returned to the client.

disable_mountd_reply_exportlist

Specify this option if you want to see whether the list of NFS shares is returned to the client.

disable_rquotad_startup

Specify this option if you want to check whether the Quota operation from the NFS client is suppressed.

nfsd_show_quota_value

This option applies if the capacity is set as limited based on hard namespace quotas when the HDI system is linked with the HCP system at the NFS share level. If this option is specified, the command displays whether to display the hard quota allocated to the namespace or the block capacity of the file system as the disk capacity of the NFS client.

nfsd2_advanced_acl_type

Specify this to view whether NFS clients are permitted to access file systems of the Advanced ACL type over the NFSv2 protocol.

nfsd3_jukebox_behavior

Specify this to view whether to return an EJUKEBOX response to NFS clients.

`wan_optimization`

Specify this to view the settings for responding to network environment delay times.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-313 Information displayed when executing the nfsoptlist command

Item	Description
`disable_mountd_reply_dumplist`	This option displays whether the list of NFS shares mounted by the requesting client is returned to the client. 0 This value indicates that the list of NFS shares mounted by the requesting client is returned to the client. 1 This value indicates that the list of NFS shares mounted by the requesting client is not returned to the client.
`disable_mountd_reply_exportlist`	This option displays whether the list of NFS shares is returned to the client. 0 This value indicates that the list of NFS shares is returned to the client. 1 This value indicates that the list of NFS shares is not returned to the client.
`disable_rquotad_startup`	This option displays whether the Quota operation from the NFS client is suppressed. 0 This value indicates that the Quota operation from the NFS client is not suppressed. 1 This value indicates that the Quota operation from the NFS client is suppressed.
`nfsd_show_quota_value`	Displays whether to display the hard quota allocated to the namespace or the block capacity of the file system as the disk capacity of the NFS client. Note that this option applies if the capacity is set as limited based on hard namespace quotas when the HDI system is linked with the HCP system at the NFS share level.

Item	Description

	`0`
	
	    The hard quota allocated to the namespace is displayed.
	
	`1`
	
	    The block capacity of the file system is displayed.

`nfsd2_advanced_acl_type`	Displays whether NFS clients are permitted to access file systems of the Advanced ACL type over the NFSv2 protocol.
	
	`0`
	
	    Access is not permitted.
	
	`1`
	
	    Access is permitted.

`nfsd3_jukebox_behavior`	Displays whether to return an EJUKEBOX response to NFS clients.
	
	`0`
	
	    Displays when an EJUKEBOX response is returned.
	
	`1`
	
	    Displays when no EJUKEBOX response is returned.

`wan_optimization`	Displays the settings for the responding to network environment delay times.
	
	`0`
	
	    Displays when the settings specify to act in response to short network environment delay times.
	
	`1`
	
	    Displays when the settings specify to act in response to long network environment delay times.

Return values

Table 2-314 Return values of the nfsoptlist command

Return value	Description
`0`	Normal termination
`1, 3`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.

nfsoptset (Set the NFS environment)

Synopsis

```
nfsoptset keyword=value
```

```
nfsoptset -h
```

Description

Sets the NFS environment for the OS on a node.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Options and arguments

keyword = value

Specify the keyword and the value.
You can specify the following:

```
disable_mountd_reply_dumplist={0|1}
```

This option specifies whether the list of NFS shares mounted by the requesting client is to be returned to the client.

If you set this option not to return the list of NFS shares, the option returns an empty list when both the command `showmount -d` and the command `showmount -a` are executed by the client. In this case, if the NFS client uses any other function to mount the accessed shares automatically, the NFS client might not work.

This command should be executed for each node so that all nodes have the same setting within the cluster. The default setting is 0. Be sure to restart the NFS service if you execute the command with this option specified.

`0`

Specify this value if the list of NFS shares mounted by the requesting client is to be returned to the client.

`1`

Specify this value if the list of NFS shares mounted by the requesting client is not to be returned to the client.

```
disable_mountd_reply_exportlist={0|1}
```

This option specifies whether the list of NFS shares is to be returned to the client.

If you set this option not to return the list of NFS shares, the option returns an empty list when the command `showmount -e` is executed by the client. In this case, if the NFS client uses any other function to mount the accessed shares automatically, the NFS client might not work.

This command should be executed for each node so that all nodes have the same setting within the cluster. The default setting is 0. Be sure to restart the NFS service if you execute the command with this option specified.

`0`

Specify this value if the list of NFS shares is to be returned to the client.

`1`

Specify this value if the list of NFS shares is not to be returned to the client.

`disable_rquotad_startup={0|1}`

This option specifies whether the Quota operation from the NFS client is to be suppressed.

If you set to suppress the Quota operation by using this option, the Quota-related commands executed by the client will terminate abnormally.

This command should be executed for each node so that all nodes have the same setting within the cluster. The default setting is 0. Be sure to restart the NFS service if you execute the command with this option specified.

`0`

Specify this value if the Quota operation from the NFS client is not to be suppressed.

`1`

Specify this value if the Quota operation from the NFS client is to be suppressed.

`nfsd_show_quota_value={0|1}`

This option applies if the capacity is set as limited based on hard namespace quotas when the HDI system is linked with the HCP system at the NFS share level. This option specifies whether to display the hard quota allocated to the namespace or the block capacity of the file system as the disk capacity of the NFS client. The initial value is 0.

`0`

Specify this to display the hard namespace quota allocated to the namespace.

`1`

Specify this to display the block capacity of the file system.

`nfsd2_advanced_acl_type={0|1}`

Specify this to determine whether to permit NFS clients to access file systems of the Advanced ACL type over the NFSv2 protocol. The initial value is 0.

0

Specify this not to permit access.

1

Specify this to permit access.

When NFS clients use the NFSv2 protocol to access file systems of the Advanced ACL type, access control is not performed according to the ACEs. Therefore, permit access to such file systems only when you must use the NFSv2 protocol for system operation.

`nfsd3_jukebox_behavior={0|1}`

Specify this to view whether to return an EJUKEBOX response to NFS clients. Execute this command on each node to ensure the same setting in a cluster. The default value is 0.

0

Specify this to return an EJUKEBOX response.

1

Specify this to not return an EJUKEBOX response.

`wan_optimization={0|1}`

Specify this to set actions in response to the delay time of the network environment. The default value is 0.

If you specify this option and execute the command, restart the NFS service.

0

Specify this to act in response to short network environment delay times.

1

Specify this to act in response to long network environment delay times.

Return values

Table 2-315 Return values of the nfsoptset command

Return value	Description
0	Normal termination
1[#], 2	The error cannot be handled by the system administrator. Contact maintenance personnel.
1[#], 3	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.

\#

The command ended abnormally due to multiple causes.

Example

To permit NFS clients to access file systems of the Advanced ACL type over the NFSv2 protocol:

```
$ sudo nfsoptset nfsd2_advanced_acl_type=1
```

nfsrestore (Restore NFS share information)

Synopsis

```
nfsrestore information-definition-file-name
nfsrestore --list information-definition-file-name
nfsrestore --template template-file-name
    information-definition-file-name
nfsrestore -h
```

Description

Restores information about NFS shares based on the NFS share information that has been backed up to an information definition file by using the `nfsbackup` command. You can also view NFS share information without restoring it, or create a template file of scripts for performing restoration.

Note that depending on the number of NFS shares that will be restored and the number of NFS shares that have already been created, the restoration process might take a while. For example, it takes about two and a half minutes to restore 20 NFS shares.

You can restore NFS share information if the following conditions are met:

- The name of the target file system has not been changed since the NFS information was backed up.
- The target file system has been mounted.
- The directories in which the NFS shares were created still exist in the target file system.
- The target file system has no NFS share information.
- The names of the public destination hosts for NFS shares can be resolved.

Options and arguments

`--list`

   Specify this option to display the contents of an information definition file.

`--template` *template-file-name*

   Specify this option to create a template file of scripts for performing restoration based on the contents of an information definition file.

   Specify a template file name using no more than 255 characters. You can use alphanumeric characters, hyphens (-), and underscores (_). However, hyphens cannot be used as the first character of the file name. You can also use periods (.), except at the beginning or end of the character string.

   The template file will be output immediately under the SSH account home directory (`/home/nasroot`). The file cannot have the same name as an existing file in the `/home/nasroot` directory.

   The template file can be transferred, and then edited or executed on a remote host. If you want to restore NFS share information that is different from the backed up information, edit the template file according to your

purpose, and then execute the template file. To transfer the template file, use the `scp` command or some other secure transfer tools.

The following shows an example of a template file.

```
#!/bin/sh
##############################################################################
#####
# This template is for scripts used to restore NFS share settings.
# Note:
#    You must edit this template to create a script that can handle
#    command execution errors, and execute commands from remote hosts.
##############################################################################
#####

PRECMD=""

/bin/echo "Executing the command nfscreate(/mnt/FS01/dir01)....."
$PRECMD sudo nfscreate -d "/mnt/FS01/dir01" -u "1212" -g "1212" -t
"perform" -s "do_not_perform" -l "perform" -m "16" -H
"10.208.47.0:rw_sync:everyone:sys,@netgroup1:rw_sync_opt:root_only:sys.krb5
"

/bin/echo "Executing the command nfscreate(/mnt/FS01/dir02)....."
$PRECMD sudo nfscreate -d "/mnt/FS01/dir02" -u "65534" -g "65534" -t
"perform" -s "do_not_perform" -l "perform" -m "32" -H
"10.208.136.0/255.255.255.0:rw_sync:everyone:sys.krb5.krb5i,@netgroup01:rw_
sync:everyone:sys.krb5.krb5i"

/bin/echo "Executing the command nfscreate(/mnt/FS01/dir03)....."
$PRECMD sudo nfscreate -d "/mnt/FS01/dir03" -u "65534" -g "65534" -t
"perform" -s "do_not_perform" -l "perform" -m "16" -H
"*:rw_sync:everyone:sys.krb5i"

/bin/echo "Executing the command nfscreate(/mnt/FS01/dir04)....."
$PRECMD sudo nfscreate -d "/mnt/FS01/dir04" -u "1212" -g "1212" -t
"perform" -s "do_not_perform" -l "perform" -m "16" -H
"@netgroup1:rw_sync_opt:root_only:sys.krb5,[fdf1:afcb:
44f9:1000::3:25]:rw_sync:everyone:sys"

exit 0
```

Notes:

- For the variable `PRECMD`, specify the syntax of the `ssh` command to be executed from a remote host.

Example: `ssh -2 nasroot@fshost01`

- When using special characters, use the escape characters appropriate for the remote host environment.

Information-definition-file-name

Specify the name of the information definition file. You can specify only the name of an NFS share information definition file that is immediately under the home directory for the SSH account (`/home/nasroot`).

Displayed information

The following table lists the information displayed by this command when the `--list` option is specified.

Table 2-316 Information displayed when executing the nfsrestore command with the --list option specified

Item	Description
`Backup date and time`	Displays the data and time when information about the NFS share was backed up.
`Shared directory`	Displays the absolute path for the directory of the created NFS share.
`Public destination host/network`	Displays the name of the host or network on which the NFS share is made public.

`Permission mode / Synchronous writing`	Displays information about the access permission for the NFS share and the synchronous write mode.
	
	`ro`
	    The NFS share is read-only.
	
	`rw_sync`
	    Read and write operations are permitted on the NFS share, and synchronous writing without optimization is enabled.
	
	`rw_sync_opt`
	    Read and write operations are permitted on the NFS share, and synchronous writing with optimization is enabled.

`Anonymous mapping`	Displays users who are mapped as anonymous users.
	
	`everyone`
	    All users are mapped as anonymous users.
	
	`root_only`
	    Only the root user is mapped as an anonymous user.
	
	`none`
	    Users are not mapped as anonymous users.

`Anonymous UID`	Displays the user ID to be used when accessing the NFS share as an anonymous user.
`Anonymous GID`	Displays the group ID to be used when accessing the NFS share as an anonymous user.

`Transmission port restriction`	Displays whether the only accepted requests are those from an Internet port whose port number is lower than 1024.
	
	`perform`
	    Transmission ports are restricted.
	
	`do_not_perform`
	    Transmission ports are not restricted.

`Subtree check`	Displays whether the system, in addition to checking the access permission for the file or directory to be accessed, also checks that the user has the execute permission (`x`) for all directories (subtrees) from the shared directory to the directory in which the file or directory to be accessed exists. `perform` A subtree check is performed.

Item	Description
	`do_not_perform` A subtree check is not performed.

`Access check with lock request`	Displays whether there is a check of permissions (authorization) for lock requests.
	
	`perform`
	
	Permissions are checked for lock requests.
	
	`do_not_perform`
	
	Permissions are not checked for lock requests.

`Maximum rwsize(KB)`	Displays the maximum transfer length for the NFS share. When no maximum transfer length is set, `--` is displayed.
`Security flavor`	Displays the security flavor set for the public destination of the NFS share. If multiple destinations have been set, each security flavor is separated by a comma (,).

Return values

Table 2-317 Return values of the nfsrestore command

Return value	Description
`0`	Normal termination
`1, 10`#	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10`#`, 66`#`, 70, 99`#	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65, 66`#	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`80`	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
`97, 98, 99`#	The error cannot be handled by the system administrator. Contact maintenance personnel.
`99`#	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Examples

To restore information about NFS shares according to the following conditions:

- The file system name is `FS1`.
- The information definition file name is `FS1_nfsshares.xml`.

```
$ sudo nfsrestore FS1_nfsshares.xml
```

To create a template file of scripts for performing restoration according to the following conditions:

- The template file name is `FS1_nfsrestore.sh`.
- The information definition file name is `FS1_nfsshares.xml`.

```
$ sudo nfsrestore --template FS1_nfsrestore.sh FS1_nfsshares.xml
```

nfsstatus (Display NFS daemon information)

Synopsis

```
nfsstatus [-m|-z]
nfsstatus -h
```

Description

Displays NFS daemon information. If no options are specified, the command displays the NFS daemon usage information.

Options and arguments

`-m`

Specify this option to display the NFS daemon usage information and the memory usage status.

`-z`

Specify this option to reset all items other than the NFS daemon memory usage status (`Buffer size in use`) to 0. Make sure that you use this option after the NFS service is restarted or the NFS service is halted and then resumed. If you do not do this, then the displayed NFS daemon usage might be higher than usual.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-318 Information displayed when executing the nfsstatus command

Item	Description
`Total number of nfsd threads`	Displays the number of active NFS daemons.
`Number of times that all threads were in use`	Displays the number of times that the usage of active NFS daemons reached 100%.
NFS-daemon-usage	Displays the time distribution (in seconds) about the NFS daemon usage in each 10% interval after the NFS daemons are activated.
`Buffer size in use`	Displays the status of memory usage for the NFS daemon.
`Retry count of buffer acquisition`	Displays the number of retry attempts the NFS daemon makes if it cannot acquire memory.

Return values

Table 2-319 Return values of the nfsstatus command

Return value	Description
`0`	Normal termination
`1`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`70, 71, 72`	The error cannot be handled by the system administrator. Contact maintenance personnel.

nfssvget (Display the port number allocation method for the NFS service)

Synopsis

```
nfssvget --port
nfssvget -h
```

Description

Displays the port number allocation method used by the NFS service.

Options and arguments

`--port`
> Displays the port number allocation method used by the NFS service.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-320 Information displayed when executing the nfssvget command

Item	Description

`Port number allocation`	Displays the port number allocation method used by the NFS service.
	
	`dynamic`
	    Port numbers are dynamically allocated.
	
	`fixed`
	    Fixed port numbers are set.
	
	`privileged`
	    Privileged port numbers are set.

Return values

Table 2-321 Return values of the nfssvget command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`65, 68`[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`68`[#]`, 95`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

nfssvset (Change the port number allocation method for the NFS service)

Synopsis

```
nfssvset --port {dynamic|fixed|privileged}
nfssvset -h
```

Description

Changes the port number allocation method used by the NFS service on the node you are logged in to.

By default, port numbers are dynamically allocated. Change the default setting if you need to allocate fixed port numbers in an environment that uses a firewall.

In a cluster configuration, you must specify the same settings on both nodes.

If you change the port number allocation method, restart the NFS service. The new allocation method will not be applied until you restart the NFS service.

Options and arguments

`--port {dynamic|fixed|privileged}`

　　Specify the port number allocation method to be used by the NFS service.

　　`dynamic`

　　　　Specify this to dynamically allocate port numbers. The default is `dynamic`.

　　`fixed`

　　　　Specify this to set fixed port numbers.

　　`privileged`

　　　　Specify this to set privileged port numbers.

Return values

Table 2-322 Return values of the nfssvset command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
68#, 95	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

nncreset (Reset a node)

Synopsis

```
nncreset [-y] [--vserver virtual-server-ID]
nncreset -h
```

Description

For cluster configurations, resets the other node in the cluster. For single node configurations, resets the node you are logged in to.

Before executing this command, make sure that the OS of the node that you will reset has completely started up. If you execute this command while the node OS is still starting up, you might not be able to collect the dump files on the node, or the node OS might stop running.

Options and arguments

--vserver *virtual-server-ID*
    This option is not supported.

Return values

Table 2-323 Return values of the nncreset command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If

Return value	Description
	this error occurs repeatedly, contact maintenance personnel.
98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

peerstatus (Display the status of the other node in the cluster)

Synopsis

```
peerstatus [-h]
```

Description

Displays the status of the other node in the cluster.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-324 Information displayed when executing the peerstatus command

Item	Description

Status	Displays the status of the other node in the cluster.
	
	BOOT START
	    The OS is starting.
	
	BOOT COMPLETE
	    The OS is running normally.
	
	SHUTDOWN
	    The OS is stopping.
	
	STOP
	    Displayed when:
	    - The OS stops.
	    - The OS is being restarted.
	    - The OS is blocked.
	
	DUMP
	    A dump file is being acquired.
	
	ON
	    Power is supplied to the hardware on the node, and the node is not in any other statuses.
	
	OFF
	    Power is not supplied to the hardware on the node.

Item	Description
	UNKNOWN The status of the OS cannot be acquired.

Note:

> The status at the moment that the command was executed is displayed. However, if a hardware error has occurred, the status before the error occurred might be displayed. In addition, while the OS is being started on the node, ON or the status just before the status changes to OFF might be displayed.

Return values

Table 2-325 Return values of the peerstatus command

Return value	Description
0	Normal termination
1	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.

perfmonctl (Managing the service performance statistics)

Synopsis

```
perfmonctl [--cifs {on|off}] [--nfs {on|off}]
perfmonctl --setdir directory-name
perfmonctl --unsetdir [-y]
perfmonctl -h
```

Description

Specify whether to collect performance statistics of the services on the node to which you are logged in. In addition, you can transfer log files to a directory in the file system to view the collected performance statistics. You can also use this command to view the current settings.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Options and arguments

`--cifs {on|off}`

> If the real-time scan function is running when you modify the settings to not collect the CIFS performance statistics, a scan error might occur.

on

    Collect performance statistics of the CIFS service. The initial setting is
    `on`.

off

    Do not collect performance statistics of the CIFS service.

`--nfs {on|off}`

    If the real-time scan function is running when you modify the settings to
    not collect the NFS performance statistics, a scan error might occur.

on

    Collect performance statistics of the NFS service. The initial setting is
    `on`.

off

    Do not collect performance statistics of the NFS service.

`--setdir` *directory-name*

    To transfer a log file to a directory in the file system, specify the absolute
    path of the directory by using no more than 255 characters, beginning
    with /mnt/. Note
    that `.conflict`, `.conflict_longpath`, `.snaps`, `.history`, `.arc`, `.system
    _gi`, `.system_reorganize`, `lost+found`, or `.lost+found` cannot be
    specified for the directory name.
    In addition, the following directories cannot be specified.
    - A directory in a file system that has been set to reference the data from
    another HDI system as read-only
    - A directory in a home-directory-roaming file system
    - A directory in a read-write-content-sharing file system

    Note:

        The transfer directory requires the following amount of free space:
        `Required free space = (Number of days passed since the output
        of the log file began) x 64MB`
        If the directory does not have enough free space, the log file is not
        transferred and the KAQM09214-E message appears. As a result,
        delete old log data from the directory on a regular basis. We
        recommend that you use the `fsfullmsg` command to enable warning
        notifications that are sent when the file system usage exceeds a
        threshold value.

`--unsetdir`

    Specify this to cancel the setting for the transfer directory specified by the
    `--setdir` option.

    Note:

        Before deleting the transfer directory, cancel the setting for the
        directory.

If you omit all options, the current setting is displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-326 Information displayed when executing the perfmonctl command

Item	Description
Collecting performance statistics	Displays information about the collection of the performance statistics of a service.
CIFS	Displays whether to collect performance statistics of a CIFS service. On 　　Collect performance statistics of the CIFS service. Off 　　Do not collect performance statistics of the CIFS service.
NFS	Displays whether to collect performance statistics of an NFS service. On 　　Collect performance statistics of the NFS service. Off 　　Do not collect performance statistics of the NFS service.
Output-destination directory	Displays the directory used for saving the transferred log file of the performance statistics. If no transfer directory is specified, Unsetting is displayed.

Return values

Table 2-327 Return values of the perfmonctl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

pmctl (Manage private maintenance port interfaces)

Synopsis

```
pmctl [-p {v4|v6}] [-a IP-address -n netmask interface]
pmctl
pmctl -p v6 --delete interface
pmctl [-p {v4|v6}]
pmctl -h
```

Description

Sets an interface for the private maintenance port. You can also use this command to view the current settings.

Note that an IPv4 IP address is required for the interface of the private maintenance port.

The network addresses that are allocated to the private maintenance port are `192.168.0.0`, `192.168.233.0`, `10.0.0.0`, `172.23.211.0`, `10.197.181.0`, and addresses from `fe80::1:00` to `fe80::1:ff`.

This command is applied to the node on which the command is executed. In cluster configurations, this command must be executed on both nodes.

Options and arguments

`-a` *IP-address*

For a cluster configuration, specify the fixed IP addresses of the private maintenance port.

For a single node configuration, specify the IP address of the private maintenance port.

`-n` *netmask*

For IPv4, specify this to use a netmask for a fixed IP address. As the netmask, `255.255.255.0` is always used.

For IPv6, specify this to use a prefix length for a fixed IP address. As the prefix length, `64` is always used.

`-p` `{v4|v6}`

Specify the protocol version of the interface for the private maintenance port. If you omit this option when setting up the interface, the protocol version determined from the specified IP address is set. If you omit this option when referencing the interface settings, interface information in IPv4 and IPv6 format is displayed.

v4

    Specify this to use IPv4 IP addresses.

v6

    Specify this to use IPv6 IP addresses.

-p v6 --delete

    Specify this to delete the interface for the private maintenance port. This option takes effect when an interface for the private maintenance port has been set in IPv6.

interface

    Specify the name of the private maintenance port for which you are setting an interface.

If you omit all the options, the current settings are displayed.

Displayed information

The following table lists the information displayed when this command is executed in a cluster configuration.

Table 2-328 Information displayed when the pmctl command is executed in a cluster configuration

Item	Description
Interface	Displays the port name.
Fixed IP addr	Displays the fixed IP address of the node you are logged in to.
Netmask	For IPv4, the netmask of the node you are logged in to appears.
Prefix length	For IPv6, the prefix length of the node you are logged in to appears.

Note:

    The items for which information is set are displayed in the following order:

    ○   Interface information items set for IPv4 for the private maintenance port on the node you are logged in to

    ○   Interface information items set for IPv6 for the private maintenance port on the node you are logged in to

The following table lists the information displayed when this command is executed in a single-node configuration.

Table 2-329 Information displayed when the pmctl command is executed in a single-node configuration

Item	Description
Interface	Displays the port name.

Item	Description
IP address	Displays the IP address.
Netmask	For IPv4, the netmask appears.
Prefix length	For IPv6, the prefix length appears.

Note:

The items for which information is set are displayed in the following order:

- Interface information items set for IPv4 for the private maintenance port
- Interface information items set for IPv6 for the private maintenance port

Return values

Table 2-330 Return values of the pmctl command

Return value	Description
0	Normal termination
1, 3	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To view interface information for the private maintenance port:

```
$ sudo pmctl
Interface       : pm0
 [IPv4]
 Fixed IP addr  : 172.23.211.10
 Netmask        : 255.255.255.0
 [IPv6]
 Fixed IP addr  : 3ffe:200:0:10a::1
 Prefix length  : 64
```

the fixed IP address of the interface for the private maintenance port to
`172.23.211.10`:

```
$ sudo pmctl -a 172.23.211.10 -n 255.255.255.0 pm0
```

To use IPv6 IP addresses to set the fixed IP address of the interface for the
private maintenance port to `3ffe:200:0:10a::1`:

```
$ sudo pmctl -p v6 -a [3ffe:200:0:10a::1] -n 64 pm0
```

quotaget (Display the quota information set for each file system)

Synopsis

```
quotaget [-c] [-n] [-u [user-name|user-ID][,[user-name|user-ID]...]|
    -g [group-name|group-ID][,[group-name|group-ID]...]]
    file-system-name
quotaget [-c] [-u|-g] -v file-system-name
quotaget [-c] [-n] [-u|-g] -w file-system-name
quotaget [-c] -d file-system-name
quotaget [-c] -t file-system-name
quotaget [-c] -m file-system-name
quotaget -h
```

Description

Displays the information and current usage status of the quota that is set for
each file system.

When you want to view the quota information of a user or group, the
displayed information varies, depending on the combination of an option and
an argument. Use options and arguments appropriately according to your
purpose.

When specifying a specific user or group
    The quota information of a specified user or group is displayed.

When specifying the `-v` option
    The quota information of all users or groups registered by File Services
    Manager, the NIS server, and the LDAP server for user authentication is
    displayed.

When you specify the `-w` option
    The information of users and groups that have exceeded the soft limit or
    grace period, among all users or groups registered by File Services
    Manager, the NIS server, and the LDAP server for user authentication, is
    displayed.

When you omit the `-v` option and `-w` option without specifying a specific user or group

The following information is displayed:

- The quota information of all users or groups that are using the file system
- The information of all users or groups for which quotas are set

Options and arguments

`-c`

Specify this to display quota information in colon-separated format. Note that the block usage, the soft limit for block usage, and the hard limit for block usage are displayed in MB (even though no unit is designated).

`-d`

Specify this to display the default quota information set for a specified file system.

`-g`

Specify this option if you want to view group quota information.

`-g [ group-name | group-ID ] [, [ group-name | group-ID ] ...]`

If you want to view the specific group information only, specify the target group names or group IDs.

You can specify any of the following groups by the group name. Note that the built-in group of a Windows domain cannot be specified.

- Groups registered by File Services Manager (group IDs: 97 and 200 to 2147483147)
- Groups registered in the NIS server or LDAP server for user authentication (other than groups whose group ID is 0)
- Groups registered by user mapping
- Groups authenticated by Active Directory

To specify groups that were authenticated by Active Directory, specify the domain name and group name in the following format:

"domain-name\group-name" or domain-name\\group-name

When you specify a group ID, specify a valid value within the range 0 to 2147483147. Note that you cannot specify 0 at the beginning of a group ID that begins with a value other than 0.

When specifying multiple group names or group IDs, separate them with commas (,). Group names and group IDs can coexist.

If multiple groups are specified and one of the group names or group IDs is invalid, quota information will not be displayed for any groups.

`-m`

Specify this to view the quota monitoring method.

`-n`

Specify this option to not display the quota information for user IDs or group IDs that cannot be converted to user names or group names.

-t

Specify this option to view the grace period after the soft limit is exceeded.

-u

Specify this option to view user quota information.

-u [*user-name* | *user-ID*] [, [*user-name* | *user-ID*] ...]

Specify this option to view the information of a specific user.

You can specify any of the following users by the user name. Note that the built-in user of a Windows domain cannot be specified.

- ○ Users registered by File Services Manager (user IDs: 97 and 200 to 2147483147)
- ○ Users registered in the NIS server or LDAP server for user authentication (other than users whose user ID is 0)
- ○ Users registered by user mapping
- ○ Users authenticated by Active Directory

To specify users that were authenticated by Active Directory, specify the domain name and user name in the following format:

"*domain-name**user-name*" or *domain-name**user-name*

When you specify a user ID, specify a valid value within the range 0 to 2147483147. Note that you cannot specify 0 at the beginning of a user ID that begins with a value other than 0.

When specifying multiple user names or user IDs, separate them with commas (,). User names and user IDs can coexist.

If multiple users are specified and one of the user names or user IDs is invalid, quota information will not be displayed for any users.

-v

Specify this option to view the quota information of all users or groups registered by File Services Manager, the NIS server, and the LDAP server for user authentication.

-w

Specify this option to view only the information of users or groups that have exceeded the soft limit or grace period.

file-system-name

Specify the name of the file system.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-331 Information displayed when executing the quotaget command (quota information of a user or group)

Item	Description
`List of Quota Information of File System`	The file system name is displayed.
`User name or Group name`	The user name or the group name is displayed. If the user ID or group ID cannot be converted to a user name or group name, a hyphen (`-`) is displayed.
`UID or GID`	The user ID or the group ID is displayed.

`Block`	Block usage by individual users or each group is displayed.
	`Used capacity`
	
	    The block usage is displayed as an integer followed by the unit (MB, GB, or TB). The value is rounded up to the nearest integer. In addition to this information, the value in MB is also displayed in parentheses.
	
	`Soft limit`
	
	    The soft limit for block usage is displayed as an integer followed by the unit (MB, GB, or TB). In addition to this information, the value in MB is also displayed in parentheses.
	
	`Hard limit`
	
	    The hard limit for block usage is displayed as an integer followed by the unit (MB, GB, or TB). In addition to this information, the value in MB is also displayed in parentheses.
	
	`Grace period`
	
	    Remaining grace time until a new block can no longer be assigned after the block usage exceeds the soft limit. Displayed in one of the following formats:
	
	    n `days`
	
	    The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.
	
	    n `hours`
	
	    The remaining grace time is less than 24 hours. For example, `0 hours` appears if less than 1 hour remains.
	
	    `over`
	
	    Either the grace period has expired or block usage has reached the hard limit.
	
	    `-`
	
	    The user's or group's block usage is within the soft limit.
	
	When either of the following conditions is met, `0MB(0MB)` is displayed for `Soft limit` and `Hard limit`:
	
	• No soft or hard limit is specified for block usage.

Item	Description
	• The target file system is of the Advance ACL type and the user name is __groupowner (user ID: 4294967292).
i-node	inode usage by individual users or each group is displayed. Used count Number of inodes used. Soft limit Soft limit for inode usage. Hard limit Hard limit for inode usage. Grace period Remaining grace time until files can no longer be created after the user's or group's inode usage exceeds the soft limit. Displayed in one of the following formats: *n* days The remaining grace time is 24 hours or longer. For example, 1 days appears if there are 24 hours or more, but less than 48 hours remaining. *n* hours The remaining grace time is less than 24 hours. For example, 0 hours appears if less than 1 hour remains. over Either the grace period has expired or inode usage has reached the hard limit. – The user's or group's inode usage is within the soft limit. When either of the following conditions is met, 0 is displayed for Soft limit and Hard limit: • No soft or hard limit is specified for inode usage. • The target file system is of the Advance ACL type and the user name is __groupowner (user ID: 4294967292).

Table 2-332 Information displayed when executing the quotaget command (the default quota)

Item	Description
Default Quota Information of File System	The file system name is displayed.
Block	The soft and hard limit values for block usage that have been set as the default quotas are displayed. Soft limit(default) The soft limit for block usage is displayed as an integer followed by the unit (MB, GB, or TB). In addition to this

Item	Description
	information, the value in MB is also displayed in parentheses.
	`Hard limit(default)` The hard limit for block usage is displayed as an integer followed by the unit (MB, GB, or TB). In addition to this information, the value in MB is also displayed in parentheses.
	If the soft limit and the hard limit for block usage are not specified, `0MB(0MB)` appears for `Soft limit(default)` and for `Hard limit(default)`.

`i-node`	The soft and hard limits values for inode usage that have been set as the default quotas are displayed.
	
	`Soft limit`
	
	Soft limit for inode usage.
	
	`Hard limit`
	
	Hard limit for inode usage.
	
	If the soft limit and the hard limit for inode usage are not specified, `0` appears for `Soft limit` and for `Hard limit`.

Table 2-333 Information displayed when executing the quotaget command (the grace period)

Item	Description
`Grace Period Information of File System`	The file system name is displayed.
`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`	Displays the grace period until files can no longer be created after inode usage exceeds the soft limit.

Table 2-334 Information displayed when executing the quotaget command (the monitoring method)

Item	Description
`Monitoring Time of File System`	The file system name is displayed.

`SNMP notification mode`	Displays the SNMP trap notification mode that applies when a quota is exceeded.
	
	`Use a summary notification`
	
	Summary notification mode is set.
	
	`Use individual notifications`
	
	Individual notification mode is set.

monitoring-times	Displays quota monitoring times. If more than one time is set, each additional time is displayed on an additional line.

Item	Description
	Note that if the `-c` option is specified, multiple monitoring times are delimited by commas (`,`) and the colon (`:`) is omitted from each monitoring time.

Return values

Table 2-335 Return values of the quotaget command

Return value	Description
`0`	Normal termination
`1, 10`[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10`[#]`, 70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65, 66`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

quotaset (Set quotas for each file system)

Synopsis

```
quotaset
    {-u {user-name|user-ID}[,{user-name|user-ID}...]|
    -g {group-name|group-ID}[,{group-name|group-ID}...]}
    [-b block-soft-limit,block-hard-limit]
    [-i inode-soft-limit,inode-hard-limit]
    file-system-name
quotaset -d
    [-b block-soft-limit,block-hard-limit]
    [-i inode-soft-limit,inode-hard-limit]
    file-system-name
quotaset -t
    [-b block-grace-period]
    [-i inode-grace-period]
    file-system-name
```

```
quotaset -m
    {[-s monitoring-time[,monitoring-time...]]
    [-n {summary|individual}]|
    -s default}
    file-system-name
quotaset -h
```

Description

Set quotas for each file system.

Options and arguments

-b *block-soft-limit* , *block-hard-limit*

Specify the soft limit and hard limit for block usage with a comma (,) placed between them. Specify an integer value and a unit from 0 MB to 1,023 TB. After a specified value, add M, G, or T to indicate the unit (M: MB; G: GB; T: TB). If the unit is not specified, MB is assumed. Note that this option takes effect when the -d option is also specified or when the -d, -t, or -m option is not specified.

If this option is omitted, the soft and hard limits for block usage are set as follows:

When the -d option is specified:

> If the default quota is already specified, the current setting value is inherited.

> If no default quota is set, the soft and hard limits for block usage will be set to 0 (no limits).

When the -g option is specified:

> If a quota is already specified for the group, the current setting value is inherited.

> If no quota is set for the specified group, the soft and hard limits for block usage will be set to 0 (no limits).

When the -u option is specified:

> If a quota is already specified for the user, the current setting value is inherited.

> If only a default quota is set and no quota is set for the user, the set default quota will apply.

> If no default quota is set and no quota is set for the specified user, the soft and hard limits for block usage by the specified user will be set to 0 (no limits).

-b *block-grace-period*

Specify the grace period (units: days) until a new block can no longer be assigned after the block usage exceeds the soft limit. Specify a value from 1 to 9,999. The value cannot begin with 0. Note that this option takes effect only the -t option is also specified.

The latest end time for a grace period is 2038/1/19 03:14:07. Therefore, if the value 9,999 is set for this option and the date and time when the

amount of block usage exceeds the soft limit is `2038/1/19 00:00:00`, the remaining grace period at that point will be 3 hours 14 minutes and 7 seconds.

The initial setting is 7 days. If you omit this option, the current setting information applies.

`-d`

Specify this option if you want to set the default quota for the specified file system.

`-g` { *group-name* | *group-ID* } [, { *group-name* | *group-ID* } ...]

Specify the group names or group IDs for which you want to set quotas.

You can specify any of the following groups by the group name. Note that the built-in group of a Windows domain cannot be specified.

- Groups registered by File Services Manager (group IDs: 97 and 200 to 2147483147)
- Groups registered in the NIS server or LDAP server for user authentication (other than groups whose group ID is 0)
- Groups registered by user mapping
- Groups authenticated by Active Directory

To specify groups that were authenticated by Active Directory, specify the domain name and group name in the following format:

"*domain-name\group-name*" or *domain-name\\group-name*

When you specify a group ID, specify a valid value within the range 0 to 2147483147. Note that you cannot specify 0 at the beginning of a group ID that begins with a value other than 0.

When specifying multiple group names or group IDs, separate them with commas (,). Group names and group IDs can coexist.

If multiple groups are specified and one of the specified group names or group IDs is invalid, a quota is not set for any of the specified groups.

`-i` *inode-soft-limit* , *inode-hard-limit*

Specify the soft limit and hard limit for inode usage with a comma (,) placed between them. You can specify a value from `0` to `4294967295`. Note that this option takes effect when the `-d` option is also specified or when the `-d`, `-t`, or `-m` option is specified.

If this option is omitted, the soft and hard limits for inode usage are set as follows:

When the `-d` option is specified:

If the default quota is already set, the current setting value is inherited.
If no default quota is set, the soft and hard limits for inode usage will be set to `0` (no limits).

When the `-g` option is specified:

If a quota is already set for the group, the current setting value is inherited.

Hitachi Data Ingestor CLI Administrator's Guide

If no quota is set for the specified group, the soft and hard limits for inode usage by the specified group will be set to `0` (no limits).

When the `-u` option is specified:

If a quota is already set for the user, the current setting value is inherited.

If only a default quota is set and no quota is set for the user, the set default quota will apply.

If no default quota is set and no quota is set for the specified user, the soft and hard limits for inode usage by the specified user will be set to `0` (no limits).

`-i` *inode-grace-period*

Specify the grace period (units: days) until files can no longer be created after inode usage exceeds the soft limit. Specify a value from 1 to 9,999. The value cannot begin with 0. Note that this option takes effect when the `-t` option is also specified.

The latest end time for a grace period is `2038/1/19 03:14:07`. Therefore, if the value `9,999` is set for this option and the date and time when the amount of block usage exceeds the soft limit is `2038/1/19 00:00:00`, the remaining grace period at that point will be 3 hours 14 minutes and 7 seconds.

The initial setting is 7 days. If you omit this option, the current setting information applies.

`-m`

Specify this option to set or clear the quota monitoring method.

`-n {summary|individual}`

Specify this option to set the SNMP trap notification mode when File Services Manager detects users or groups that exceed the soft limit or grace period.

The initial setting disables the SNMP trap notification. If you omit this option with no monitoring times set, the summary notification mode is applied. Also, if you omit this option with one or more monitoring times set, the current setting information applies.

`summary`

Specify this to output an SNMP trap in summary notification mode. You can also specify `s` instead of `summary`.

`individual`

Specify this to output an SNMP trap in individual notification mode. You can also specify `i` instead of `individual`.

If more than 100 users or groups exceeded their soft limit or grace period, individual notifications are suppressed and only the number of users or the number of groups that exceeded their soft limit or grace period are reported to the SNMP manager.

`-s`

Specify this option to set or clear monitoring times for File Services Manager to monitor quotas.

The initial setting is no quota monitoring. If you omit this option, the current setting information applies.

monitoring-time [, *monitoring-time* ...]

>Specify the times at which File Services Manager monitors quotas. All previously set monitoring times are cleared, and then the specified times are set.

>Specify a value from 00 hours 00 minutes to 23 hours 55 minutes (format: *hhmm*) in units of 5 minutes. If specifying a value by using a colon (:) as a delimiter, you can omit 0 at the uppermost digit of hours and minutes of the monitoring time. For example, to specify 01 hour 05 minutes as a monitoring time, write `01:05`, `01:5`, `1:05`, `1:5`, or `0105`.

>Separate multiple monitoring times with commas. You can specify a maximum of 48 monitoring times.

`default`

>Specify this option to clear all monitoring times and set quota monitoring to the initial state (no monitoring).

`-t`

Specify this option to set a grace period.

`-u` { *user-name* | *user-ID* }[, { *user-name* | *user-ID* } ...]

>Specify the user names or user IDs for which you want to set quota.

>You can specify any of the following users by user name. Note that the built-in user of a Windows domain cannot be specified.

>○ Users registered by File Services Manager (user IDs: 97 and 200 to 2147483147)

>○ Users registered in the NIS server or LDAP server for user authentication (other than users whose user ID is 0)

>○ Users registered by user mapping

>○ Users authenticated by Active Directory

>To specify users that were authenticated by Active Directory, specify the domain name and user name in the following format:

>"*domain-name\user-name*" or *domain-name\\user-name*

>When you specify a user ID, specify a valid value within the range 0 to 2147483147. Note that you cannot specify 0 at the beginning of a user ID that begins with a value other than 0.

>When specifying multiple user names or user IDs, separate them with commas (,). User names and user IDs can coexist.

>If multiple users are specified and one of the specified user names or user IDs is invalid, a quota is not set for any of the specified users.

>Even if the target file system is of the Advanced ACL type and `__groupowner` (user ID: 4294967292) is specified as the user name, no quota will be set.

file-system-name
  Specify the name of the file system.

Return values

Table 2-336 Return values of the quotaset command

Return value	Description
0	Normal termination
1, 10#	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10#, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
  The command ended abnormally due to multiple causes.

Examples

To set user quotas according to the following conditions:

- The file system name is `FS1`.
- Set quotas for `User1` (user ID: `6000`) and `User2` (user ID: `6001`).
- Set the soft limit of block usage to 1 GB and the hard limit to 2 GB.
- Set the soft limit of inode usage to `300` and the hard limit to `400`.

```
$ sudo quotaset -u User1,6001 -b 1g,2g -i 300,400 FS1
```

To set user quotas according to the following conditions:

- The file system name is `FS1`.
- Set quotas for `user3`, which was registered by user mapping.
- Set the soft limit of block usage to 1 GB and the hard limit to 2 GB.
- Set the soft limit of inode usage to `300` and the hard limit to `400`.

```
$ sudo quotaset -u "DOMAIN02\user3" -b 1g,2g -i 300,400 FS1
```

Command Reference

To set group quotas according to the following conditions:

- The file system name is `FS1`.
- Set quotas for `Group1` (group ID: `5000`) and `Group2` (group ID: `5001`).
- Set the soft limit of block usage to 1 GB, and the hard limit to 2 GB.
- Set the soft limit of inode usage to `300`, and the hard limit to `400`.

```
$ sudo quotaset -g Group1,5001 -b 1g,2g -i 300,400 FS1
```

To set a default quota according to the following conditions:

- The file system name is `FS1`.
- Set the soft limit of block usage to 1 GB and the hard limit to 2 GB.
- Set the soft limit of inode usage to `300` and the hard limit to `400`.

```
$ sudo quotaset -d -b 1g,2g -i 300,400 FS1
```

To set grace periods according to the following conditions:

- The file system name is `FS1`.
- Set the grace period for block usage to 10 days.
- Set the grace period for inode usage to 10 days.

```
$ sudo quotaset -t -b 10 -i 10 FS1
```

To set the monitoring method according to the following conditions:

- The file system name is `FS1`.
- Set the quota monitoring times to 01:05 and 13:15.
- Use SNMP traps or email notifications to report summary information.

```
$ sudo quotaset -m -s 0105,1315 -n summary FS1
```

rgmon (Disable and restart resource group monitoring)

Synopsis

```
rgmon {-on|-off} [--] resource-group-name
rgmon -h
```

Description

Disables or restarts monitoring of a resource group.

You can execute this command when the resource group status is as follows:

To disable resource group monitoring:
The resource group status is `Online/No error`.

To restart resource group monitoring:

The resource group status is `Online Maintenance/No error`.

Options and arguments

`-off`

Specify this if you want to disable monitoring of the resource group.

The resource group will automatically restart monitoring when the following operations are performed:

- The resource group is stopped or started (including the behaviors performed when a cluster is operated).
- The execution node of the resource group is changed.

`-on`

Specify this option if you want to restart monitoring of the resource group.

resource-group-name

Specify the name of the resource group you want to disable or restart monitoring of.

Return values

Table 2-337 Return values of the rgmon command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 22, 32, 33, 66, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 68	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To disable monitoring of the resource group `node0`:

```
$ sudo rgmon -off node0
```

To restart monitoring of the resource group `node0`:

```
$ sudo rgmon -on node0
```

rgmove (Change the execution node of a resource group)

Synopsis

```
rgmove [-y] [--] resource-group-name
rgmove -h
```

Description

Changes the execution node of a resource group.

You can execute this command when the status of the destination node and resource group to be moved is as follows:

- The status of the destination node is `UP`.

- The status of the resource group to be moved is `Online/No error` or `Online Maintenance/No error`.

You can use the `clctl` command to check the timeout values for the processing that changes the execution node of the resource group.

Notes:

- If the `nasshutdown` or `nasreboot` commands are executed for a node in the same cluster while the this command is processing, the processing might not finish. Confirm that the status of the resource group to be moved is `Online/No Error`, and then execute the `nasshutdown` or `nasreboot` commands.

- If a resource group that is failed over is failed back to the default startup node and the resource group fails to start on the destination node (the default startup node), the resource group restarts on the source node. If the restart is successful, the `rgmove` command terminates normally. After executing the `rgmove` command, check the operating node by using the `clstatus` command.

Options and arguments

resource-group-name
    Specify the name of the resource group whose execution node you want to change.

Return values

Table 2-338 Return values of the rgmove command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 22, 30, 37, 38, 39, 66, 69[#], 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
68, 69[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Example

To change the execution node of the resource group `node0`:

```
$ sudo rgmove node0
KAQM06136-Q Performing this operation will temporarily stop the services.
Are you sure you want to change the execution node of the resource group?
(y/n)
```

rgstart (Start a resource group)

Synopsis (for cluster configurations)

```
rgstart [--] resource-group-name
```

Synopsis (for single node configurations)

```
rgstart [-q]
```

Synopsis (to reference the command syntax)

```
rgstart -h
```

Description

Starts a resource group on the default startup node.

If the resource group fails to start on the default startup node, the start processing for the resource group is executed on the other node. If the startup is successful, the `rgstart` command terminates normally.

You can execute this command when the status of the cluster, nodes, and resource groups is as follows:

- `ACTIVE` is displayed in `Cluster status`.
- `UP` is displayed in `Node status` for the node of the resource group to be started.
- For cluster configurations, `Offline/No error` or `Online Ready/No error` is displayed in `Resource group status` for the resource group to be started.
- For single node configurations, `Offline/No error` is displayed in `Resource group status` for the resource group to be started.

Options and arguments

`-q`

This option can be used in single-node configurations. Specify this if you do not want to display the progress of resource group start processing.

resource-group-name

Specify the name of the resource group you want to start.

Return values

Table 2-339 Return values of the rgstart command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 22, 31, 35, 42, 66, 69[#], 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 68, 69[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Example

To start the resource group `node0`:

```
$ sudo rgstart node0
```

rgstatus (Display resource group status)

Synopsis (for cluster configurations)

```
rgstatus [-c] [--] [resource-group-name]
```

Synopsis (for single node configurations)

```
rgstatus
```

Synopsis (to reference the command syntax)

```
rgstatus -h
```

Description

Displays the status of resource groups.

Options and arguments

`-c`

Specify this to display resource group status information separated with colons (`:`). When the `-c` option is specified, any colon (`:`) contained in the resource group names is replaced with a hash mark (`#`).

resource-group-name

Specify this argument to view the status of a particular resource group.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-340 Information displayed when executing the rgstatus command

Item	Description
`--Resource Group Status--`	Status of the resource group is displayed.
	If you do not specify a resource group, the command displays the status of the resource group belonging to the node you are logged in to, and the status of the resource group belonging to the other node in the cluster, in that order.
`Resource group name`	Name of a resource group is displayed.
`Resource group status`	Status and error information about a resource group, displayed in the following format:

Item	Description	
	resource-group-status/error-information	
	resource-group-status	`Online Ready` [1]
		The resource group cannot start because the cluster is inactive, or an error was detected when the cluster was stopping.
		`Initializing`
		The resource group is initializing.
		`Discovery (exclusivity)`
		Online processing is being performed for the resource group, before operations begin.
		`Online Pending`
		The resource group is starting.
		`Online`
		The resource group is active.
		`Online Maintenance`
		Monitoring is disabled. If a failure occurs automatic failover will not be performed.
		`Offline Pending`
		The resource group is stopping.
		`Offline` [1]
		The resource group is stopped.
		`Internal Error`
		An internal error was detected. Contact the maintenance personnel.
		`Partial Online`
		If a single node configuration is used, the resource group is partially blocked.
	error-information [2]	`No error`
		No errors occurred.
		`Internal error - not recoverable`
		An unrecoverable internal error occurred. Contact the maintenance personnel.
		`Monitor activity unknown`
		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.

Item	Description

	`No available nodes` or `No available nodes in failure domain after monitor failure`
	
	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.
	
	`Node not available (exclusivity)`
	
	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.
	
	`Node unknown`
	
	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.
	
	`Split resource group (exclusivity)`
	
	A duplicate resource group is active in the cluster. Perform a forced stop for the cluster, and then ask maintenance personnel to stop and restart the OS on the nodes in the cluster.
	
	`srmd executable error`
	
	An error occurred during start or stop processing. Perform a forced stop and fix the problem.
	
	`OS error`
	
	For single node configurations, an error occurred during start or stop processing. Perform a forced stop and fix the problem

`Running node`	Name of the node on which the resource group is running is displayed.

Note:

If you execute the `rgstatus` command immediately after executing the `clstart` command or the `ndstart` command, the command might remain in the processing status for some time.

#1:

> This information is also displayed when the cluster status is `DISABLE`. If `Online Ready`, or `Offline` is displayed, execute the `clstatus` command and also check the cluster status.

#2:

> For details on how to correct each type of error, see the *Administrator's Guide*.

Return values

Table 2-341 Return values of the rgstatus command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 22, 66, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 68	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

rgstop (Stop a resource group)

Synopsis (for cluster configurations)
```
rgstop [-f] [-y] [--] resource-group-name
```

Synopsis (for single node configurations)
```
rgstop [-f] [-y] [-q]
```

Synopsis (to reference the command syntax)
```
rgstop -h
```

Description

Stops a resource group.

For cluster configurations, you can execute this command when the status of the resource group is `Online/No error`, `Online Ready/No error`, or `Online Maintenance/No error`. For single node configurations, you can execute this command when the status of the resource group is `Online/No error` or `Partial Online`. In addition, before executing this command, notify the administrator of the NFS client host that the NFS share will be inaccessible until the resource group is started.

Options and arguments

`-f`

Specify this option if you want to forcibly stop the specified resource group. If processing is discontinued due to an error during startup or stopping of a cluster, node, or resource group, you can forcibly stop the resource group by specifying this option.

`-q`

This option can be used in single-node configurations. Specify this if you do not want to display the progress of resource group stop processing.

resource-group-name

Specify the name of the resource group you want to stop or forcibly stop.

Return values

Table 2-342 Return values of the rgstop command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 22, 30, 41, 66, 69, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 68	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

rmfile (Delete a file stored in the home directory)

Synopsis

```
rmfile [-y] [--] file-name
rmfile -h
```

Description

Deletes a file stored in the home directory for the SSH account (`/home/nasroot`).

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Options and arguments

file-name

Specify the name of the file you want to delete from the home directory. Note that you cannot specify a file name that includes double quotation marks ("), dollar signs (`$`), apostrophes (`'`) , asterisks (`*`), forward slashes (`/`), colons (`:`), left angle brackets (`<`), right angle brackets (`>`), question marks (`?`), backslashes (`\`), grave accent marks (`` ` ``), and vertical bars (`|`). You also cannot specify a file name that has only one period (`.`) or two periods (`..`).

Return values

Table 2-343 Return values of the rmfile command

Return value	Description
0	Normal termination
1, 5	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
13, 14, 16	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

routeadd (Add routing information)

Synopsis (for a cluster configuration)

```
routeadd [-p {v4|v6}] -t net -d network-address -n netmask
    [-g gateway|--reject] [-m segment-size] [-S virtual-server-name]
    interface
routeadd [-p {v4|v6}] -t host -d host
    [-g gateway|--reject] [-m segment-size] [-S virtual-server-name]
    interface
routeadd [-p {v4|v6}] -t default
    {-g gateway|--reject} [-m segment-size] [-S virtual-server-name]
    interface
```

Synopsis (for a single-node configuration)

```
routeadd [-p {v4|v6}] -t net -d network-address -n netmask
    [-g gateway|--reject] [-m segment-size] interface
routeadd [-p {v4|v6}] -t host -d host
    [-g gateway|--reject] [-m segment-size] interface
routeadd [-p {v4|v6}] -t default
    {-g gateway|--reject} [-m segment-size] interface
```

Synopsis (to reference the command syntax)

```
routeadd -h
```

Description

Adds routing information to an interface.

In a cluster configuration, processing for this command is executed for both nodes of the cluster.

You cannot specify an IP address from the networks below as a routing target.

- The network of an IP address set in the private maintenance port
  You can use the `pmctl` command to check the network that contains the IP address set for the maintenance port.
- The network of an IP address set in the heartbeat port
  You can use the `clstatus` command to check the network that contains the IP address set for the heartbeat port.

In addition, you cannot specify the same routing targets as those that are already set in the routing information.

For routing targets set in the routing information, you can use the `routelist` command to check the routing targets set by the system administrator, and you can use the `routelist -l` command to check the routing targets set automatically by the system.

When executing this command, note the following points:

- Routing information that you added with `net` specified in the `-t` option and `0.0.0.0` or `0` specified for the `-n` option operates as the default route.
- Routing information that you added with `net` specified in the `-t` option and `255.255.255.255` or `128` specified for the `-n` option operates the same way as routing in which you directly specify a host as the routing target.
- 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.

Options and arguments

`-d` *target*

Specify the routing target.

network-address

To set a network as the routing target, specify a network address.

host

To set a host as the routing target, specify a host name or IP address.

`-g` *gateway*

Specify the host name or IP address of the gateway.

`-m` *segment-size*

For IPv4, specify the maximum segment size ranging from 64 to 65,536 (in bytes) for TCP connections over this route. If you omit this option, the result of subtracting 40 from the MTU value set for the specified interface is set.

`-n` *netmask*

For IPv4, specify the netmask to set a network as the routing target.

For IPv6, specify the prefix length to set a network as the routing target.

`-p` `{v4|v6}`

Specify the protocol version of the routing information to be added. If you omit this option, the protocol version determined from the specified IP address is set. If a protocol version cannot be determined, `v4` is set.

`v4`

Specify this to use IPv4 IP addresses.

`v6`

Specify this to use IPv6 IP addresses.

`--reject`

Specify this to set a reject route.

-S *virtual-server-name*

This option is not supported.

-t {net|host|default}

Set the specification method for the routing target.

net

Specify this to set a network as the routing target.

host

Specify this to set a host as the routing target.

default

Specify this to set the default route as the route. You can have only one default route.

interface

Specify the interface to which the routing information will be added. Specify the name of the interface for which the `iflist` command can acquire information.

If a tagged VLAN is used, specify it in the following format:

port-name.*VLAN-ID*

Return values

Table 2-344 Return values of the routeadd command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 11, 66[#], 67, 70, 71[#], 72	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Examples

To add routing information to the data port interface `eth12` according to the following conditions:

- The routing target address is `172.16.3.0`.
- The netmask is `255.255.255.0`.
- The gateway address is `172.16.2.1`.

```
$ sudo routeadd -t net -d 172.16.3.0 -n 255.255.255.0 -g 172.16.2.1 eth12
```

To use IPv6 IP addresses to add routing information to the data port (`eth12`):

- The routing target address is `2001:2c0:418:10::0`.
- The prefix length is `64`.
- The gateway is `fd00::4`.

```
$ sudo routeadd -p v6 -t net -d [2001:2c0:418:10::0] -n 64 -g [fd00::4]
eth12
```

routedel (Delete routing information)

Synopsis (for a cluster configuration)
```
routedel [-p {v4|v6}] -d network-address -n netmask
    [-g gateway] [-f] [-V] [--nochk] [-S virtual-server-name]
    interface
routedel [-p {v4|v6}] -d {host|default}
    [-g gateway] [-f] [-V] [--nochk] [-S virtual-server-name]
    interface
routedel [-p {v4|v6}] --all [-f] [-V]
```

Synopsis (for a single-node configuration)
```
routedel [-p {v4|v6}] -d network-address -n netmask
    [-g gateway] [-f] [-V] [--nochk] interface
routedel [-p {v4|v6}] -d {host|default}
    [-g gateway] [-f] [-V] [--nochk] interface
routedel [-p {v4|v6}] --all [-f] [-V]
```

Synopsis (to reference the command syntax)
```
routedel -h
```

Description

Deletes routing information set for the interface. However, routing information acquired from the DHCP server cannot be deleted.

In a cluster configuration, processing for this command is executed for both nodes of the cluster.

Deleting routing information disables communication between the HDI system and the client that was using the deleted routing information.

Note that you may not be able to log in to File Services Manager if you delete the routing information for the management port. In this case, log in to File Services Manager from another machine on the same network as the HDI system, and set the required routing information again.

If the name of a host that you set as a routing target or gateway cannot be resolved, you might not be able to delete routing information correctly. If you have specified a host name as a routing target or gateway, before you delete routing information, confirm that the name of the host can be resolved.

Options and arguments

`--all`

Specify this to delete all routing information set in the cluster, except that set for the management port.

`-d` *target*

Specify the routing target to be deleted.

network-address

If you have set a network as a routing target, specify the target network address.

host

If you have set a host as a routing target, specify the target host name or IP address.

`default`

Specify this to delete the default route.

`-f`

Specify this to prevent the confirmation message from appearing.

`-g` *gateway*

Specify the host name or IP address of the gateway of the routing information you are deleting.

If a gateway is specified, this option must be specified.

`-n` *netmask*

If a network is set as the routing target in IPv4, specify the netmask of the network.

If a network is set as the routing target in IPv6, specify the prefix length of the network.

`--nochk`

    Specify this if you also want to delete routing information not associated with any interface.

    Note:

        Specify this option only when you perform the procedure for checking the routing described in the *Troubleshooting Guide*.

`-p {v4|v6}`

    Specify the protocol version of the routing information to be deleted. If you omit this option, the protocol version determined from the specified IP address is set. If a protocol version cannot be determined, `v4` is set.

    `v4`

        Specify this to use IPv4 IP addresses.

    `v6`

        Specify this to use IPv6 IP addresses.

`-S` *virtual-server-name*

    This option is not supported.

`-V`

    Specify this to display the progress of the deletion processing. This option is ignored if the `-S` option is specified.

interface

    Specify the interface whose routing information will be deleted.

    If a tagged VLAN is used, specify it in the following format:

    port-name.VLAN-ID

Return values

Table 2-345 Return values of the routedel command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
3, 10, 66[#], 67, 70, 72	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
97, 98, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Examples

To delete routing information for the data port interface `eth12` under the following conditions:

- The routing target is `172.16.3.0`.
- The netmask is `255.255.255.0`.
- The gateway address is `172.16.2.1`.

```
$ sudo routedel -d 172.16.3.0 -n 255.255.255.0 -g 172.16.2.1 eth12
KAQM05099-Q Do you want to delete the specified routing information? (y/n)
```

To use IPv6 IP addresses to delete routing information for the data port (`eth12`):

- The routing target is `2001:2c0:418:10::0`.
- The gateway is `fd00::4`.

```
$ sudo routedel -p v6 -d [2001:2c0:418:10::0] -g [fd00::4] eth12
KAQM05099-Q Do you want to delete the specified routing information? (y/n)
```

routefilterctl (Set reverse path filtering)

Synopsis

```
routefilterctl [--on|--off]
routefilterctl -h
```

Description

Views or changes the setting for reverse path filtering. To use this command, log in by specifying the management port IP address from a computer on the management LAN.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Note:

If you disable the reverse path filtering function, before using Hitachi File Services Manager, check the routing target to ensure that the same port is used for communication between the management server and node.

Options and arguments

`--off`

    Specify this to disable the reverse path filtering function.

`--on`

    Specify this to enable the reverse path filtering function. The initial setting is `--on`.

If you omit all options, the current setting is displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-346 Information displayed when executing the routefilterctl command

Item	Description

Status	Displays whether the reverse path filtering function is enabled.
	
	`On`
	
	    The reverse path filtering function is enabled.
	
	`Off`
	
	    The reverse path filtering function is disabled.

Return values

Table 2-347 Return values of the routefilterctl command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`65`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`70, 71`[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`71`[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
`97, 98, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Example

To disable the reverse path filtering function:

```
$ sudo routefilterctl --off
```

routelist (List routing information)

Synopsis (for cluster configurations)

```
routelist [-p {v4|v6}] [-l] [{-c|--del delimiter}]
    [-S virtual-server-name]
```

Synopsis (for single-node configurations)

```
routelist [-p {v4|v6}] [-l] [{-c|--del delimiter}]
```

Synopsis (to reference the command syntax)

```
routelist -h
```

Description

Displays the routing information currently set for the interface.

Options and arguments

`-c`

Specify this to display routing information separated with colons (:).

`--del` *delimiter*

Specify this to display the information separated with an alphanumeric character, symbol, or space, whichever is specified.

`-l`

Specify this to display all the routing information for the interfaces used in the HDI system.

Note that the information to be displayed is not sorted by interface port name.

When you specify this option, information is displayed not only for the routing set by the system administrator, but also for the routing set by

the system automatically. When this option is omitted, only information on the routing set by the system administrator is displayed.

Note:

Specify this option only when you perform the procedure for checking the routing described in the *Troubleshooting Guide* or when you check the routing information set by the system automatically.

Also, do not change the routing information set by the system automatically.

`-p {v4|v6}`

Specify the protocol version of the routing information to be displayed. If you omit this option, both IPv4 and IPv6 routing information is displayed.

`v4`

Specify this to display only IPv4 routing information.

`v6`

Specify this to display only IPv6 routing information.

`-S` *virtual-server-name*

This option is not supported.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-348 Information displayed when executing the routelist command

Item	Description
Target	For IPv4, the routing target appears as a network name, host name, or IP address.
	If the default route is set as the routing target, default appears in this item.
	For IPv6, the routing target appears in the following format: *routing-target/prefix-length*
	If the default route is set and the -l option is specified, ::/0 appears in this item.
	If the default route is set and the -l option is not specified, default appears in this item.
Netmask #	Displays the netmask when a network is set as the routing target.
	If the default route is set as the routing target, 0.0.0.0 appears in this item.
	If a host is set and the -l option is specified, 255.255.255.255 appears in this item.
	If a host is set and the -l option is not specified, - appears in this item.
Gateway	Displays the host name or IP address of the gateway.

Item	Description
	If no gateway is set and the `-l` option is specified, `0.0.0.0` or `::` appears in this item.
	If no gateway is set and the `-l` option is not specified, `*` appears in this item.
	If a reject route is set and the `-l` option is specified, `0.0.0.0` or `::` appears in this item.
	If a reject route is set and the `-l` option is not specified, `-` appears in this item.

Method	Displays the routing method used for the route.
	`Allow`
	　　The route is set as a normal route.
	`Reject`
	　　The route is set to be rejected.
	Nothing appears in this item when you specify the `-l` option.

Type	Displays the type of routing target set for the route.
	`net`
	　　The routing target is a network.
	`host`
	　　The routing target is a host.
	`default`
	　　The routing target is the default route.
	Nothing appears in this item when you specify the `-l` option.

Flags	Displays the routing status. This item is displayed when the `-l` option is specified.
	`A` [#]
	　　The route is set by the `addrconf` command.
	`C` [#]
	　　The route is entered in the routing cache.
	`D` [#]
	　　The route is set dynamically by a daemon or redirect.
	`G`
	　　A gateway is set for the route.
	`H`
	　　The routing target is set to a host.
	`M` [#]
	　　The route is set dynamically by a routing daemon or redirect.
	`n`
	　　No router is found on the path to the routing target.
	`R` [#]
	　　The route is set to be reinstated dynamically.
	`U`
	　　The route is a normal route.

Item	Description
	`!` The route is a reject route.
`MSS`[#]	Displays the maximum segment size for TCP connections over the route. If no value has been specified for the `routeadd` command, a hyphen (`-`) is displayed. In this case, the result of subtracting 40 from the MTU value set for the interface is set as the maximum segment size.
`Iface`	Displays information about the interface. If routing information is set by using the DHCP server, `(DHCP)` is displayed after the interface name. If a tagged VLAN is used, it is displayed in the following format: `port-name.VLAN-ID`

Note:

    The items for which information is set are displayed in the following order:

- Routing information items set for IPv4
- Routing information items set for IPv6

\#

    This item is not displayed in IPv6.

Return values

Table 2-349 Return values of the routelist command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10, 67, 72`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`97, 98, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To view the routing information:

```
$ sudo routelist
[IPv4]
Target           Netmask         Gateway          Method Type      MSS    Iface
172.16.3.0       255.255.255.0   172.16.3.1       Allow  net       -      eth12
10.200.100.100   -               10.200.100.1     Allow  host      -
eth13.0002
10.20.30.50      -               -                Reject host      -      eth14
default          0.0.0.0         192.168.3.1      Allow  default   -      mng0

[IPv6]
Target                   Gateway              Method Type    Iface
default                  fd00::1              Allow  default eth12
fd00:2::10/64            fd00:2::             Allow  net     eth13.0002
fdf1:afcb:44f9:1000::3:130/128 fdf1:afcb:44f9:1000::3:132 Allow  host
mng0
```

secureshellctl (Enable the security enhancement)

Synopsis

```
secureshellctl [-y] [--enable]
secureshellctl -h
```

Description

Enable the security enhancement. The command can also be used to view the current setting.

Security enhancement is disabled initially when the HDI system is upgraded from a version other than 5.4.1-*xx* or 6.1.1-*xx* (regardless of the number of *x*).(x represents any number).

If you want to enable security enhancement, note the following points:

- If you enable security enhancement, you will not be able to disable it.
- The following operations, which are not supported by the HDI system, are restricted:
  - Executing LINUX commands
  - Executing scripts in the HDI system
  - Redirecting command output to a file

Note that changes to the settings are applied the next time you log in.

In a cluster configuration, processing for this command is executed for both nodes of the cluster.

Options and arguments

```
--enable
```
   Specify this if you want to enable the security enhancement.

Command Reference

If you omit all options, the current setting is displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-350 Information displayed when executing the secureshellctl command

Item	Description

`Enabled` or `Disabled`	Displays whether the security enhancement is enabled.
	`Enabled`
	    Displayed if the security enhancement is enabled.
	`Disabled`
	    Displayed if the security enhancement is disabled.

Return values

Table 2-351 Return values of the secureshellctl command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`66`, `70`, `71`[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`71`[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
    The command ended abnormally due to multiple causes.

sshkeyadd (Register a public key)

Synopsis

```
sshkeyadd [-2] -c comment public-key
sshkeyadd -h
```

Description

Registers a public key for an SSH account.

Register the public key on both nodes so that the settings are the same in the cluster.

When registration completes successfully, the specified public key file is deleted from the home directory for the SSH account.

Options and arguments

-2

Specify this to use SSH protocol version 2 (default).

-c *comment*

Specify a comment for a public key by using a maximum of 32 characters. Note that comments should not be duplicated within the same protocol. Any comment string must be written in alphanumeric characters and hyphens (-). You can also specify spaces, but not at the beginning or end of the character string.

public-key

Specify the name of the public key file to be registered. The public key must be in OpenSSH format. To register a public key file, the file name must satisfy the following conditions:

- The maximum number of characters that can be used for the name of the public key file is 256.

- The characters that can be used for the name of the public key file are alphanumeric characters, exclamation marks (!), hash marks (#), percent signs (%), ampersands (&), left parentheses ((), right parentheses ()), plus signs (+), commas (,), hyphens (-), periods (.), semicolons (;), equal signs (=), at marks (@), left square brackets ([), right square brackets (]), carets (^), underscores (_), left curly brackets ({), right curly brackets (}), and tildes (~). You can also specify spaces, but not at the beginning or end of the character string.

- The following names cannot be used for the public key file name:

  - A name consisting of only the character 0

  - A name starting with the character -

  - A name already used for a directory or file that exists in the home directory for the SSH account (/home/nasroot)

Return values

Table 2-352 Return values of the sshkeyadd command

Return value	Description
0	Normal termination

2-588

Return value	Description
1, 3, 4, 5, 6, 7, 8, 9	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 11, 17, 23, 66, 68[#], 71, 95	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Example

To register the file `ssh-key-nasroot.pub` with a `ssh key` comment:

```
$ sudo sshkeyadd -2 -c "ssh key" ssh-key-nasroot.pub
```

sshkeydel (Delete a public key)

Synopsis

```
sshkeydel [-2] -c comment
sshkeydel -h
```

Description

Deletes a public key.

Delete the target public key from both nodes to have the same settings in the cluster.

If you (the system administrator) execute this command to delete the public key that you are currently using, you will not be able to log in with that key again. If you mistakenly delete all public keys, register a public key again via the GUI.

Options and arguments

-2

Specify this to delete a public key for use in SSH protocol version 2 (default).

-c *comment*

Specify a comment for the public key file.

Return values

Table 2-353 Return values of the sshkeydel command

Return value	Description
0	Normal termination
1, 3, 4, 6	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
12, 15, 67, 68[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Example

To delete a public key, which was registered with a `nasroot-key` comment:

```
$ sudo sshkeydel -c nasroot-key
```

sshkeylist (List public key information)

Synopsis

```
sshkeylist [-h]
```

Description

Lists information about registered public keys.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-354 Information displayed when executing the sshkeylist command

Item	Description
User	Displayed `nasroot`.
Ver.	Displays the SSH protocol version for the public key. `SSH2` The SSH protocol is version 2.
Comment	Displays the comment set for the public key.

Return values

Table 2-355 Return values of the sshkeylist command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
15, 68[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

stquota (Display the quota information set for each directory)

Synopsis

```
stquota [-c] [-l] [-w]
    file-system-name[/directory-name[/directory-name...]]
```

```
stquota [-c] [-l] [-u] [-w]
    file-system-name[/directory-name[/directory-name...]] user...
stquota [-c] -g [-l] [-w]
    file-system-name[/directory-name[/directory-name...]] group...
stquota -d [-c] [-l]
    file-system-name[/directory-name[/directory-name...]]
stquota -t [-c] [-l] [-u|-g]
    file-system-name[/directory-name[/directory-name...]]
stquota -m [-c] [-l]
    file-system-name[/directory-name[/directory-name...]]
stquota -h
```

Description

Displays the information and the current usage status of the quota set for each directory (subtree quota).

When a specific user or group is specified, the command displays the quota information set for the user or group for each directory.

Options and arguments

-c

Specify this to display quota information separated with colons (:).

When this option is specified, the name and ID are displayed for user or group information, the values for block usage are displayed in kilobytes, and the grace period is displayed in seconds.

In addition, the display differs depending on the setting of the monitoring method. For the set monitoring methods for each file system, `Filesystem:` is displayed at the beginning. For the set monitoring methods for each directory, `Directory:` is displayed at the beginning. Any monitoring methods that are not set are not displayed.

-d

Specify this option to view quota information for the directory where the default quota is set.

-g

Specify this option to view quota information for the directory where the group quota is set.

-l

Specify this option to view the directory names in ascending order.

-m

Specify this to view the quota monitoring method.

-t

Specify this option to view the grace period after the soft limit is exceeded.

-u

Specify this option to view quota information for the directory where the user quota is set.

-w

Specify this to display the quota information for the directories, users, or groups that have exceeded their soft limit.

file-system-name[/*directory-name*[/*directory-name*...]]

Specify the file system name and directory names in no more than 4,000 bytes. For example, specify `FS1/dir01` for the `/mnt/FS1/dir01` directory.

user ...

When you want to display the quota information for one or more specific users, specify their names or IDs.

You can specify any of the following users by the user name. Note that the built-in user of a Windows domain cannot be specified.

- ○ Users registered by File Services Manager (user IDs: 97 and 200 to 2147483147)
- ○ Users registered in the NIS server or LDAP server for user authentication (other than users whose user ID is 0)
- ○ Users registered by user mapping
- ○ Users authenticated by Active Directory

To specify users that were authenticated by Active Directory, specify the domain name and user name in the following format:

"*domain-name**user-name*" or *domain-name**user-name*

When you specify a user ID, specify a valid value from 1 to 2147483147.

When specifying multiple user names or user IDs, separate them with space. User names and user IDs can coexist.

group ...

When you want to display the quota information for one or more specific groups, specify their names or IDs.

You can specify any of the following groups by the group name. Note that the built-in group of a Windows domain cannot be specified.

- ○ Groups registered by File Services Manager (group IDs: 97 and 200 to 2147483147)
- ○ Groups registered in the NIS server or LDAP server for user authentication (other than groups whose group ID is 0)
- ○ Groups registered by user mapping
- ○ Groups authenticated by Active Directory

To specify groups that were authenticated by Active Directory, specify the domain name and group name in the following format:

"*domain-name**group-name*" or *domain-name**group-name*

When you specify a group ID, specify a valid value from 1 to 2147483147.

When specifying multiple group names or group IDs, separate them with space. Group names and group IDs can coexist.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-356 Information displayed when executing the stquota command (quota information of a directory, user, or group)

Item	Description
`Report for subtree quotas on file system` [#1]	The file system name is displayed. This item is displayed when the `-g` or `-u` option are not specified.
`Report for subtree group quotas on file system` [#1]	The file system name is displayed. This item is displayed when the `-g` option is specified.
`Report for subtree user quotas on file system` [#1]	The file system name is displayed. This item is displayed when the `-u` option is specified.
`Report for subtree quotas on directory` [#2]	The directory name is displayed. This item is displayed when the `-g` or `-u` option are not specified.
`Report for subtree group quotas on directory` [#2]	The directory name is displayed. This item is displayed when the `-g` option is specified.
`Report for subtree user quotas on directory` [#2]	The directory name is displayed. This item is displayed when the `-u` option is specified.
`User` or `Group`[#3]	The user or group names are displayed. When user or group IDs are displayed instead of names, a hash mark (`#`) is prefixed to the IDs.
`Directory`	The names of directories for which quotas have been set are displayed. If subtree quotas have been set for the directories, a period (`.`) is displayed instead of the name of such directories. The directory names are followed by two symbols, each of which can be a plus sign (`+`) or a minus sign (`-`). The first symbol indicates block usage and the second symbol indicates inode usage. Plus sign (`+`) The block usage or inode usage has exceeded the soft limit or has reached the hard limit. Minus sign (`-`) The block usage or inode usage has neither exceeded the soft limit nor reached the hard limit.
`Block limits`	Block usage is displayed. `Used`

Item	Description
	Block space used. The display unit for this value is bytes. The binary prefix for the unit, such as `K` (for KB), `M` (for MB), `G` (for GB), `T` (for TB), or `P` (for PB), is appended after the displayed value. The displayed value is rounded up to two decimal places.
	`Soft`
	Soft limit for block usage. The display unit for this value is bytes. The binary prefix for the unit, such as `K` (for KB), `M` (for MB), `G` (for GB), `T` (for TB), or `P` (for PB), is appended after the displayed value. The displayed value is rounded to two decimal places.
	`Hard`
	Hard limit for block usage. The display unit for this value is bytes. The binary prefix for the unit, such as `K` (for KB), `M` (for MB), `G` (for GB), `T` (for TB), or `P` (for PB), is appended after the displayed value. The displayed value is rounded to two decimal places.
	`Grace`
	Remaining grace time until a new block can no longer be assigned after the block usage exceeds the soft limit. Displayed in one of the following formats:
	n `days`
	The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.
	hh : *mm*
	The remaining grace time is less than 24 hours. For example, `10:00` appears if there are ten hours remaining.
	`over`
	Either the grace period has expired or block usage has reached the hard limit.
	If the target file system is of the Advanced ACL type and the user name is `__groupowner` (user ID: 4294967292), `0` is displayed for both `Soft` and `Hard`.
`i-node limits`	inode usage is displayed.
	`Used`
	Number of inodes used.
	`Soft`
	Soft limit for inode usage.
	`Hard`
	Hard limit for inode usage.
	`Grace`
	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:
	n `days`

Item	Description
	The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.
	hh : *mm*
	The remaining grace time is less than 24 hours. For example, `10:00` appears if there are ten hours remaining.
	`over`
	Either the grace period has expired or inode usage has reached the hard limit.
	If the target file system is of the Advanced ACL type and the user name is `__groupowner` (user ID: 4294967292), `0` is displayed for both `Soft` and `Hard`.

Note:

   If a directory name has 10 or more characters, the symbols that indicate whether limits have been exceeded, the block usage value, and the inode usage value are displayed on the next line.

#1:

   Displayed for the file system quota information.

#2:

   Displayed for the directory quota information.

#3:

   For the directory quota information, this item will not appear.

Table 2-357 Information displayed when executing the stquota command (the default quota)

Item	Description
`Report for subtree user quotas on file system`	The file system name is displayed.
`Report for subtree user quotas on directory`	The directory name is displayed.
`Directory`	The names of directories for which quotas have been set are displayed.
`Default block limits`	The soft and hard limits for block usage that are set as default quotas are displayed.
	`Soft`
	Soft limit for block usage. The display unit for this value is bytes. The binary prefix for the unit, such as `K` (for KB), `M` (for MB), `G` (for GB), `T` (for TB), or `P` (for PB), is appended after the displayed value. The displayed value is rounded to two decimal places.
	`Hard`

Item	Description
	Hard limit for block usage. The display unit for this value is bytes. The binary prefix for the unit, such as `K` (for KB), `M` (for MB), `G` (for GB), `T` (for TB), or `P` (for PB), is appended after the displayed value. The displayed value is rounded to two decimal places.

`Default i-node limits`	The soft and hard limits values for inode usage that are set as default quotas are displayed.
	
	`Soft`
	
	    Soft limit for inode usage.
	
	`Hard`
	
	    Hard limit for inode usage.

Table 2-358 Information displayed when executing the stquota command (the grace period)

Item	Description
`Report for subtree quotas on file system`	The file system name is displayed. This item is displayed when the `-g` or `-u` option are not specified.
`Report for subtree group quotas on file system`	The file system name is displayed. This item is displayed when the `-g` option is specified.
`Report for subtree user quotas on file system`	The file system name is displayed. This item is displayed when the `-u` option is specified.
`Report for subtree quotas on directory`	The directory name is displayed. This item is displayed when the `-g` or `-u` option are not specified.
`Report for subtree group quotas on directory`	The directory name is displayed. This item is displayed when the `-g` option is specified.
`Report for subtree user quotas on directory`	The directory name is displayed. This item is displayed when the `-u` option is specified.
`Directory`	The names of directories for which quotas have been set are displayed.
`Block grace time`	Displays the grace period until a new block can no longer be assigned after the block usage exceeds the soft limit.
`i-node grace time`	Displays the grace period until files can no longer be created after inode usage exceeds the soft limit.

Table 2-359 Information displayed when executing the stquota command (the monitoring method)

Item	Description
`Report for the monitoring start time on file system`	The file system name is displayed.

Item	Description
Report for the monitoring start time on directory	The directory name is displayed.
Settings for the directory	The names of directories for which quotas have been set are displayed.

SNMP notification mode	Displays the SNMP trap notification mode when the quota set for the directory is exceeded.
	
	`Use a summary notification`
	
	    Summary notification mode is set.
	
	`Use individual notifications`
	
	    Individual notification mode is set.

SNMP notification time	Displays the set monitoring time for the directory. If you specified the `-c` option, the monitoring times are displayed without a colon (:) between the hour and minute. If several times are set, those times are displayed, separated by a comma (,).

Return values

Table 2-360 Return values of the stquota command

Return value	Description
0	Normal termination
10#, 99#	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
10#, 99#	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99#	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

stquotalist (List the quota information set for users or groups for each directory)

Synopsis

```
stquotalist [-c] [-u|-g] [-n] [-w]
    file-system-name/directory-name[/directory-name...]
stquotalist -m [-c]
    file-system-name/directory-name[/directory-name...]
stquotalist -h
```

Description

Displays the information and current usage status of the quota (subtree quota) set for users or groups in the specified directory.

Options and arguments

-c

Specify this to display quota information separated with colons (:).

When this option is specified, the name and ID are displayed for user or group information, the values for block usage are displayed in kilobytes, and the grace period is displayed in seconds.

In addition, the display differs depending on the setting of the monitoring method. For the set monitoring methods for each file system, `Filesystem`: is displayed at the beginning. For the set monitoring methods for each directory, `Directory`: is displayed at the beginning. Any monitoring methods that are not set are not displayed.

-g

Specify this option to display the group quota information.

-m

Specify this option to view the monitoring method set for users or groups.

-n

Specify this option to not display the quota information for user IDs or group IDs that cannot be converted to user names or group names.

-u

Specify this option to display the user quota information.

-w

Specify this to display the quota information for the users or groups that have exceeded their soft limit.

file-system-name/*directory-name*[/*directory-name*...]

Specify the file system name and directory names in no more than 4,000 bytes. For example, specify `FS1/dir01` for the `/mnt/FS1/dir01` directory.

To specify the `-g` or `-u` option, specify a directory in which a quota is set.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-361 Information displayed when executing the stquotalist command (quota information of a user or group)

Item	Description
`Report for subtree group quotas on directory`	The name of the file system or directory as specified by the `-w` option is displayed. This item is displayed when the `-g` option is specified.
`Report for subtree user quotas on directory`	The name of the file system or directory as specified by the `-w` option is displayed. This item is displayed when the `-u` option is specified.

`User` or `Group`	The user or group names are displayed.
	
	When user or group IDs are displayed instead of names, a hash mark (`#`) is prefixed to the IDs.
	
	Each user or group name is followed by two symbols, each of which can be a plus sign (`+`) or a minus sign (`-`). The first symbol indicates block usage and the second symbol indicates inode usage.
	
	Plus sign (`+`)
	
	    The block usage or inode usage has exceeded the soft limit or has reached the hard limit.
	
	Minus sign (`-`)
	
	    The block usage or inode usage has neither exceeded the soft limit nor reached the hard limit.

`Block limits`	Block usage is displayed.
	
	`Used`
	
	    Block space used. The display unit for this value is bytes. The binary prefix for the unit, such as `K` (for KB), `M` (for MB), `G` (for GB), `T` (for TB), or `P` (for PB), is appended after the displayed value. The displayed value is rounded up to two decimal places.
	
	`Soft`
	
	    Soft limit for block usage. The display unit for this value is bytes. The binary prefix for the unit, such as `K` (for KB), `M` (for MB), `G` (for GB), `T` (for TB), or `P` (for PB), is appended after the displayed value. The displayed value is rounded to two decimal places.
	
	`Hard`
	
	    Hard limit for block usage. The display unit for this value is bytes. The binary prefix for the unit, such as `K` (for KB), `M` (for MB), `G` (for GB), `T` (for TB), or `P` (for PB), is appended after the displayed value. The displayed value is rounded to two decimal places.
	
	`Grace`

Item	Description
	Remaining grace time until a new block can no longer be assigned after the block usage exceeds the soft limit. Displayed in one of the following formats:
	n days
	The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.
	hh : *mm*
	The remaining grace time is less than 24 hours. For example, `10:00` appears if there are ten hours remaining.
	`over`
	Either the grace period has expired or block usage has reached the hard limit.
	If the target file system is of the Advanced ACL type and the user name is `__groupowner` (user ID: 4294967292), `0` is displayed for both `Soft` and `Hard`.
`i-node limits`	inode usage is displayed.
	`Used`
	Number of inodes used.
	`Soft`
	Soft limit for inode usage.
	`Hard`
	Hard limit for inode usage.
	`Grace`
	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:
	n days
	The remaining grace time is 24 hours or longer. For example, `1 days` appears if there are 24 hours or more, but less than 48 hours remaining.
	hh : *mm*
	The remaining grace time is less than 24 hours. For example, `10:00` appears if there are ten hours remaining.
	`over`
	Either the grace period has expired or inode usage has reached the hard limit.
	If the target file system is of the Advanced ACL type and the user name is `__groupowner` (user ID: 4294967292), `0` is displayed for both `Soft` and `Hard`.

Note:

> If a user or group name has 10 or more characters, the symbols that indicate whether limits have been exceeded, the block usage value, and the inode usage value are displayed on the next line.

Table 2-362 Information displayed when executing the stquotalist command (the monitoring method)

Item	Description
`Report for the monitoring start time on file system`	The file system name is displayed.
`Setting to the directory`	The names of directories for which quotas have been set are displayed.
`SNMP notification mode`	Displays the SNMP trap notification mode when the quota set for users or groups is exceeded. `Use a summary notification` Summary notification mode is set.
`SNMP notification time`	Displays the set monitoring time for users or groups. If you specified the `-c` option, the monitoring times are displayed without a colon (`:`) between the hour and minute. If several times are set, those times are displayed, separated by a comma (`,`).

Return values

Table 2-363 Return values of the stquotalist command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10`[#]`, 99`[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`10`[#]`, 99`[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`99`[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

    The command ended abnormally due to multiple causes.

stquotaset (Set quotas for each directory)

Synopsis

```
stquotaset limit-options
    file-system-name/directory-name[/directory-name...]
stquotaset [-u] limit-options
    file-system-name/directory-name[/directory-name...] user...
stquotaset -g limit-options
    file-system-name/directory-name[/directory-name...] group...
stquotaset -d limit-options
    file-system-name/directory-name[/directory-name...]
stquotaset -t [-u|-g] grace-period-options
    file-system-name/directory-name[/directory-name...]
stquotaset -t [-u|-g] grace-period
    file-system-name/directory-name[/directory-name...]
stquotaset {-x|-r [-p]} [-q]
    file-system-name/directory-name[/directory-name...]
stquotaset -m -s monitoring-time[,monitoring-time...]
    [-n {summary|individual}] file-system-name
stquotaset -m [-s monitoring-time[,monitoring-time...]]
    -n {summary|individual} file-system-name
stquotaset -m -s monitoring-time[,monitoring-time...] [-n individual]
    file-system-name/directory-name[/directory-name...]
stquotaset -m -u -s monitoring-time[,monitoring-time...]
    [-n summary] file-system-name[/directory-name[/directory-name...]]
stquotaset -m [-u] -s default file-system-name[/directory-name]
stquotaset -h
```

limit-options:

```
-b block-soft-limit
-B block-hard-limit
-i inode-soft-limit
-I inode-hard-limit
```

grace-period-options:

```
-b block-grace-period
-i inode-grace-period
```

Description

Sets quotas (subtree quotas) for each directory.

The soft limit, hard limit, and grace period can be set for each directory, user, or group.

The command operates differently depending on whether the -u or -g option is specified, as described below.

When the -u option is specified

The command sets the soft limit, hard limit, or grace period for users.

When the -g option is specified

The command sets the soft limit, hard limit, or grace period for groups.

When neither the `-u` option nor the `-g` option is specified

The command sets the soft limit, hard limit, or grace period for directories.

The subtree quota monitoring method can be set for each file system or directory. If you set the monitoring method for a file system, all directories immediately under the mount point for which subtree quota is set are monitored.

If you set quotas for a directory, the usage status of all directories under that directory is monitored. You can set quotas for a maximum of three locations (directories) on the same path in the directory tree. Even if you set multiple quotas in the upper or lower directories, the integrity of the specified values will not be checked.

Note:

In directories where namespace quota is set, this command cannot be used to set quotas for individual directories.

Options and arguments

`-d`

Specify this option to set the default quota for the specified directory.

`-g`

Specify this option to set a quota for the specified group.

`-m`

Specify this to set or clear the quota monitoring method. When you specify this option with the `-u` option, the quota monitoring method for the specified user or group is set or cleared.

If this command accepts a signal when you set the monitoring method, the signal is blocked.

`-n individual`

Specify this to output an SNMP trap in the individual notification mode when File Services Manager detects a directory that has exceeded its soft limit or grace period. You can also specify `i` instead of `individual`. You can specify this option when you specify the quota monitoring time for a directory.

If more than 100 directories exceeded their soft limit or grace period, individual notifications are suppressed and only the number of directories that have exceeded their soft limits or grace period are reported to the SNMP manager.

The initial setting disables the SNMP trap notification. If you omit this option in the state where the monitoring time is not set, the summary notification mode is set when a quota is set for each file system and the individual notification mode is set when a quota is set for each directory. Also, if you omit this option with one or more monitoring times set, the current setting information applies.

`-n summary`

Specify this option to output an SNMP trap in the summary notification mode when File Services Manager detects directories, users or groups that exceeded their soft limit or grace period. You can also specify `s` instead of `summary`.

You can specify this option when:

○ The quota monitoring time for users or groups is set.

○ The quota monitoring time for directories is set by the file system.

The initial setting disables the SNMP trap notification. If you omit this option with no monitoring times set, the summary notification mode is applied. Also, if you omit this option with one or more monitoring times set, the current setting information applies.

`-p`

Specify this option to apply command processing to all the directories in the specified directory. This option is enabled only when the `-r` option is specified.

`-q`

Specify this option if you do not want to display the processing progress. This option is enabled only when the `-r` or `-x` option is specified.

`-r`

Specify this option to remove the quotas set for the specified directory.

If you specify this option with the `-p` option, the quotas set for all the directories in the specified directory are removed.

The processing time varies depending on the number of directories and files residing under the specified directory. If you execute the command with this option specified when the total number of directories and files is 100,000, it takes about 30 seconds to complete the processing. At this time, the command first displays the directory path and the string `Wait...`, and then displays one period (.) every time the command removes quotas for 10,000 files.

If the command executed with this option specified stops, the specified directory might contain files that have different quota information. Re-execute the command with the same specification when the command executed with this option specified has stopped.

If the system administrator executes the `stquotaset` command with the `-r` option specified while clients are performing operations such as creating or deleting files, the quotas might not be removed correctly. Make sure that no client is performing operations, and then remove the quotas.

`-s`

Specify this option to set or clear monitoring times for File Services Manager to monitor quotas.

The initial setting is no quota monitoring. If you omit this option, the current setting information applies.

monitoring-time [, *monitoring-time* ...]

Specify the times at which File Services Manager monitors quotas. All previously set monitoring times are cleared, and then the specified times are set.

Specify a value from 00 hours 00 minutes to 23 hours 55 minutes (format: *hhmm*) in units of 5 minutes. If specifying a value by using a colon (`:`) as a delimiter, you can omit 0 at the uppermost digit of hours and minutes of the monitoring time. For example, to specify 01 hour 05 minutes as a monitoring time, write `01:05`, `01:5`, `1:05`, `1:5`, or `0105`.

Separate multiple monitoring times with commas. You can specify a maximum of 48 monitoring times for each file system or directory.

`default`

Specify this option to clear all monitoring times and set quota monitoring to the initial state (no monitoring).

`-t`

Specify this option to set the grace period until a new block can no longer be assigned or files can no longer be created after the block usage or inode usage exceeds the soft limit.

`-u`

Specify this option to set a quota for the specified user.

When you specify this option with the `-m` option, the quota monitoring method is set or cleared for the specified user or group.

`-x`

Specify this option to apply a quota for the existing directories.

When this option is specified, the block space and the number of inodes used by the directories and files under the target directory will be counted as the quota usage.

The command execution time varies depending on the total number of directories and files under the specified directory. If you execute the command when the total number of directories and files is 100,000, it takes about 30 seconds to complete the processing. At this time, the command first displays the directory path and the string `Wait...`, and then displays one period (`.`) every time the command processes 10,000 files.

If the command executed with this option specified stops, the specified directory might contain files that have different quota information. Re-execute the command with the same specification when the command executed with this option specified has stopped.

If a client is performing an operation such as creating or deleting a file, if the system administrator executes the `stquotaset` command with the `-x` option specified, the quota usage will be recalculated after the operation finishes. For this reason, if the client frequently performs such operations, the `stquotaset` command might take more time to finish. Make sure that no client is performing operations, and then apply a quota for the existing directories.

limit-options

Specify these options if you want to set the soft and hard limits for the specified directory, user, or group. You can specify a combination of the option shown below. If you set a subtree quota for existing directories, after setting the soft or hard limits, execute the `stquotaset` command with the `-x` option specified to apply the quota.

`-b` *block-soft-limit*

Specify the soft limit for block usage and the unit. If you specify a value in MB, you can specify a value from `0` to `1073741823`. If you specify a value in GB, you can specify a value from `0` to `1048575`. If you specify a value in TB, you can specify a value from `0` to `1023`. If you do not want to set a soft limit for block usage, specify `0` or only the unit. Make sure that you specify a value that is not greater than the hard limit. After the value, add a letter that indicates the unit (`M`: MB; `G`: GB; or `T`: TB). If a unit is not specified, MB is assumed.

The initial value is `0` (no soft limit). If you omit this option, the current setting information applies.

`-B` *block-hard-limit*

Specify the hard limit for block usage and the unit. If you specify a value in MB, you can specify a value from `0` to `1073741823`. If you specify a value in GB, you can specify a value from `0` to `1048575`. If you specify a value in TB, you can specify a value from `0` to `1023`. If you do not want to set a hard limit for block usage, specify `0` or only the unit. After the value, add a letter that indicates the unit (`M`: MB; `G`: GB; or `T`: TB). If a unit is not specified, MB is assumed.

The initial value is `0` (no hard limit). If you omit this option, the current setting information applies.

`-i` *inode-soft-limit*

Specify the soft limit for inode usage. You can specify a value from `0` to `4294967295`. Make sure that you specify a value that is not greater than the hard limit.

The initial value is `0` (no soft limit). If you omit this option, the current setting information applies.

`-I` *inode-hard-limit*

Specify the hard limit for inode usage. You can specify a value from `0` to `4294967295`.

The initial value is `0` (no hard limit). If you omit this option, the current setting information applies.

grace-period-options

Specify these options to set grace periods. You can specify either or both of the following options:

`-b` *block-grace-period*

Specify the grace period (units: days) until a new block can no longer be assigned after the block usage exceeds the soft limit. Specify a value from 1 to 9,999.

The latest end time for a grace period is `2038/1/19 03:14:07`. Therefore, if the value `9,999` is set for this option and the date and time when the amount of block usage exceeds the soft limit is `2038/1/19 00:00:00`, the remaining grace period at that point will be 3 hours 14 minutes and 7 seconds.

The initial setting is 7 days. If you omit this option, the current setting information applies.

`-i` *inode-grace-period*

Specify the grace period (units: days) until files can no longer be created after inode usage exceeds the soft limit. Specify a value from 1 to 9,999.

The latest end time for a grace period is `2038/1/19 03:14:07`. Therefore, if the value `9,999` is set for this option and the date and time when the amount of block usage exceeds the soft limit is `2038/1/19 00:00:00`, the remaining grace period at that point will be 3 hours 14 minutes and 7 seconds.

The initial setting is 7 days. If you omit this option, the current setting information applies.

file-system-name`[/`*directory-name*`[/`*directory-name*`...]]`

Specify the file system name and directory names in no more than 4,000 bytes. For example, specify `FS1/dir01` for the `/mnt/FS1/dir01` directory.

user `...`

Specify the user name or user ID when you set a quota for a user.

You can specify any of the following users by the user name. Note that the built-in user of a Windows domain cannot be specified.

- Users registered by File Services Manager (user IDs: 97 and 200 to 2147483147)
- Users registered in the NIS server or LDAP server for user authentication (other than users whose user ID is 0)
- Users registered by user mapping
- Users authenticated by Active Directory

To specify users that were authenticated by Active Directory, specify the domain name and user name in the following format:

"*domain-name**user-name*" or *domain-name**user-name*

When you specify a user ID, specify a valid value from 1 to 2147483147.

When specifying multiple user names or user IDs, separate them with space. User names and user IDs can coexist.

Even if the target file system is of the Advanced ACL type and `__groupowner` (user ID: 4294967292) is specified as the user name, no quota will be set.

group . . .

Specify the group name or group ID when you set a quota for a group.

You can specify any of the following groups by the group name. Note that the built-in group of a Windows domain cannot be specified.

- Groups registered by File Services Manager (group IDs: 97 and 200 to 2147483147)
- Groups registered in the NIS server or LDAP server for user authentication (other than groups whose group ID is 0)
- Groups registered by user mapping
- Groups authenticated by Active Directory

To specify groups that were authenticated by Active Directory, specify the domain name and group name in the following format:

"*domain-name**group-name*" or *domain-name**group-name*

When you specify a group ID, specify a valid value from 1 to 2147483147.

When specifying multiple group names or group IDs, separate them with space. Group names and group IDs can coexist.

grace-period

Specify the number of days for the grace period to be applied to both the block usage and inode usage. Specify a value from 1 to 9,999.

The initial setting is 7 days. If you omit this option, the current setting information applies.

Return values

Table 2-364 Return values of the stquotaset command

Return value	Description
0	Normal termination
1, 10[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
10[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Examples

To set a quota for the `/mnt/filesystem01/dir01` directory under the following conditions:

- ○ Set the soft limit of block usage to 10 GB and the hard limit to 12 GB.
- ○ Set the soft limit of inode usage to 30,000 and the hard limit to 35,000.

```
$ sudo stquotaset -b 10G -B 12g -i 30000 -I 35000 filesystem01/dir01
```

To set quotas for users for the `/mnt/filesystem01/dir01/dir02` directory under the following conditions:

- ○ The target users are `user1` and `user2`.
- ○ Set the soft limit of block usage to 800 MB and the hard limit to 1 GB.
- ○ Set the soft limit of inode usage to 3,000 and the hard limit to 3,500.

```
$ sudo stquotaset -u -b 800M -B 1g -i 3000 -I 3500 filesystem01/dir01/
dir02 user1 user2
```

To set the default quota for the `/mnt/filesystem01/dir01/dir02/dir03` directory under the following conditions:

- ○ Set the soft limit of block usage to 1 GB and the hard limit to 2 GB.
- ○ Set the soft limit of inode usage to 3,000 and the hard limit to 3,500.

```
$ sudo stquotaset -d -b 1g -B 2G -i 3000 -I 3500 filesystem01/dir01/dir02/
dir03
```

To set the quota grace periods for the `/mnt/filesystem01/dir01/dir02` directory under the following conditions:

- ○ Set the grace period for the directory.
- ○ Set the grace period for block usage to 10 days.
- ○ Set the grace period for inode usage to 3 weeks.

```
$ sudo stquotaset -t -b 10 -i 21 filesystem01/dir01/dir02
```

To set monitoring times 01:05 and 13:15 for the `/mnt/filesystem01/dir01/dir02` directory:

```
$ sudo stquotaset -m -s 0105,1315 -n individual filesystem01/dir01/dir02
```

To apply quotas for the existing `/mnt/filesystem01/dir01/dir02` directory (when there are 100,000 files):

```
$ sudo stquotaset -x filesystem01/dir01/dir02
filesystem01/dir01/dir02: Wait .............. Success
```

svctl (Control a service)

Synopsis
```
svctl [-y] -s {cifs|ftp|nfs|sftp|tftp} {--start|--stop|--restart}
svctl -h
```

Description

Starts, stops, or restarts the specified service.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

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.

To enable the TFTP service, you must first set a TFTP access directory by executing the `tftpset` command.

Options and arguments

`--restart`

    Specify this to restart the specified service.

`-s {cifs|ftp|nfs|sftp|tftp}`

    Specify the service to be controlled. For a CIFS service, if an attempt to restart the CIFS service fails when the configuration definition of the CIFS service has not been modified, the CIFS service stops.

`--start`

    Specify this to start the specified service.
    You can start a service when the operating status of the service is `Stopped`.

`--stop`

    Specify this to stop the specified service.
    You can stop a service when the operation status of the service is `Running`, `Down`, `Failover` or `Offline`.

`-y`

    Specify this to prevent the confirmation message from appearing.
    This option is enabled only when the `--stop` or `--restart` option is specified.

Return values

Table 2-365 Return values of the svctl command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
30, 31, 32, 33, 34, 35, 36, 37[#], 38, 39, 40, 41, 42, 43, 44, 46, 50, 51, 68[#], 70, 71, 72, 73, 74, 75[#], 76[#], 77[#], 78[#], 79, 94[#], 95	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
37[#], 65, 68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
68[#], 97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.
75[#], 76[#], 77[#], 78[#], 94[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.

\#
    The command ended abnormally due to multiple causes.

Example

To restart the CIFS service:

```
$ sudo svctl -s cifs --restart
KAQM16131-Q Are you sure you want to restart the specified service? (y/n)
```

svstartuplist (Display automatic startup settings for a service)

Synopsis

```
svstartuplist [-c] [-s {cifs|ftp|nfs|ssh|sftp|ssh|tftp}]
svstartuplist -h
```

Description

Displays whether each service on a node is automatically started when the OS is started or restarted.

Options and arguments

`-c`

Specify this to display the automatic startup setting for services, separated with a colon (:).

`-s {cifs|ftp|nfs|sftp|ssh|tftp}`

Specify this to view the automatic startup setting for the CIFS, FTP, NFS, SFTP, SSH or TFTP service.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-366 Information displayed when executing the svstartuplist command

Item	Description
Service name	Displays the service name.

Automatic startup	Displays whether the service on a node is automatically started when the OS is started or restarted.
	`On`
	　Displayed when the service is automatically started.
	`Off`
	　Displayed when the service is not automatically started.

Return values

Table 2-367 Return values of the svstartuplist command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
68[#], 70, 95	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If

Return value	Description
	this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

svstartupset (Switch the automatic startup settings for a service)

Synopsis

```
svstartupset -s {cifs|ftp|nfs|sftp|tftp} {--on|--off}
svstartupset -h
```

Description

Switches the setting for whether each service on a node is automatically started when the OS is started or restarted.

Execute this command for each node so that the settings will be the same within the cluster.

Before you attempt to enable automatic startup of the TFTP service, you must execute the `tftpset` command to set a TFTP access directory. Then you can start or restart the service.

Options and arguments

`--off`

Specify this to disable automatic startup of a service.

`--on`

Specify this to enable automatic startup of a service.

`-s {cifs|ftp|nfs|sftp|tftp}`

Specify the service for which the automatic startup setting is to be switched.

Return values

Table 2-368 Return values of the svstartupset command

Return value	Description
0	Normal termination

Return value	Description
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
36, 68[#], 70, 95	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Example

To enable automatic startup of the CIFS service:

```
$ sudo svstartupset -s cifs --on
KAQM16189-I An automatic start setting for a service on this node was
changed. Confirm that the setting is consistent in the cluster.
```

svstatus (Display the operating status of a service)

Synopsis
```
svstatus [-c] [-s {cifs|ftp|nfs|ssh|sftp|ssh|tftp}]
svstatus -h
```

Description

Displays the operating status of the service on the node you are logged in to.

If you omit the -s option, the operating statuses of all services are displayed.

Options and arguments

-c

Specify this to display the operating statuses of the services, separated with a colon (:).

-s {cifs|ftp|nfs|sftp|ssh|tftp}

Specify this to view the operating status of the CIFS, FTP, NFS, SFTP, SSH or TFTP service.

`-s ssh`

Specify this to view the operating status of the SSH service.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-369 Information displayed when executing the svstatus command

Item	Description
Service name	Displays the service name.

Status	Displays the operating status of the service.
	
	`Running`
	
	    Displayed when the service is normally running.
	
	`Down`
	
	    Displayed when the service is running incompletely.
	
	`Failover`
	
	    Displayed when a failover has occurred for the resource group.
	
	`Offline`
	
	    Displayed when the status of the resource group is `Offline`.
	
	`Stopped`
	
	    Displayed when the service is stopped.

Information	Displays the information when the service needs to be restarted or started.
	
	`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.`
	
	    Displayed when the service has not been restarted after the NFS service configuration definition was modified. Make sure that the file system has been unmounted from the NFS client, and then restart the service. Restarting the OS on a node will not apply the changes of the configuration definition.
	
	`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.`
	
	    Displayed when the service remains stopped after the NFS service configuration definition was modified. Make sure that the file system has been unmounted from the NFS client, and then start the service. Restarting the OS on a node will not apply the changes of the configuration definition.
	
	`The configuration has been modified. Restart the service. Rebooting the OS will not apply the changes.`

Item	Description
	Displayed when the service has not been restarted after the NFS service, CIFS service, SFTP service, FTP service or TFTP service was reconfigured or the LDAP server settings were changed. Restart the service. Restarting the OS will not apply the changes.
	`The configuration has been modified. Start the service. Rebooting the OS will not apply the changes.`
	Displayed when the service remains stopped after the NFS service, CIFS service, SFTP service, FTP service or TFTP service was reconfigured or after the LDAP server settings were changed. Start the service. Restarting the OS on a node will not apply the changes.
	`The service is incomplete. Restart the service.`
	Displayed when the service is running incompletely. A problem might have occurred, so restart the service.
	If the display contents do not change after restarting the service, collect the error information and contact the maintenance personnel. For details on how to collect error information, see the *Troubleshooting Guide*.

Return values

Table 2-370 Return values of the svstatus command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
65, 68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
68[#], 95	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
The command ended abnormally due to multiple causes.

sysinfoget (Output the operating information of the system and specify settings related to output)

Synopsis

```
sysinfoget --all [--load] [--ftrace-time collection-time]
    [--fprof-time collection-time] [-o directory-name]
sysinfoget [--ftrace] [--fprof] [--ftrace-time collection-time]
    [--fprof-time collection-time] [--pstack] [--pfile] [--load]
    [-o directory-name]
sysinfoget --del [-o directory-name]
sysinfoget -h
```

Description

In addition to outputting the system's operating information, you can specify the output destination and the operating information to be output. If the information is not output to a directory on a file system, the operating information is output to an OS disk. You can check the operating information that is output to the OS disk by downloading all the log data. Note that if the system load changes greatly or if the operating information is output before all log data is downloaded, the operating information is automatically output to an OS disk.

The output destination directory requires at least 500 MB of free space. If the directory has insufficient free space, the KAQG53012-E message appears, and the operating information cannot be output. In addition, if the operating information remains, the file system capacity might be compressed. After retrieving the operating information from the output destination directory, immediately delete the information.

You can interrupt this command by pressing **Ctrl** + **C**. If command processing is interrupted because **Ctrl** + **C** was pressed or because of a timeout, the operating information obtained up to the point when the processing was interrupted is output.

> *Notes:*
>
> - Make sure to execute this command in accordance with the instructions from maintenance personnel.
>
> - When this command is used to output system operating information to a directory in a file system, if the name of that directory contains multi-byte characters, depending on the OS environment to which the operating information is transferred, you might not be able to expand an archive file. In this case, output the operating information to a directory whose name does not contain any multi-byte characters. Alternatively, use an application to convert the character encoding of the archive file to the encoding used in the OS environment to which the operating information is to be transferred.

Options and arguments

```
--all
```

Specify this option to output all the operating information (a list of function traces, function profiles, process stack traces, and process open files).

`--del`

Deletes the operating information that was output to the directory specified in the `-o` option. If the `-o` option is omitted, the operating information that was output to the OS disk is deleted.

`--fprof`

Specify this to output function profiles as part of the operating information.

`--fprof-time` *collection-time*

Specify the collection time for function profiles in the range from 1 to 30 (in seconds). Specify this option together with `--all` or `--fprof`. If you omit this option, `20` is set.

`--ftrace`

Specify this option to output function traces as part of the operating information.

`--ftrace-time` *collection-time*

Specify the collection time for function traces in the range from 1 to 10 (in seconds). Specify this option together with `--all` or `--ftrace`. If you omit this option, `1` is set.

`--load`

Specify this option to limit, to specific processes, the processes that are to be targeted by other options that are specified at the same time. Specify this option together with `--all`, `--pstack`, or `--pfile`.

`-o` *directory-name*

To output the operating information to a directory on a file system, specify the absolute path to the directory, beginning with `/mnt/`.

`--pfile`

Specify this option to output a list of process open files as part of the operating information.

`--pstack`

Specify this option to output process stack traces as part of the operating information.

Note:

If you do not specify the `--all`, `--del`, or `-h` options, make sure that you specify at least one omittable option.

Table 2-371 Return values of the sysinfoget command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 11	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

syslurestore (Restore system LUs)

Synopsis (for cluster configurations)

```
syslurestore --trans [--system-only] [--system-name cluster-name]
syslurestore -f settings-file-name [--id virtual-server-ID]
syslurestore -s osdisk IP-address
syslurestore -s cmlu
```

Synopsis (for single node configurations)

```
syslurestore --trans [--system-only] [--system-name host-name]
syslurestore -f settings-file-name
```

Synopsis (to reference the command syntax)

```
syslurestore -h
```

Description

Uses the information obtained from the `syslusave` and `sysluscheduleset` commands to restore system LUs. If the system settings file is saved in an HCP system and the user data has been migrated to the same HCP system, this command can also be used to batch restore all the information saved in the system LUs and user LUs. For details on how to restore the system settings file, see the *Troubleshooting Guide*.

When you use the system settings file and user data stored in HCP to restore the information of the system LU and user LUs, if you specify that all the files

in the file system are to be restored as a stub file by background processing, one of the following triggers is used to start the restore operation:

For a physical node in a cluster configuration:

When the cluster is rebuilt and the resource group is started after the system LU is restored.

For a single-node configuration:

When the OS is automatically restarted after the system LU is restored.

When the restore of the stub file starts, the KAQM37113-I message is displayed. When the restore of the stub file finishes, the KAQM37114-I message is displayed.

Notes:

- If an error occurred simultaneously on an OS disk and the cluster management LU, you cannot restore them separately. Restore the system LUs in a batch operation.

- If an error occurred simultaneously on the OS disks on both nodes, you cannot restore them separately. Restore the system LUs in a batch operation.

- The system settings file for a system that will be restored is identified by using the fixed IP address of the management port interface on the node. Therefore, do not change the fixed IP addresses of the management port interfaces on either node after you save system settings. Also, make sure that the fixed IP address of the BMC port is the same as the IP address that existed when the settings were saved.

- Execute the command in an HDI system that uses the same version of the OS that was used when the information was acquired.

- If you rename a directory while the stub file is being restored by background processing, the stub file for the files or directories in the directory you renamed might not be restored. In this case, the stub file is restored when a client accesses a file or directory in the directory you renamed.

- While the `syslurestore` command is being executed, do not perform other operations. If you have inadvertently performed other operations, ask maintenance personnel to perform initial setup and then to re-execute the `syslurestore` command.

For a cluster configurations:

To recover the OS disk or all system LUs, ask maintenance personnel to perform initial setup beforehand.

If you restore all the system LUs in a batch operation, use the system settings file (a file in which the information within the system LU is archived). If you restore either an OS disk or the cluster management LU, use the information stored in the system LU. If you restore an OS disk, you need to log in to the node to be restored.

If an OS disk is restored, the OS on the execution node is automatically restarted.

If you restore the cluster management LU or all system LUs, the OSs on both nodes in the cluster are automatically restarted. In addition, because the cluster configuration is initialized after the restart, you need to create the cluster again.

For a single-node configuration:

Make sure that maintenance personnel have performed initial setup beforehand.

The operating system will restart automatically when the system LUs are restored.

Options and arguments

`-f` *settings-file-name*

Specify the name of the system settings file when restoring a system LU. You can only specify a file in the SSH account home directory (`/home/nasroot`). If the target file is in a directory on a remote host or a user LU, you must transfer the file to the SSH account home directory (`/home/nasroot`). If you specify this option, the command will output messages indicating the progress of the restoration process and the time remaining.

Specify the name of the system settings file. You can only specify a file in the SSH account home directory (`/home/nasroot`). If the target file is in a directory on a remote host or a user LU, you must transfer the file to the SSH account home directory (`/home/nasroot`).

`--id` *virtual-server-ID*

This option is not supported.

`-s cmlu`

Specify this to restore the cluster management LU.

`-s osdisk` *IP-address*

Before restoring an OS disk, specify the fixed IP address of the management port interface. IPv6 IP addresses cannot be specified.

`--trans [--system-only] [--system-name` *cluster-name-or-host-name*`]`

If data is migrated to an HCP system, specify this to use the system settings file and user data saved on the HCP system to recover the system LU and user LU information. The following information will be specified in an interactive mode:

- HCP information
- Data port information for use with communication with an HCP system
- Common key information for keys used for encryption of data stored on an HCP system (when data stored on an HCP system has been encrypted)
- Data recovery methods

In single-node configurations, also specifies whether DHCP is used. If `mng0` is used to communicate with HCP, do not specify the data-port information.

If you specify this option, the command will output messages indicating the progress of the restoration process and the time remaining.

To end interactive entry and cancel the command execution, press **Ctrl +D** without entering anything for any of the items.

`--system-only`

> Specify this to restore only the system LU information.

`--system-name` *cluster-name-or-host-name*

> Specify this when multiple sets of system configuration information are saved on a single tenant. Be sure to specify the cluster name or host name that was specified when the system settings file was saved.
>
> For a cluster configuration, specify a cluster name. For a single-node configuration, specify a host name.

The table below lists the HCP system information that is to be specified interactively.

Table 2-372 The HCP system information to be specified by using the syslurestore command

Item	Explanation
host-name	Specify the HCP host name (FQDN).
host-address	Specify the HCP IP address. If the HCP system to be linked uses a relaying device such as a load balancer when connecting to the network, specify the IP address that has been made external and is used to connect to the HCP system.
tenant-name	Specify the HCP tenant name.
user-name	Specify the user name of the data access account that can access all namespaces in the tenant.
password	Specify the password of the data access account that can access all namespaces in the tenant.

The table below lists the information on the data port used for communication with HCP system that is to be specified interactively:

Table 2-373 Information of a data port to be specified by using the syslurestore command

Item	Explanation
port-name	Specify the port name to be used for communication with the HCP system.
ip-address	Specify the IP address to be used for communication with the HCP system. This is not displayed when DHCP is used.

Item	Explanation
netmask	Specify the netmask of the IP address to be used for communication with the HCP system. This is not displayed when DHCP is used.
gateway	Specify the IP address of the gateway to be used for communication with the HCP system. Note that you can omit this item if gateway settings do not need to be specified.

Information about the common keys used for encryption of data on an HCP system set in interactive mode will be displayed in the following table:

Table 2-374 Keys for encryption of data stored on an HCP system designated by using the syslurestore command

Item	Description
Enter key	Specify the key saved in storage media outside the system.
Enter passphrase	Specify the passphrase specified for the hcpdisplaykey command.

Notes:

- The character strings specified for Enter passphrase is not displayed.

- When you specify the key saved in storage media outside the system, make sure that the key does not include a linefeed character.

The table below lists the information about the restore methods that are to be specified interactively:

Table 2-375 Information on the restore method to be specified by using the syslurestore command

Item	Explanation

Restore method	Select the data restore method.
	
	1. Background
	
	   Specify this to restore all the files as a stub file by background processing.
	
	2. On-demand
	
	   Specify this to restore the target files and directories and their parent directory when a client accesses one of the target files or directories.
	
	Note that this item is not displayed when the --system-only option is specified.

Background restore speed	Select the restore speed if you specified 1. Background for Restore method. By selecting the restore speed, you can specify which operation takes priority (the restore operation or processing of I/O requests from clients). 1. Slow

Item	Explanation
	Specify this to perform a restore at a speed slower than the speed when the `--normal` option is specified (rough guide of the processing time: about twice longer), to make the processing of I/O requests from the clients take priority over the restore operation. 2. `Normal` Specify this to perform the restore operation at the normal speed. 3. `Fast` Specify this to perform a restore at a speed faster than the speed when the `--normal` option is specified (rough guide of the processing time: about half shorter), to make the restore operation take priority over the processing of I/O requests from the clients.

Return values

Table 2-376 Return values of the syslurestore command

Return value	Description
`0`	Normal termination
`1, 2`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`11, 12, 15, 25, 26, 27, 28, 29, 30, 31, 68, 69, 70, 71`[#]`, 74, 75, 76`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65, 66, 77`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`71`[#]`, 72, 73`	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`80`	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Examples

To restore the system LU (settings file name: `sysbk_FC-GW4230NW0-T122000092_20120313_1629.tgz`) in one operation:

```
$ sudo syslurestore -f sysbk_FC-GW4230NW0-T122000092_20120313_1629.tgz
KAQM13133-Q Processing might take a while. Do you want to restore the
system settings by using the specified file (saved date and time =
2012/09/25 15:07)? (y/n)y
Restoring the system configuration. (remaining time = 63 seconds)
  Step 1/7 Pre-processing will now start. (remaining time = 63 seconds)
  Step 2/7 Decompressing the system backup files. (remaining time = 33
seconds)
  Step 3/7 Initializing management area-1. (remaining time = 32 seconds)
  Step 4/7 Initializing management area-2. (remaining time = 31 seconds)
  Step 5/7 Initializing management area-3. (remaining time = 30 seconds)
  Step 6/7 Restoring the system files. (remaining time = 20 seconds)
  Step 7/7 Performing post-processing. (remaining time = 10 seconds)
KAQM13131-I The settings for the cluster management LU and both OS disks
in the cluster have been restored, and the OSs in the cluster have been
restarted. After restarting the OSs, define a cluster.
```

To restore the OS disks:

```
$ sudo syslurestore -s osdisk 10.213.75.135
KAQM13122-Q Processing might take a while. Do you want to restore the OS
disks by using the saved settings (saved date and time = 2012/03/13
16:29)? (y/n)
```

To restore the cluster management LU:

```
$ sudo syslurestore -s cmlu
KAQM13123-Q Processing might take a while. Do you want to restore the
cluster management LU by using the saved settings (saved date and time =
2012/03/13 16:30)? (y/n)
```

To use the user data and the system settings file that are saved on the HCP system to restore the information saved in the system LU and user LUs (for cluster configurations):

```
$ sudo syslurestore --trans --system-name cluster01
[Transfer settings]
host-name: hcp.example.com
host-address: 10.213.88.77
tenant-name: tenant01
user-name: user01
password:

KAQM13211-Q Do you want to set the data port? (y/n) n
KAQM13214-I A summary of the system settings is now being acquired...
System settings summary
  System name                : cluster01
  System model               : example
  System version             : 5.2.0-00
  Network information
    node 0(DN000000038)      : 10.213.92.59(mng0)
    node 1(DN000000039)      : 10.213.92.60(mng0)
  Total number of file systems : 4
  Backup date and time       : 2015/03/12 08:51

[HCP payload encryption]
Enter key:
53616c7465645f5fd33d2b96c75f2f3fe7d63be2312908663f47d394813851c029a65deae02
```

```
ba867a8998bb6b1d34976478ae0359c5356f8511915f698025c6ca062c1309cf6c31afe4b56
84ca1a1e22e527c4d15adac514a1e3461b1e23bd9694927dd5c3e4548ff981b0b54a520f399
521aa5fd7d60fddc22837121ed5e90b
Enter passphrase:
[Restore method]
1. Background
2. On-demand
KAQM13226-I Select a number indicating the method for restoring files in
the file system as stub files, and then press [Enter]. (1/2): 1

[Background restore speed]
1. Slow
2. Normal
3. Fast
KAQM13227-I Select a number indicating the speed for restoring stub files
in the background, and then press [Enter]. (1/2/3): 2

KAQM13185-Q Processing will take about 353 seconds. Do you want to restore
system settings by using the saved file? (y/n)y
Restoring the system configuration. (remaining time = 353 seconds)
  Step 1/9 Pre-processing will now start. (remaining time = 353 seconds)
  Step 2/9 Decompressing the system configuration information files.
(remaining time = 293 seconds)
  Step 3/9 Initializing management area-1. (remaining time = 292 seconds)
  Step 4/9 Initializing management area-2. (remaining time = 291 seconds)
  Step 5/9 Initializing management area-3. (remaining time = 290 seconds)
  Step 6/9 Restoring the system files. (remaining time = 280 seconds)
  Step 7/9 Creating the file systems. (remaining time = 230 seconds)
  Step 8/9 Restoring the file systems. (remaining time = 140 seconds)
    1/4 fs01 (remaining time = 140 seconds)
    2/4 fs02 (remaining time = 110 seconds)
    3/4 node1_fs01 (remaining time = 80 seconds)
    4/4 node1_fs02 (remaining time = 50 seconds)
  Step 9/9 Performing post-processing. (remaining time = 20 seconds)
KAQM13131-I The settings for the cluster management LU and both OS disks
in the cluster have been restored, and the OSs in the cluster have been
restarted. After restarting the OSs, define a cluster.
```

To use the user data and the system settings file that are saved on the HCP system to restore the information saved in the system LU and user LUs (for single node configurations):

```
$ sudo syslurestore --trans --system-name DT235001059
[Transfer settings]
host-name: hcp.example.com
host-address: 10.213.88.77
tenant-name: vm-cse
user-name: backup
password:

KAQM13211-Q Do you want to set the data port? (y/n) n
KAQM13214-I A summary of the system settings is now being acquired...
System settings summary
The number of system information(1)
  System name                 : DT235001059
  System model                : example
  System version              : 5.2.0-00
  Network information
    node 0(DT235001059)       : 10.213.137.178(mng0)
  Total number of file systems : 2
  Backup date and time        : 2015/03/12 09:38

The number of system information(2)
  System name                 : DT235001059
  System model                : example
  System version              : 5.2.0-00
```

Hitachi Data Ingestor CLI Administrator's Guide

```
   Network information
     node 0(DT235001059)      : 10.213.137.178(mng0)
   Total number of file systems : 2
   Backup date and time       : 2015/03/12 08:23

KAQM13213-I Enter the number of the system settings to be recovered, and
then press the [Enter] key. (1 - 2) 1
System settings summary
   System name                : DT235001059
   System model               : example
   System version             : 5.2.0-00
   Network information
     node 0(DT235001059)      : 10.213.137.178(mng0)
   Total number of file systems : 2
   Backup date and time       : 2015/03/12 09:38

[HCP payload encryption]
Enter key:
53616c7465645f5f0f6234d29adddff6811ad1d97acb588e9e112281891ee1df0f991b9b3ca
15a31802e80252fa9ec54f1883a74416b1cb7309954d66e756037f94aed780e615d42583597
cd73b51a1cb53f79a96be6a43311d9406a1c5fe38b05dab7258c1fd6f6f8e34efc812c72337
2eb07c5a528203d114a18809076a7ea
Enter passphrase:
[Restore method]
1. Background
2. On-demand
KAQM13226-I Select a number indicating the method for restoring files in
the file system as stub files, and then press [Enter]. (1/2): 1

[Background restore speed]
1. Slow
2. Normal
3. Fast
KAQM13227-I Select a number indicating the speed for restoring stub files
in the background, and then press [Enter]. (1/2/3): 2

KAQM13185-Q Processing will take about 181 seconds. Do you want to restore
system settings by using the saved file? (y/n)y
Restoring the system configuration. (remaining time = 181 seconds)
  Step 1/8 Decompressing the system configuration information files.
(remaining time = 181 seconds)
  Step 2/8 Initializing management area-1. (remaining time = 166 seconds)
  Step 3/8 Initializing management area-2. (remaining time = 165 seconds)
  Step 4/8 Initializing management area-3. (remaining time = 164 seconds)
  Step 5/8 Restoring the system files. (remaining time = 154 seconds)
  Step 6/8 Creating the file systems. (remaining time = 129 seconds)
  Step 7/8 Restoring the file systems. (remaining time = 85 seconds)
    1/2 fs01 (remaining time = 85 seconds)
    2/2 fs02 (remaining time = 55 seconds)
  Step 8/8 Performing post-processing. (remaining time = 25 seconds)
KAQM13171-I The settings for the cluster management LU and the OS disk
have been restored, and the OS has been restarted.
```

syslusave (Save system LUs)

Synopsis (for cluster configurations)

```
syslusave
syslusave -o
syslusave -d {trans|directory-path}
```

Synopsis (for single node configurations)

```
syslusave -o
syslusave -d {trans|directory-path}
```

Synopsis (to reference the command syntax)

```
syslusave -h
```

Description

Saves system LUs.

Before executing this command, check the information in *Before saving a system LU:* in Management of system settings on page 3-80.

When this command is executed in a cluster configuration, the information about the OS disk is saved on the cluster management LU, and the information about the cluster management LU is saved on the OS disk. Note that, depending on the option specifications, the system settings file (an archived file containing the information in the system LUs) can be saved outside the system LU in addition to on the system LU.

Options and arguments

-d {trans| *directory-path* }

Specify the destination for saving the system settings file (a file in which the information within the system LU is archived).

trans

Specify this to save the system settings file in an HCP system or FTP server. To save the system settings file in an HCP system, information about the migration-destination HCP system must be specified beforehand. To save the system settings file on an FTP server, information about the transfer-destination FTP server must be specified by using the sysluscheduleset command beforehand.

For a cluster configuration, you can save the system settings file in the HCP system. For a single-node configuration, you can save the system settings file on the HCP system or an FTP server.

directory-path

If you want to save the system settings file in a directory located in the file system, specify the absolute path of the directory beginning with /mnt/.

You can use alphanumeric characters, exclamation marks (!), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), plus signs (+), commas (,), hyphens (-), periods (.), forward slashes (/), semicolons (;), equal signs (=), at marks (@), left square brackets ([), right square brackets (]), carets (^), underscores (_), grave accent marks (`), left curly brackets ({), right curly brackets (}), tildes (~), and spaces. You can also specify multibyte characters. However, you cannot specify a path that includes a symbolic link. Note

that `.snaps` , `.history`, and `.lost+found` cannot be specified for a directory name. In addition, for a read-write-content-sharing file system, `.conflict` and `.conflict_longpath` also cannot be specified as a directory name. Also, `.arc`, `.system_gi`, `.system_reorganize`, or `lost+found` cannot be specified for the name of a directory immediately under the file system. Forward slashes and spaces specified at the end are deleted.

Note that the following directories cannot be specified:

- A directory in a file system that is not mounted as read/write enabled

- A directory in a home-directory-roaming file system

-o

Specify this to output system settings files to the SSH account home directory (`/home/nasroot`). You can output a system settings file for one generation for each node. After executing this command with this option specified, you must use the `scp` command or another secure transfer tool to transfer the system settings file to a remote host, and then delete the file from the SSH account home directory (`/home/nasroot`).

Return values

Table 2-377 Return values of the syslusave command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 14, 17, 18, 19, 20, 21, 22, 23, 24, 30, 67, 68, 70, 71[#], 74[#], 75, 76[#], 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71[#], 72, 73, 74[#], 76[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

> The command ended abnormally due to multiple causes.

Examples

To save the system LU information to the system LU:

```
$ sudo syslusave
```

To save the system settings file in an HCP system or on an FTP server:

```
$ sudo syslusave -d trans
```

To output the system settings file to a location immediately under the home directory of the SSH account (`/home/nasroot`):

```
$ sudo syslusave -o
KAQM13128-I The settings were successfully saved. Transfer the settings
file to an external location, and then erase the file stored in the
system. (output file = sysbk_FC-GW9P67NBX_20100108_0851.tgz)
```

syslusavestatus (Display the save status of system LUs)

Synopsis

```
syslusavestatus [--del delimiter]
syslusavestatus -h
```

Description

Displays the save status of the system LUs.

Options and arguments

`--del` *delimiter*
> Specify this to display the information separated with an alphanumeric character, symbol, or space, whichever is specified.

Displayed information

The following table lists the information displayed when this command is executed in a cluster configuration.

Table 2-378 Information displayed when executing the syslusavestatus command in a cluster configuration

Item	Description
Setting save status	Displays information for the system LUs.

Item	Description
`Transfer all system settings`	Displays the date and time when the data of the system LU was last saved as the system settings file (a file in which the information within the system LU is archived) in the HCP system. This information is displayed in the following format: *date* (format: *YYYY/MM/DD*) *time* (format: *hh*:*mm*) Note, however, that a hyphen (-) is displayed if the data of the system LU has never been output as a system settings file or if the data from the system LU is being saved or restored.
`Download all system settings`	Displays the date and time when the system settings file was last downloaded or saved. This information is displayed in the following format: *date* (format: *YYYY/MM/DD*) *time* (format: *hh*:*mm*) Note that the time is updated when any of the following are performed: • The system settings file is downloaded. • The system settings file is saved in a file system. • The system settings file is saved in an HCP system. Note, however, that a hyphen (-) is displayed if the data of the system LU has never been output as a system settings file or if the data from the system LU is being saved or restored.
`Cluster management LU save status`	Displays information about the cluster management LU.

`Save status`	Displays the save status of the cluster management LU.
	`Normal`
	    Data from the cluster management LU has been saved or restored.
	`Now saving...`
	    Data from the cluster management LU is being saved.
	`Now restoring...`
	    Data from the cluster management LU is being restored.
	Do not execute a save or restoration operation for the system LU if anything other than `Normal` appears for this item.

`Last save date`	Displays the date and time that the data of the cluster management LU was last saved. This information is displayed in the following format: *date* (format: *YYYY/MM/DD*) *time* (format: *hh*:*mm*) Note, however, that a hyphen (-) is displayed if there is no saved data from the cluster management LU on the node or if the data from the cluster management LU is being saved or restored.
`OS disk save status`	Displays information for the OS disk.
node-number , *host-name*	Displays information about the cluster node you are logged in to. This information is displayed in the following format: *node-number*(*host-name*)

Item	Description

Save status	Displays the save status of the OS disk on the cluster node you are logged in to.
	
	`Normal`
	
	    Data from the OS disk has been saved or restored.
	
	`Now saving...`
	
	    Data from the OS disk is being saved.
	
	`Now restoring...`
	
	    Data from the OS disk is being restored.
	
	Do not execute a save or restoration operation for the system LU if anything other than `Normal` appears for this item.

Last save date	Displays the date and time that the data of the OS disk on the cluster node you are logged in to was last saved. This information is displayed in the following format: *date* (format: *YYYY/MM/DD*) *time* (format: *hh:mm*) Note, however, that a hyphen (–) is displayed if there is no saved data from the OS disk on the node or if the data from the OS disk is being saved or restored.
node-number , *host-name*	Displays information about the cluster node you are not logged in to. This information is displayed in the following format: *node-number*(*host-name*)

Save status	Displays the save status of the OS disk on the cluster node you are not logged in to.
	
	`Normal`
	
	    Data from the OS disk has been saved or restored.
	
	`Now saving...`
	
	    Data from the OS disk is being saved.
	
	`Now restoring...`
	
	    Data from the OS disk is being restored.
	
	Do not execute a save or restoration operation for the system LU if anything other than `Normal` appears for this item.

Last save date	Displays the date and time that the data of the OS disk on the cluster node you are not logged in to was last saved. This information is displayed in the following format: *date* (format: *YYYY/MM/DD*) *time* (format: *hh:mm*) Note, however, that a hyphen (–) is displayed if there is no saved data from the OS disk on the node or if the data from the OS disk is being saved or restored.

In addition, the following table lists the information displayed when you execute the command in a single-node configuration.

Table 2-379 Information displayed when executing the syslusavestatus command in a single-node configuration

Item	Description
Setting save status	Displays information for the system LUs.
Save status	Displays the save status of system LU data. Normal System LU data has been saved or restored. Now saving... System LU data is being saved. Now restoring... System LU data is being restored. Do not execute a save or restoration operation for the system LU if anything other than Normal appears for this item.
Transfer all system settings	Displays the date and time that the system LU data was last saved in the system settings file (a file in which system LU information is archived) in the HCP system. This information is displayed in the format shown below. *date* (format: *YYYY/MM/DD*) *time* (format: *hh:mm*) Note, however, that a hyphen (-) is displayed if the data of the system LU has never been output as a system settings file or if the data from the system LU is being saved or restored.
Download all system settings	Displays the date and time when the system settings file was last downloaded or saved. This information is displayed in the following format: *date* (format: *YYYY/MM/DD*) *time* (format: *hh:mm*) Note that the time is updated when any of the following are performed: • The system settings file is downloaded. • The system settings file is saved in a file system. • The system settings file is saved on an FTP server.(for a single-node configuration) • The system settings file is saved in the HCP system. Note, however, that a hyphen (-) is displayed if the data of the system LU has never been output as a system settings file or if the data from the system LU is being saved or restored.

Return values

Table 2-380 Return values of the syslusavestatus command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.

Return value	Description
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
68, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To view the save status of the cluster management LU and the OS disks on both nodes in the cluster (delimiter: `%`)

```
$ sudo syslusavestatus --del "%"
Normal%2010/11/01 06:29%node 0(D3Z7MNBX)%Normal%2010/11/01 06:28%node
1(D5Z7MNBX)%Normal%2010/11/01 06:28%2010/11/01 06:28%2010/11/01 00:07
```

sysluscheduleget (Display the periodic-saving settings for the system LU)

Synopsis

```
sysluscheduleget [-h]
```

Description

Displays whether the periodic saving function of the system LU is enabled, and the schedule for periodic saving.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-381 Information displayed when executing the sysluscheduleget command

Item	Description
Schedule settings for saving all system settings	Displays the information about the periodic saving function of the system LU.

Item	Description

Schedule setting status	Displays whether the periodic saving function of the system LU is enabled.
	
	`On`
	
	    The periodic saving function is enabled.
	
	`Off`
	
	    The periodic saving function is disabled.

Schedule interval	Displays the interval for periodic saving of the system LU.
	
	`Daily`
	
	    The interval for periodic saving is daily.
	
	`Weekly`
	
	`Day of week :` *day-of-week*
	
	    If the interval for periodic saving is weekly, the day of the week that the saving occurs is displayed as `Sun`, `Mon`, `Tue`, `Wed`, `Thu`, `Fri`, and `Sat`. If multiple days of the week are specified, they are displayed separated by a comma (,).
	
	`Monthly`
	
	`Day :` *date*
	
	    If the interval for periodic saving is monthly, the day of the month is displayed in the range from `1` to `31`. If multiple dates are specified, they are displayed separated by a comma (,).

Schedule time	The time when the system LU was saved in `hh:mm` format.

Output setting	Displays the destination for saving the system settings file.
	
	`Server transfer(HCP)`
	
	    Displayed if the system settings file is saved in the HCP system.
	
	`Server transfer(FTP)`
	
	    Displayed if the system settings are saved on the FTP server.
	
	directory-path
	
	    If the system settings file is saved in the file system, the absolute path for the directory is displayed.
	
	`FTP server` [#]
	
	    Displays the IP address or host name of the FTP server. If no host name or IP address is set, a hyphen (-) is displayed.
	
	`User name` [#]
	
	    Displays the user name for the FTP server. If no user name is set, a hyphen (-) is displayed.
	
	`Directory` [#]
	
	    Displays the destination directory. If no destination directory is set, a hyphen (-) is displayed.
	
	`-`
	
	    Displayed if the system settings file is not output.

#
> This item is displayed when a single-node configuration.

Return values

Table 2-382 Return values of the sysluscheduleget command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

sysluscheduleset (Specify the periodic-saving settings for the system LU)

Synopsis (for cluster configurations)

```
sysluscheduleset {[-S periodic-saving-interval]
    [-d {trans|directory-path|off}]} [-t hcp]
sysluscheduleset {--on|--off}
```

Synopsis (for single node configurations)

```
sysluscheduleset {[-S periodic-saving-interval]
    [-d trans [-t {hcp|ftp}]]
    [--server transfer-destination-server]
    [-u user-name] [-p password]
    [--directory transfer-destination-directory-path]}
sysluscheduleset {[-S periodic-saving-interval]
    [-d {home|directory-path}]}
sysluscheduleset {--on|--off}
```

Synopsis (to reference the command syntax)

```
sysluscheduleset -h
```

Description

Specifies whether to enable or disable the periodic saving function of the system LU, or sets the periodic saving schedule. Before executing this

command, check the information in *Before saving a system LU:* in [Management of system settings on page 3-80](#).

The default setting only saves the system LU in the system. By specifying the `-d` option, you can save the system settings file in HDI file systems and transfer-destination servers. The following name is used to save the system settings file in HDI file systems:

```
schedule_syslu_backup.tgz
```

If the HDI system is linked with the HCP system, and if the system settings files are saved in the file system of the HDI system, do not delete the saved system settings files.

Notes:

- You can only enable the periodic saving function of the system LU for either of the nodes.
- You can save only one generation of the system setting file.

By default, the setting is specified so that the system LU is periodically saved at 00:07 every day. 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.

Options and arguments

`-d`

Specify this to save the system settings file. You also need to specify one of the arguments below. If you omit an option, the current settings are used.

`home`

You can specify this option for a single-node configuration.

Specify this to save the settings file immediately under the home directory (`/home/nasroot`) of the SSH account.

`off`

You can specify this option in a cluster configuration.

Specify this to change the settings back to the default settings (where only the system LU is saved in the system).

`trans`

Specify this to save the settings file on the transfer-destination server.

Note that if this argument is specified in a cluster configuration, the system settings file is also saved on the system LU. If this argument is specified in a single-node configuration, the system settings file is also saved immediately under the SSH account's home directory (`/home/nasroot`).

directory-path

If you want to save the settings file in a file system, specify the absolute path of the directory beginning with `/mnt/`.

Note that `.snaps` , `.history`, and `.lost+found` cannot be specified for a directory name. In addition, for a file system for which read-write-content-sharing functionality is enabled, `.conflict` and `.conflict_longpath` also cannot be specified as a directory name. Also, `.arc`, `.system_gi`, `.system_reorganize`, or `lost+found` cannot be specified for the name of a directory immediately under the file system.

The directories on a home-directory-roaming file system cannot be specified as the location where the system setting file is to be saved.

Note that if this argument is specified in a cluster configuration, the system settings file is also saved on the system LU. If this argument is specified in a single-node configuration, the system settings file is also saved immediately under the SSH account's home directory (`/home/nasroot`).

`--directory` *transfer-destination-directory-path*

Specify a directory on the destination FTP server. The directory must be created on the FTP server before transfer starts. Note that you cannot specify a path that includes double quotation marks ("), dollar signs ($), asterisks (*), grave accent marks (`), space, and multibyte characters. In addition, You cannot use the backslash (\) as the last character. If you omit this option, the current settings are used.

`{--on|--off}`

Specify this to explicitly declare whether you want to enable or disable the periodic saving function of the system LU. The initial setting is `--on` for the execution node, and `--off` for the other node.

`--on`

Specify this to enable the periodic saving function of the system LU.

`--off`

Specify this to disable the periodic saving function of the system LU.

`-p` *password*

Specify the password used to log in to the destination FTP server. Note that you cannot specify a password that includes double quotation marks ("), dollar signs ($), grave accent marks (`), space, and multibyte characters. In addition, You cannot use the backslash (\) as the last character. If you omit this option, the current settings are used.

`-S` *periodic-saving-interval*

Specify the interval for periodic saving of the system LU.

The intervals that can be specified for periodic saving are described below. If you omit this option, the current setting value remains in effect. The initial setting is `D-0007` (saved at 0:07 every day).

`D-`*time*

Specify this if you want to specify daily as the periodic-saving interval. Specify *time* in *hhmm* format.

`W`–*day-of-week*–*time*

Specify this if you want to specify weekly as the periodic-saving interval. Uses `Sun`, `Mon`, `Tue`, `Wed`, `Thu`, `Fri`, and `Sat` to specify the *day-of-week*. To specify multiple days of the week, separate the days by using a comma (`,`). Specify *time* in *hhmm* format.

`M`–*date*–*time*

Specify this to specify monthly as the periodic-saving interval. Specify *date* in the range from `1` to `31`. If you specify a value from `29` to `31`, periodic saving is performed only in months that contain the specified day. To specify multiple days, separate the days by using a comma (`,`). Specify *time* in *hhmm* format.

`--server` *transfer-destination-server-name*

Specify an IP address or host name of no more than 255 characters for the destination FTP server. We recommend you specify an IP address.

`-t`

Specify the destination server. You also need to specify either of the options below. If you omit this option in a single-node configuration, `hcp` is set.

`hcp`

Specify this to save the settings file in the HCP system.

`ftp`

You can specify this option for a single-node configuration.
Specify this to save the settings file on the FTP server. Start the FTP server in advance. Note that you also need to specify this with the `--server` option.

`-u` *user-name*

Specify the user name used to log in to the destination FTP server. Note that you cannot specify a user name that includes double quotation marks (`"`), dollar signs (`$`), grave accent marks (`` ` ``), space, and multibyte characters. In addition, You cannot use the backslash (`\`) as the last character. If you omit this option, the current settings are used.

Return values

Table 2-383 Return values of the sysluscheduleset command

Return value	Description
0	Normal termination

Return value	Description
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
18, 19, 20, 21, 22, 23, 24, 25, 27, 30, 70, 71[#], 74[#], 75, 76[#], 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71[#], 72, 73, 74[#], 76[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
80	The command has finished executing. However, you need to check the message to ensure that there are no problems in the settings and system status.
97, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Examples

To disable the system LU periodic-saving function:

```
$ sudo syslusheduleset --off
```

To specify the system LU periodic-saving function according to the following conditions:

- The system LU is to be saved at 12:30 on Sundays, Mondays, and Tuesdays.
- The system settings file is to be output to the /mnt/FS01/dir directory.

```
$ sudo syslusheduleset -S W-Sun,Mon,Tue-1230 -d /mnt/FS01/dir
```

tapeadd (Register tape drive information)

Synopsis

```
tapeadd -a [-nomsg]
tapeadd -t WWN[:LUN][,WWN[:LUN]...] [-nomsg]
```

Description

The `tapeadd` command registers information with the NDMP server about a tape drive connected to a node over a SAN.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

To register tape drive information by executing this command, make sure that the tape drives to be registered on the NDMP server have already been connected to the node by maintenance personnel or the SAN administrator. The maximum number of tape drives that can be registered with the NDMP server is as follows: 32 for a node.

After the operation that uses tape drives connected to a node via a SAN starts, execute this command specifying `-t` option and both a WWN and LUN to limit the target tape drives. Also, make sure that no backup or restore operations are being performed before you execute this command.

Do not execute this command during backup or restore processing. When this is executed, any backups or restorations being processed on the tape drive specified for registration might terminate with an error.

If you execute this command while the NDMP server is running, the NDMP server will be restarted automatically. After executing the command, check the operating status of the NDMP server.

Options and arguments

`-a`

Specify this option to register all tape drives with the NDMP server

`-t` *WWN* [: *LUN*][, *WWN* [: *LUN*]...]

Specify the WWN and LUN for a particular tape drive to be registered. Note that the alphabetic characters in each WWN must be lower case.

If only the WWN is specified, all tape drives belonging to the specified WWN are registered.

Return values

Table 2-384 Return values of the tapeadd command

Return value	Description
0	Normal termination
1, 2, 3, 4	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
6, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation.

Return value	Description
	If this error occurs repeatedly, contact maintenance personnel.
`7, 11, 31, 32, 33, 34, 37, 38, 39`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`98, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To register all tape drives connected to a node via a SAN on the NDMP server:

```
$ sudo tapeadd -a
Aug 14 17:29:05 KAQB11500-I tapeadd command execution has started.
Aug 14 17:29:15 KAQB11501-I tapeadd command has finished.
```

To register a particular tape drive connected over a SAN to a node (`WWN`: `500104f00094ad66`, `LUN`: 0):

```
$ sudo tapeadd -t 500104f00094ad66:0
Aug 14 17:29:59 KAQB11500-I tapeadd command execution has started.
Aug 14 17:30:10 KAQB11501-I tapeadd command has finished.
```

tapedel (Unregister registered tape drive information)

Synopsis

```
tapedel -a [-nomsg]
tapedel -t WWN[:LUN][,WWN[:LUN]...] [-nomsg]
tapedel -h
```

Description

The `tapedel` command unregisters tape drive information registered on an NDMP server.

This command is applied to the node on which the command is executed. This command must be executed on both nodes in cluster configurations.

Do not execute this command while performing a backup or restore operation. If you execute this command while the NDMP server is running, the NDMP server will be restarted automatically. After executing the command, check the operating status of the NDMP server.

Options and arguments

`-a`

Specify this option to unregister information for all tape drives registered on an NDMP server.

`-t` *WWN* `[:` *LUN* `][,` *WWN* `[:` *LUN* `]...]`

Specify the target tape drive WWN and LUN to unregister information registered for a specific tape drive. Note that the alphabetic characters in each WWN must be lower case.

If only the WWN is specified, information for all tape drives belonging to the specified WWN is unregistered.

Return values

Table 2-385 Return values of the tapedel command

Return value	Description
`0`	Normal termination
`1, 2, 3, 4`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`6, 12, 13, 14, 15, 16, 17, 18, 19`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`11, 51, 52, 53, 54`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`98, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To unregister the specified tape drive (`WWN: 500104f00094ad66`, `LUN: 0`):

```
$ sudo tapedel -t 500104f00094ad66:0
Aug 14 17:33:45 KAQB11500-I tapedel command execution has started.
Aug 14 17:33:48 KAQB11501-I tapedel command has finished.
```

tapelist (Display information about tape drives)

Synopsis

```
tapelist [[-d][-A]|-D] [-t WWN[:LUN][,WWN[:LUN]...]] [-c] [-nomsg]
tapelist -h
```

Description

The `tapelist` command displays a list of the tape drive information.

When you execute this command, be careful in specifying options. When no options are specified, only the registration status of the registered tape drives is displayed, and the connection status of the tape drives is not detected.

The following table describes the meaning of specifying each option.

Table 2-386 Specification of the tapelist command options and their purposes of use

Options	Purposes of use
None (`-d`, `-A`, nor `-D`) specified	During normal operation, such as before performing a backup or recovery operation, use this option to check whether tape drive information is registered on the NDMP server.
`-d` specified[#]	Checks whether the tape drives are working properly such as when installing a new tape drive or when tape drives cannot be used.
`-A` specified[#]	Checks whether the tape drives are working properly when tape drives cannot be used.
`-D` specified[#]	Checks the information of tape drives that are not registered yet on the NDMP. This option is usually used when installing an additional tape drive.

#:

The `tapelist` command with these options specified might return an error or cause processing to terminate with an error, depending on the situation. If a backup or restore operation is being performed on the node on which you execute the command, the command returns an error (return value `74`). If the backup or restore operation is being performed on the other node, the operation currently being performed might terminate with an error.

If you execute this command with these options specified, make sure that no backup or restore operation is being performed. In addition, to minimize the effect on a backup or restore operation performed while the command is being executed, we recommend that you specify both WWN and LUN in the `-t` option when you execute this command.

Options and arguments

`-A`

Specify this option to view information about only the tape drives registered on the NDMP server.

When this option is specified, the connection status of the tape drive is also displayed.

`-c`

Specify this option to display each piece of information delimited with colons (`:`), rather than showing the item names.

-d

Specify this option to view information about only the active tape drives connected to a node via a SAN.

When this option is specified, the connection status of the tape drive is also displayed.

-D

Specify this option to view information about only the active tape drives that are connected to a node via a SAN and that are not registered on the NDMP server.

When this option is specified, the connection status of the tape drive is also displayed.

-t *WWN* [: *LUN*] [, *WWN* [: *LUN*] ...]

Specify this option to view information about specific tape drives. For *WWN* and *LUN*, specify the WWN and LUN of each tape drive for which you want to view information. Note that the alphabetic characters in each WWN must be lower case.

If you specify a WWN without specifying an LUN, information about all the tape drives that belong to the WWN is displayed.

Displayed information

The following table lists the information items displayed for a tape device.

Table 2-387 Information displayed when executing the tapelist command

Item	Description
WWN	Displays the WWN of a tape drive in hexadecimal format.
LUN	Displays the LUN of a tape drive in decimal format.
Status	Displays the connection status and the registration status of a tape drive in the following format: *tape-drive-connection-status*,*tape-drive-registration-status* Either of the following is displayed for *tape-drive-connection-status*: - The `tapelist` command did not detect the connection status of a tape drive. D The tape drive is connected to the node and is active. N The tape drive is not connected to the node or is not turned on. Either of the following is displayed for *tape-drive-registration-status*: A The tape drive is registered on the NDMP server. B The connection between a tape drive and a node is blocked.

Item	Description

	`D`
	
	    The tape drive is not registered on the NDMP server.
	
	`I`
	
	    The registration information of a tape drive is disabled.

`Model`	Displays the model name of a tape drive. If information about a tape drive could not be acquired because of an error on the tape drive, `Error` is displayed.

`Type`	Displays the type of a tape device.
	
	`Medium Changer`
	
	    The tape device is a robot.
	
	`Sequential-Access`
	
	    The tape device is a tape drive.
	
	`Error`
	
	    Information about the tape device type could not be acquired because an error occurred on the tape drive.

`Path`	Displays the path to the device file for the tape drive.

Return values

Table 2-388 Return values of the tapelist command

Return value	Description
`0`	Normal termination
`1`, `2`, `3`, `4`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`6`, `17`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`11`, `72`, `73`, `74`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

tftpget (Display the TFTP service configuration)

Synopsis
```
tftpget [-h]
```

Description

Displays the TFTP service configuration.

This command cannot be executed for HDI Remote Server.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-389 Information displayed when executing the tftpget command

Item	Description
`Access directory`	Displays the path of the access directory. If a access directory has not been set, a hyphen (-) is displayed.

Return values

Table 2-390 Return values of the tftpget command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`65, 68`[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`68`[#]`, 70, 95`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
    The command ended abnormally due to multiple causes.

tftpset (Change the TFTP service configuration)

Synopsis

```
tftpset -d access-directory-path
tftpset [-y] --clear
```

```
tftpset -h
```

Description

Changes the TFTP service configuration on the node you are logged in to.

This command cannot be executed for HDI Remote Server.

In a cluster configuration, you must specify the same settings on both nodes.

When you have changed the TFTP service configuration, restart the TFTP service. The new configuration will not be applied until you restart the TFTP service.

Options and arguments

`--clear`

Specify this option to clear all settings related to the TFTP service.
The following conditions must be met before you can specify this option:

- The TFTP service is stopped.
- Automatic startup of the TFTP service is disabled.

`-d` *access-directory-path*

Specify the absolute path of the access directory, using no more than 255 characters beginning with `/mnt/` .

For a home-directory-roaming file system and read-write-content-sharing file system, you must specify the mount point as a access directory. Note that directories in a home-directory-roaming file system cannot be specified.

You can use alphanumeric characters, exclamation marks (`!`), hash marks (`#`), dollar signs (`$`), percent signs (`%`), ampersands (`&`), single quotation marks (`'`), left parentheses (`(`), right parentheses (`)`), plus signs (`+`), commas (`,`), hyphens (`-`), periods (`.`), forward slashes (`/`), semicolons (`;`), equal signs (`=`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), carets (`^`), underscores (`_`), grave accent marks (`` ` ``), left curly brackets (`{`), right curly brackets (`}`), and tildes (`~`). However, you cannot specify a path that includes a symbolic link. Note that `.conflict`, `.conflict_longpath`, `.snaps` , `.history`, and `.lost +found` cannot be specified for a directory name.
Also, `.arc`, `.system_gi`, `.system_reorganize`, or `lost+found` cannot be specified for the name of a directory immediately under the file system. Forward slashes specified at the end are deleted.

Return values

Table 2-391 Return values of the tftpset command

Return value	Description
0	Normal termination

Return value	Description
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
1, 10, 32, 35, 36, 38, 39, 41, 42, 44, 46, 68[#], 70, 74, 94[#], 95	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
94[#], 96	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

timeget (Display the time settings)

Synopsis

```
timeget [{-c|--del delimiter}] [-u] [-s]
timeget -h
```

Description

Displays the current node time, or the IP address or host name of an NTP server.

When you omit all options, the command displays the current node time in the following format:

```
day-of-the-week month date time(hh:mm:ss) time-zone year
```

Note that when you specify both the -u and -s options, the -u option is ignored.

Options and arguments

-c

Specify this to display the items separated with colons (:). When you specify this option, the current node time is displayed in the following format:

$year$:$month$:day:$hour$:$minute$:$second$:$time$-$zone$

`--del` *delimiter*

Specify this to display the items separated with an alphanumeric character, symbol, or space, whichever is specified.

`-s`

Specify this to view the IP address or host name of the NTP server.

`-u`

Specify this to display the current node time in UTC.

Return values

Table 2-392 Return values of the timeget command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

timeset (Set the time settings)

Synopsis

```
timeset [-s NTP-server[,NTP-server]] [[-u] YYYYMMDDhhmm[ss]]
timeset -h
```

Description

For cluster configurations:

Sets whether to use the node time or an NTP server time.

To set the node time, the status of the node to which you are logged in must be `INACTIVE`. Note that the `timeset` command must be executed on both nodes in the cluster.

When you set up an NTP server, executing the `timeset` command on one node applies the settings to both nodes in the cluster.

Restart the OS on both nodes after changing the settings. The times on the nodes are synchronized with the NTP server after the OSs on the nodes are restarted.

For single-node configurations:

Sets whether to use the node time or an NTP server time.

Restart the OS after changing the settings. The settings are applied and the node time is synchronized with the NTP server time after the OS is restarted.

Options and arguments

-s *NTP-server* [, *NTP-server*]

Specify one or two IP addresses or host names when you use an NTP server. If you specify two IP addresses or host names, separate them with a comma (,).

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.

-u

Specify this to handle the specified time as UTC.

YYYYMMDDhhmm [*ss*]

Specify the node time by using a 4-digit number for *year*, and 2-digit numbers for other information. The specification of *second* is optional. If you do not specify the second, the system assumes 00 seconds.

Return values

Table 2-393 Return values of the timeset command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.

Return value	Description
`96, 97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

Examples

To set NTP servers according to the following conditions:

- ○ Set up two NTP servers.
- ○ The IP address of one of the NTP servers is `10.208.193.53`.
- ○ The host name of the other NTP server is `ntp.host1`.

```
$ sudo timeset -s 10.208.193.53,ntp.host1
KAQM05153-Q If you change the node time, you must then restart the OS on
both nodes. Do you want to continue? (y/n)
```

To set an NTP server and the node time according to the following conditions:

- ○ The IP address of the NTP server is `10.208.193.53`.
- ○ The node time is 13:00 February 13, 2011.

```
$ sudo timeset -s 10.208.193.53 20110213130000
KAQM05153-Q If you change the node time, you must then restart the OS on
both nodes. Do you want to continue? (y/n)
```

To cancel the NTP server setting:

```
$ sudo timeset -s ""
```

tlsctl (Settings for TLS)

Synopsis

```
tlsctl [-y] [--tls10 {enable|disable}]
   [--tls11 {enable|disable}] [--tls12 {enable|disable}]
tlsctl -h
```

Description

The `tlsctl` command sets, for the HDI node, the TLS versions to be used for communication with external devices. The command can also be used to view the current setting.

In a cluster configuration, execute this command on either node.

Notes:

- ○ Check the TLS versions supported by the OS and web browser of the machine to be used as the management console. If all the supported

TLS versions are disabled, you will not be able to access the HDI node.

○ You cannot disable all the TLS versions specifiable by this command. Make sure that at least one TLS version is enabled.

○ If you change the settings by using the this command, the Web server automatically restarts, and the management server is disconnected from the node. If you were using the HDI GUI or HDI commands, log in again.

Options and arguments

`--tls10 {enable|disable}`

Specify whether to enable the TLS 1.0.

`enable`

Specify this to enable the TLS 1.0. The initial setting is `enable`.

`disable`

Specify this to enable the TLS 1.0.

`--tls11 {enable|disable}`

Specify whether to enable the TLS 1.1.

`enable`

Specify this to enable the TLS 1.1. The initial setting is `enable`.

`disable`

Specify this to enable the TLS 1.1.

`--tls12 {enable|disable}`

Specify whether to enable the TLS 1.2.

`enable`

Specify this to enable the TLS 1.2. The initial setting is `enable`.

`disable`

Specify this to enable the TLS 1.2.

If you omit all options, the current setting is displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-394 Information displayed when executing the tlsctl command

Item	Description
`TLS Version 1.0`	Displays whether TLS 1.0 is enabled. `Enabled` TLS 1.0 is enabled.

Item	Description
	`Disabled` TLS 1.0 is disabled.

`TLS Version 1.1`	Displays whether TLS 1.1 is enabled.
	
	`Enabled`
	
	TLS 1.1 is enabled.
	
	`Disabled`
	
	TLS 1.1 is disabled.

`TLS Version 1.2`	Displays whether TLS 1.2 is enabled.
	
	`Enabled`
	
	TLS 1.2 is enabled.
	
	`Disabled`
	
	TLS 1.2 is disabled.

Return values

Table 2-395 Return values of the tlsctl command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10, 70, 71`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`96, 97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

umapidget (Get IDs and names mapped using RIDs)

Synopsis

```
umapidget -u {user-name|user-ID}
umapidget -g {group-name|group-ID}
umapidget -s {user-name|group-name|SID}
umapidget -r {user-name|group-name}
umapidget -h
```

Description

Gets the following items when you use user mapping using RIDs:

- User IDs and group IDs assigned to user names and group names[#]

- SIDs and RIDs assigned to user names and group names[#]

- User names or group names[#] associated with user IDs, group IDs, or SIDs

#

> You cannot specify a Windows domain built-in user or group.
>
> In addition, you cannot specify a group name that includes an at mark (@).

Options and arguments

-g { *group-name* | *group-ID* }

> Specify this to get the group ID assigned to a group name, or to get the group name associated with the group ID.

-r { *user-name* | *group-name* }

> Specify this to get the RID assigned to a user name or group name.
>
> A message appears if the RID for the specified user name or group name is outside the range of user IDs and group IDs set for the domain.

-s { *user-name* | *group-name* | *SID* }

> Specify this to get the SID assigned to a user name or group name, or to get the user name or group name associated with the SID.

-u { *user-name* | *user-ID* }

> Specify this to get the user ID assigned to a user name, or to get the user name associated with the user ID.

Return values

Table 2-396 Return values of the umapidget command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
20, 24, 25, 26, 27, 28, 29, 68[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 68[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation.

Return value	Description
	If this error occurs repeatedly, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

`#`

The command ended abnormally due to multiple causes.

Examples

To get the user ID assigned to user `user1`:

```
$ sudo umapidget -u "DOMAIN001\user1"
100032
```

To get the group name associated with group ID `100031`:

```
$ sudo umapidget -g 100031
DOMAIN001\group1
```

To get the SID assigned to user `user1`:

```
$ sudo umapidget -s "DOMAIN001\user1"
S-1-5-21-1659004503-706699826-1957994488-32
```

To get the user names or group names associated with SID `S-1-5-21-1659004503-706699826-1957994488-31`:

```
$ sudo umapidget -s S-1-5-21-1659004503-706699826-1957994488-31
DOMAIN001\group1
```

To get the RID assigned to user `user1`:

```
$ sudo umapidget -r "DOMAIN001\user1"
32
```

To get the RID assigned to user `user2` (message displayed because the RID is out of the range):

```
$ sudo umapidget -r "DOMAIN001\user2"
1000 (The user is outside the range for user mapping using RIDs.)
```

upnpctl (UPnP settings)

Synopsis

```
upnpctl [--on|--off]
upnpctl -h
```

Description

This command can be used in a single-node configuration.

This command specifies whether to enable UPnP. This command also allows you to view the current settings.

If you disable UPnP of HDI when DHCP is enabled for use, you will no longer be able to access HDI using UPnP. If you want to disable UPnP, execute this command after either disabling DHCP, or checking the host name of HDI (FQDN) in the GUI.

Options and arguments

`--off`

Specify this option to disable UPnP.

`--on`

Specify this option to enable UPnP. The initial setting is `--on`.

If you omit all options, the current setting is displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-397 Information displayed when executing the upnpctl command

Item	Description

Status	The current setting is displayed.
	`On`
	    UPnP is enabled.
	`Off`
	    UPnP is disabled.

Return values

Table 2-398 Return values of the upnpctl command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10, 70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If

Command Reference

Return value	Description
	this error occurs repeatedly, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

usradd (Add a user)

Synopsis

```
usradd -u user-ID -g {group-name|group-ID}
    -p password [-c comment] [-C]
    [-G {group-name|group-ID}[,{group-name|group-ID}...]] user-name
usradd -F CSV-file-name [-o result-file-name] [-t] [-V]
usradd -h
```

Description

Adds a user or users. You can register a maximum of 2,000 users per cluster.

Before batch-registering users using a CSV file, you must transfer the CSV file to the SSH account home directory (`/home/nasroot`). We recommend that you specify the `-o` option when you execute this command. When you specify the `-o` option, the execution results are output to a file. If you omit the `-o` option, the results of command processing will not be output. For details about how to create a CSV file, see Format of a CSV file used for batch registration or batch deletion of user information on page B-2. For details about how to check the execution results, see Format of result file used for batch registration or batch deletion of user information on page B-5.

Options and arguments

`-c` *comment*

Specify a comment about the user using no more than 32 characters.

You can use alphanumeric characters, hash marks (`#`), percent signs (`%`), ampersands (`&`), single quotation marks (`'`), left parentheses (`(`), right parentheses (`)`), asterisks (`*`), plus signs (`+`), hyphens (`-`), periods (`.`), forward slashes (`/`), semicolons (`;`), left angle brackets (`<`), right angle brackets (`>`), question marks (`?`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), carets (`^`), underscores (`_`), left curly brackets (`{`), vertical bars (`|`), right curly brackets (`}`), and tildes (`~`). You can also use spaces, except at the beginning or end of the character string.

`-C`

Specify this to permit the user to access CIFS shares.

`-F` *CSV-file-name*

To batch-register users, specify the name of the CSV file containing the user information.

The name of the CSV file must be no more than 255 characters. You can use alphanumeric characters, hyphens (-), and underscores (_). You can also use periods (.), except at the beginning or end of the character string.

-g { *group-name* | *group-ID* }

Specify the primary group to which the user belongs by group name or group ID. The group must be registered by File Services Manager.

-G { *group-name* | *group-ID* }[,{ *group-name* | *group-ID* }...]

Specify the other groups to which the user belongs by group name or group ID. A user can belong to a maximum of 32 groups.

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.

When specifying multiple groups, use a comma (,) to separate the group names or IDs.

-o *result-file-name*

To output the execution results to a file, specify a file name of no more than 255 characters. You can use alphanumeric characters, hyphens (-), and underscores (_). You can also use periods (.), except at the beginning or end of the character string.

The execution results file will be output immediately under the SSH account home directory (/home/nasroot). The file cannot have the same name as an existing file in the /home/nasroot directory.

-p *password*

Specify the user password using 6 to 20 characters.

You can use alphanumeric characters, exclamation marks (!), double quotation marks ("), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), asterisks (*), plus signs (+), commas (,), hyphens (-), periods (.), forward slashes (/), colons (:), semicolons (;), left angle brackets (<), equal signs (=), right angle brackets (>), question marks (?), at marks (@), left square brackets ([), backslashes (\), right square brackets (]), carets (^), underscores (_), grave accent marks (`), left curly brackets ({), vertical bars (|), right curly brackets (}), and tildes (~).

-t

Specify this to check the information in the CSV file without applying it.

-u *user-ID*

Specify the user ID in a range from 200 to 2147483147. You cannot specify a user ID that is already registered by File Services Manager, the NIS server, or the LDAP server for user authentication. You cannot specify 65534. If user mapping is used, you cannot specify a user ID within the range set for user mapping.

-V

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

Specify this to display the progress of the batch-registration processing or CSV file-check processing.

user-name

Specify the user name using no more than 16 characters, beginning with an alphanumeric character. From the second character, you can use alphanumeric characters, hyphens (-), and underscores (_). Alphabetic characters are not case sensitive in Windows. Specify a name that is unique regardless of the case.

You cannot specify a name that duplicates a user name already registered by File Services Manager, the NIS server, or the LDAP server for user authentication. When adding a user who accesses CIFS shares, you cannot specify a name that duplicates the name of any existing group configured to use the ACL.

You cannot specify the following user names, which are reserved in the OS on the node:

Table 2-399 User names reserved in the OS on a node

Start character	User name
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
I	identd, irc
L	libuuid, libvirt-qemu, list, lp
M	mail, messagebus, man
N	nasroot, news, nobody, ntp
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

Return values

Table 2-400 Return values of the usradd command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 66[#], 70, 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
96, 97, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

Examples

To add a user (user name: `user01`, user ID: `1000`) under the following conditions:

- The primary group to which the user belongs is `unit01`.
- The user's password is `12345678`.
- The user is to be registered in the following groups:
  - Group with the group name `unit02`
  - Group with the group ID `2500`
- Set `Unit Leader` as a comment.

```
$ sudo usradd -u 1000 -g unit01 -p 12345678 -c "Unit Leader" -G
unit02,2500 user01
```

To batch-register users under the following conditions:

- The CSV file name is `useradd100.csv`.
- The result file name is `result_adduser.txt`.

```
$ sudo usradd -F useradd100.csv -o result_adduser.txt
```

Command Reference

usrdel (Delete a user)

Synopsis

```
usrdel [-f] user-name
usrdel -F CSV-file-name [-o result-file-name] [-t] [-V] [-f]
usrdel -h
```

Description

Deletes a user or users.

Before batch-deleting users using a CSV file, you must transfer the CSV file to the SSH account home directory (`/home/nasroot`). We recommend that you specify the `-o` option when you execute this command. When you specify the `-o` option, the execution results are output to a file. If you omit the `-o` option, the results of command processing will not be output. For details about how to create a CSV file, see Format of a CSV file used for batch registration or batch deletion of user information on page B-2. For details about how to check the execution results, see Format of result file used for batch registration or batch deletion of user information on page B-5.

Options and arguments

`-f`

Specify this to prevent the confirmation message from appearing.

`-F` *CSV-file-name*

To batch-delete users, specify the name of the CSV file containing the user information.

The name of the CSV file must be no more than 255 characters. You can use alphanumeric characters, hyphens (-), and underscores (_). You can also use periods (.), except at the beginning or end of the character string.

`-o` *result-file-name*

To output the execution results to a file, specify a file name of no more than 255 characters. You can use alphanumeric characters, hyphens (-), and underscores (_). You can also use periods (.), except at the beginning or end of the character string.

The execution results file will be output immediately under the SSH account home directory (`/home/nasroot`). The file cannot have the same name as an existing file in the `/home/nasroot` directory.

`-t`

Specify this to check the information in the CSV file without applying it.

`-V`

Specify this to display the progress of the batch-deletion processing or CSV file-check processing.

user-name

Specify the name of the user to be deleted.

Return values

Table 2-401 Return values of the usrdel command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
10, 66[#], 70, 99[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#]	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
96, 97, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#
The command ended abnormally due to multiple causes.

Example

To batch-delete users under the following conditions:

- The CSV file name is `userdel100.csv`.
- The result file name is `result_deluser.txt`.

```
$ sudo usrdel -F userdel100.csv -o result_deluser.txt
KAQM07077-Q Do you want to perform a batch deletion? (y/n)
```

usrlist (List user information)

Synopsis

```
usrlist [-c] [user-name|user-ID]
usrlist -h
```

Description

Lists user information registered by File Services Manager.

Options and arguments

`-c`

    Specify this to display user information separated with colons (`:`).

user-name | *user-ID*

    To view information for a specific user, specify the user name or user ID.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-402 Information displayed when executing the usrlist command

Item	Description
`User name`	Displays the user name.
`UID`	Displays the user ID.
`GID`	Displays the ID of the primary group to which the user belongs.
`Comment`	Displays a comment about the user. This item does not appear if no comment is set.

Return values

Table 2-403 Return values of the usrlist command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
`10, 70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65`	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

versionlist (Display the version)

Synopsis

```
versionlist
versionlist --os
versionlist -h
```

Description

Displays the version.

Options and arguments

`--os`

> Specify this to view the OS name and version.

If you omit all options, the name and version of the installed product is displayed.

Displayed information

The following table lists the information displayed when you execute the command.

Table 2-404 Information displayed when executing the versionlist command

Item	Description		
`Products Version`	Displays the name and version of the installed product in the following format: `product-name:product-version`		
	product-name	Displays the name of the installed product.	
	product-version	Displays the version of the installed product.	
`System Version`	Displays the name and version of the OS in the following format: `OS-name:OS-version`		
	OS-name	Displays the name of the OS.	
	OS-version	Displays the version of the OS.	

Return values

Table 2-405 Return values of the versionlist command

Return value	Description
0	Normal termination

Return value	Description
1	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
66	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
99	The error cannot be handled by the system administrator. Contact maintenance personnel.

vgrcreate (Create a volume group)

Synopsis

```
vgrcreate [-y] [volume-group-name] LU-name[,LU-name...]
vgrcreate -h
```

Description

This command can be used in a single-node configuration.

The command creates a volume group. You can use the `lulist` command to check the LUs that can be specified.

If you execute this command without specifying a volume group name and if no volume groups satisfy the following conditions, a volume group is created for each condition and then the specified LUs are allocated to the created volume groups.

If a specified LU is not a virtual LU:

Volume groups with the same drive type exist in the same chassis as the specified LU.

If a specified LU is not a virtual LU for a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system:

Volume groups with the same DP pool exist in the same chassis as the specified LU.

If a specified LU is a virtual LU for a Hitachi AMS 2000 series storage system or an HUS 100 series storage system:

Volume groups with the same drive type and the same DP pool exist in the same chassis as the specified LU.

The new volume groups are given unique names in `vg`*four-digit-number* format.

Options and arguments

LU-name[,*LU-name*...]

Specify the names of the LUs to allocate to the volume group. If the path of the LU is `/dev/enas/lu0F`, specify `lu0F`. Separate multiple LU names with commas (,).

volume-group-name

Specify the name of the volume group as a character string starting with `vg` and containing no more than 16 alphanumeric characters and underscores (_).

Return values

Table 2-406 Return values of the vgrcreate command

Return value	Description
0	Normal termination
1, 10[#]	The command is specified in an incorrect format. Review the command format and execute it again.
10[#], 66[#], 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66[#], 99[#]	The system might be busy or a temporary error might have occurred. Wait a while and then execute the command again. If the error still occurs, contact maintenance personnel.
80	The command has finished executing. However, you need to check the output messages to ensure that there are no configuration issues or problems with the system status.
97, 99[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command terminated abnormally for more than one reason.

vgrdelete (Delete a volume group)

Synopsis

```
vgrdelete [-y] volume-group-name
vgrdelete -h
```

Description

This command can be used in a single-node configuration.

The command deletes an unused volume group from a file system.

Options and arguments

volume-group-name
    Specify the name of the volume group to be deleted.

Return values

Table 2-407 Return values of the vgrdelete command

Return value	Description
0	Normal termination
1	The command is specified in an incorrect format. Review the command format and execute it again.
10, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65	The system might be busy or a temporary error might have occurred. Wait a while and then execute the command again. If the error still occurs, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

vgrexpand (Expand a volume group)

Synopsis

```
vgrexpand [volume-group-name] LU-name[,LU-name...]
vgrexpand -h
```

Description

This command can only be used in a single-node configuration.

The command expands a volume group. You can use the `lulist` command to check the LUs that can be specified.

If you execute this command without specifying a volume group name, the specified LUs are allocated to the volume groups that satisfy the following conditions.

If a specified LU is not a virtual LU:
    Only one volume group with the same drive type exists in the same chassis as the specified LU.

If a specified LU is not a virtual LU for a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system:

Only one volume group with the same DP pool exists in the same chassis as the specified LU.

If a specified LU is a virtual LU for a Hitachi AMS 2000 series storage system or an HUS 100 series storage system:

Only one volume group with the same drive type and the same DP pool exists in the same chassis as the specified LU.

Options and arguments

LU-name[,*LU-name*...]

Specify the names of the LUs to be allocated to the volume group being expanded. If the path of the LU is `/dev/enas/lu0F`, specify `lu0F`. Separate multiple LU names with commas (,).

volume-group-name

Specify the name of the volume group to be expanded.

Return values

Table 2-408 Return values of the vgrexpand command

Return value	Description
0	Normal termination
1, 10#	The command is specified in an incorrect format. Review the command format and execute it again.
10#, 70	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
66, 99#	The system might be busy or a temporary error might have occurred. Wait a while and then execute the command again. If the error still occurs, contact maintenance personnel.
80	The command has finished executing. However, you need to check the output messages to ensure that there are no configuration issues or problems with the system status.
97, 99#	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

The command ended abnormally due to multiple causes.

vgrlist (Display information about volume groups)

Synopsis

```
vgrlist [-c] [--list] [--assign {yes|no}] [volume-group-name]
vgrlist -h
```

Description

This command can be used in a single-node configuration.

The command displays information about a volume group.

If you execute this command without any options or arguments, the command displays information about LUs that have been added recently, with a confirmation message asking whether you want to automatically allocate the LUs to volume groups.

If you choose to automatically allocate the new LUs to volume groups, the LUs are allocated to the volume groups that satisfy the conditions below.

If an added LU is not a virtual LU:

> Only one volume group with the same drive type exists in the same chassis as the added LU.

If an added LU is not a virtual LU for a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system:

> Only one volume group with the same DP pool exists in the same chassis as the added LU.

If an added LU is a virtual LU for a Hitachi AMS 2000 series storage system or an HUS 100 series storage system:

> Only one volume group with the same drive type and the same DP pool exists in the same chassis as the added LU.

If no volume groups satisfy the conditions, volume groups that satisfy the conditions are created. The new volume groups are given unique names in vg*four-digit-number* format.

Options and arguments

`--assign {yes|no}`

> Specify whether to automatically allocate newly added LUs to volume groups without displaying a confirmation message. This option is ignored if you specify a volume group name.

> `yes`
>> Specify this argument to automatically allocate new LUs to volume groups without displaying a confirmation message.

> `no`
>> Specify this argument if you do not want to automatically allocate newly added LUs to volume groups.

`-c`

Specify this option to display volume group information separated by colons (:).

`--list`

Specify this option to display volume group information. If you do not specify a volume group name, the command displays information for all volume groups.

volume-group-name

To view information for a specific volume group, specify a volume group name.

Displayed information

The following table lists the information displayed when you execute the `vgrlist` command.

Table 2-409 Information displayed when executing the vgrlist command

Item	Description
`Volume group`	Displays the name of the volume group.
`Total size(GB)`	Displays the total capacity of the volume group, in gigabytes.
`Free size(GB)`	Displays the amount of free space in the volume group, in gigabytes.

`LU status`	Displays the status of the LUs in the volume group.
	
	`normal`
	
	The LU status is normal.
	
	`error`
	
	An error was detected when attempting to access an LU.

`LUs`	Displays the names of the LUs that constitute the volume group, in ascending order. The drive type appears as a suffix to the LU name, in the following format:
	
	device-file-name(*drive-type*)
	
	The drive types are as follows:
	
	`FC/SAS`
	
	Displayed for an FC drive, an SAS drive, or an internal SAS 7.2K drive.
	
	`SAS7K`
	
	Displayed when the drive type is SAS 7.2K.
	
	`SATA`
	
	Displayed when the drive type is SATA.
	
	`SSD`
	
	Displayed when the drive type is SSD.
	
	`-`

Item	Description
	Displayed in either of the following cases:
	- The LU resides on an external storage system.
	- The device file is in a virtual LU in a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system.
	- When a virtual LU that uses HUS100 series Dynamic Tiering is being used.
	When the LU resides in an external storage system, a hash mark (#) is appended to the end of the LU name.
	For a virtual LU, provided that the FC path is intact, the DP pool ID is appended to the end of the drive type in the following format:
	device-file-name(*drive-type*,`DP` *DP-pool-ID*)
`Model`	Displays the model name of the storage system that contains the LU. If the LU is stored on an internal hard disk, `INTERNAL` is displayed.
`Serial number`	Displays the serial number of the storage system that contains the LU. If the LU is stored on an internal hard disk, a hyphen (-) is displayed.
`Auto assign`	Displays whether the added LUs can be automatically allocated to volume groups.
	`enable`
	Displayed when the new LUs can be automatically allocated.
	`disable`
	Displayed when the new LUs cannot be automatically allocated.

Return values

Table 2-410 Return values of the vgrlist command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review the command format and execute it again.
`10, 70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`65, 66`	The system might be busy or a temporary error might have occurred. Wait a while and then execute the

Return value	Description
	command again. If the error still occurs, contact maintenance personnel.
80	The command has finished executing. However, you need to check the output messages to ensure that there are no configuration issues or problems with the system status.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

Example

To automatically allocate new LUs to a volume group by responding appropriately to the confirmation message:

```
$ sudo vgrlist
Added LUs:
 /dev/enas/lu01 FC/SAS 10.000GB - N0-T002 AMS 85011261 - -
 /dev/enas/lu02 FC/SAS 10.000GB - N0-T002 AMS 85011261 - -

KAQM04226-Q The newly added LU was detected. When performing the automatic
assignment, according to storage system, drive type, and pool number,
volume group is automatically created or expanded. When not performing the
automatic assignment, the LU will be in operation suspension state and it
is necessary to create or expand the volume group manually. Are you sure
you want to perform the automatic assignment? (y/n) y
List of volume groups:
The number of volume groups(1)
 Volume group            : vg0
 Total size(GB)          : 4484
 Free size(GB)           : 3484
 LU status               : normal
 LUs                     : lu00(SATA)
 Model                   : INTERNAL
 Serial number           : -
 Auto assign             : enable

The number of volume groups(2)
 Volume group            : vg0001
 Total size(GB)          : 20
 Free size(GB)           : 19
 LU status               : normal
 LUs                     : lu01(FC/SAS) lu02(FC/SAS)
 Model                   : AMS
 Serial number           : 85011261
 Auto assign             : enable
```

vgrrepair (Repair a volume group)

Synopsis

```
vgrrepair [--list [--lu LU-name]] [-y] volume-group-name
vgrrepair -h
```

Description

This command can be used in single-node configurations.

If a failure occurs on some LUs that compose a volume group, the failed LUs are removed. Before removing the failed LUs, execute this command with the `--list` option to identify the file systems that use the failed LUs, and then delete all of those file systems.

Options and arguments

`--list`

Specify this option to display the failed LUs, and the file systems that use a specified LU. To display the file systems, also specify the `--lu` option together with this option.

Note that, of the displayed items, the following items are not supported.

`List of file systems to which unavailable diff-devs are set:`

`--lu LU-name`

Specifies the name of an LU. This option must be specified with the `--list` option.

Note that, of the displayed items, the following items are not supported.

`List of file systems to which diff-devs that are assigned the specified LU are set:`

volume-group-name

Specify the name of the volume group to be repaired.

Return values

Table 2-411 Return values of the vgrrepair command

Return value	Description
`0`	Normal termination
`1`	The command is specified in an incorrect format. Review the command format and execute it again.
`10, 70`	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
`97, 99`	The error cannot be handled by the system administrator. Contact maintenance personnel.

welcomemsgchange (Change the message displayed at login by using SSH)

Synopsis

```
welcomemsgchange [{-c 'company-name'|-m 'message'|-b}]
welcomemsgchange -h
```

Description

Changes the message displayed when you are logged in by using SSH. The changed message becomes effective the next time you log in by using SSH.

If you omit options, the current message is displayed.

Options and arguments

`-b`

> Specify this to not display the message. In addition, the `Last login` time is not displayed either.

`-c` ' *company-name* '

> Specify this to return the message to the default message and change `{Company Name Here}` in the message to the specified *company-name*. Specify a *company-name*, enclosed in single quotation marks (`'`), within 1,024 characters.
>
> You can use alphanumeric characters, exclamation marks (`!`), ampersands (`&`), left parentheses (`(`), right parentheses (`)`), asterisks (`*`), commas (`,`), hyphens (`-`), periods (`.`), forward slashes (`/`), colons (`:`), semicolons (`;`), left angle brackets (`<`), right angle brackets (`>`), question marks (`?`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), underscores (`_`), left curly brackets (`{`), right curly brackets (`}`), space characters and line feed characters.
>
> The default message is shown below:

```
 Warning Notice!

 This is a {Company Name Here} computer system, which may be accessed and
used only for authorized {Company Name Here} business by authorized
personnel. Unauthorized access or use of this computer system may subject
violators to criminal, civil, and/or administrative action.

 All information on this computer system may be intercepted, recorded,
read, copied, and disclosed by and to authorized personnel for official
purposes, including criminal investigations. Such information includes
sensitive data encrypted to comply with confidentiality and privacy
requirements. Access or use of this computer system by any person, whether
authorized or unauthorized, constitutes consent to these terms. There is
no right of privacy in this system.
```

`-m` ' *message* '

> Specify this if you want to change the message. Specify a *message*, enclosed in single quotation marks (`'`), within 1,024 characters.
>
> You can use alphanumeric characters, exclamation marks (`!`), ampersands (`&`), left parentheses (`(`), right parentheses (`)`), asterisks (`*`), commas (`,`), hyphens (`-`), periods (`.`), forward slashes (`/`), colons (`:`), semicolons (`;`), left angle brackets (`<`), right angle brackets (`>`), question marks (`?`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), underscores (`_`), left curly brackets (`{`), right curly brackets (`}`), space characters and line feed characters.

Return values

Table 2-412 Return values of the welcomemsgchange command

Return value	Description
0	Normal termination
1[#]	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
1[#]	The error cannot be handled by the system administrator. Contact maintenance personnel.

#

The command ended abnormally due to multiple causes.

Example

To change the message displayed when you log in by using SSH:

```
$ sudo welcomemsgchange -m 'Warning Notice!
> This is a Hitachi computer system, which may be accessed and used only
for authorized Hitachi business by authorized personnel. Unauthorized
access or use of this computer system may subject violators to criminal,
civil, and/or administrative action.'
```

wormctl (Manage WORM tasks)

Synopsis
```
wormctl {-S schedule|--immediate} [-o operation]
   [-c auto-commit-period] [-r retention-period]
   {--file-system file-system-name|--system}
wormctl -S schedule --immediate [-o operation]
   [-c auto-commit-period] [-r retention-period]
   {--file-system file-system-name|--system}
wormctl {--delete [-y]|--list}
   {--file-system file-system-name|--system|--all}
wormctl --dispose-list --file-system file-system-name
wormctl -h
```

Description

Managing WORM tasks allows you to perform autocommit processing, which changes files that have not been updated over a specified period of time into WORM files, and auto-deletion processing, which deletes WORM files that have exceeded the retention period. If auto-deletion processing is executed, WORM files that exceed their retention period are deleted, regardless of whether autocommit processing was used to convert the files into WORM files.

You can set up WORM tasks for the system or for individual file systems. WORM tasks can also be executed according to schedules.

WORM tasks can only be set up for file systems that satisfy the following conditions:

- The file system is mounted.
- The file system supports WORM.
- The autocommit function is disabled.#
- The file system is not synchronizing the data with other HDI systems via linked HCP systems.

The following table shows the difference between the autocommit function set for a WORM file system and WORM tasks set by this command.

Table 2-413 Difference between the autocommit function and WORM tasks set by the wormctl command

Item	Occasion to turn a file into a WORM file	Auto-deletion processing	Effect on performance
Autocommit (auto mode)	When the autocommit period has passed	N	N
WORM tasks	When WORM tasks are executed (background execution)	Y	Y

Use this command to execute WORM tasks when you want to automatically delete WORM files whose retention period has expired in a WORM file system that does not use the autocommit function.

Options and arguments

`--all`

Specify this option to target the system and all the file systems.

`-c` *commit-period*

Specify in hours how long to wait until files are turned into WORM files from the time they are last updated. You can specify from 1 to 876000.

If you omit this option, the currently set value is used. The default value is 24 (1 day). Note that this option is ignored if the `-o dispose` option is also specified.

`--delete`

Specify this option to delete WORM tasks.

`--dispose-list`

Specify this option to display the files that were deleted in the last 7 days.

`--file-system` *file-system-name*

Specify this option to target a specific file system.

`--immediate`

>   Specify this option to immediately execute a WORM task.
>
>   If the `--system` option is specified, the WORM task is executed for the file systems on the logged-in node.

`--list`

>   Specify this option to display the WORM task settings.

`-o` *operation*

>   Specify the type of WORM task operation. If you omit this option, the currently set value is used. The default value is `all`.
>
>   For *operation*, you can specify one of the following keywords:
>
>   `all`
>
>   >   The autocommit and auto-dispose functions are executed.
>
>   `commit`
>
>   >   The autocommit function is executed.
>
>   `dispose`
>
>   >   The auto-dispose function is executed.

`-r` *retention-period*

>   Specify in days the retention period that is applied to files for which the autocommit function is executed. You can specify from 1 to 36,500.
>
>   If you omit this information, the currently set value is used. The default value is 10950 (about 30 years). Note that this option is ignored when the `-o dispose` option is also specified.
>
>   To set an infinite retention period, specify `infinite`.

`-S` *schedule*

>   Specify a schedule for executing WORM tasks in one of the following formats:
>
>   `D`-*time*
>
>   >   Use this format to execute the task at a specific time every day. For *time*, specify a value in *hhmm* format.
>
>   `W`-*day-of-week*-*time*
>
>   >   Use this format to execute the task at a specific time on a specific day or on specific days every week. For *day-of-week*, you can specify the keywords `Sun`, `Mon`, `Tue`, `Wed`, `Thu`, `Fri`, and `Sat`. To specify multiple keywords, use a comma (`,`) as a separator. For *time*, specify a value in *hhmm* format.
>
>   `M`-*date*-*time*
>
>   >   Use this format to execute the task at a specific time on a specific day or on specific days every month. For *date*, you can specify from 1 to 31. If you specify a value from 29, 30, or 31, the task is executed only on the months that have the day. To specify multiple days, use a comma (`,`) as a separator. For *time*, specify a value in *hhmm* format.

`--system`

    Specify this option to target the system.

Displayed information

The following table describes the information displayed when this command is executed.

Table 2-414 Information displayed by the wormctl command (when the --list option is specified)

Item	Description
`Target`	Displays the target for which the WORM task is set. If the target is a file system, the file system name is displayed. If the target is the system, `All file systems` is displayed.

`Interval`	Displays the interval over which to execute the WORM task.
	
	`Daily`
	
	    The task is executed every day.
	
	`Weekly`
	
	`Day of week :` *day-of-week*
	
	    The task is executed on specific days every week. The days are indicated with the following keywords: `Sun`, `Mon`, `Tue`, `Wed`, `Thu`, `Fri`, and `Sat`. If multiple keywords are displayed, a comma (`,`) is used as a separator.
	
	`Monthly`
	
	`Day :` *date*
	
	    The task is executed on specific days every month. In *date*, day numbers (1 to 31) are displayed. If multiple day numbers are displayed, a comma (`,`) is used as a separator.

`Time`	Displays the time at which the WORM task is executed in the format `hh:mm`.

`Operation`	Displays the type of WORM task operation.
	
	`all`
	
	    Both the autocommit and auto-dispose functions are executed.
	
	`commit`
	
	    The autocommit function is executed.
	
	`dispose`
	
	    The auto-dispose function is executed.

`Commit period`	Displays in hours how long the autocommit function will be suppressed. If `Operation` is `dispose`, a hyphen (`-`) is displayed.
`Retention period`	Displays in days the retention period. If the infinite retention period is set, `infinite` is displayed. If `Operation` is `dispose`, a hyphen (`-`) is displayed.

Table 2-415 Information displayed by the wormctl command (when the --dispose-list option is specified)

Item	Description
Deletion date and time, and file path	Displays the date and time that the file was deleted and the file path of the file in the following format: `deletion-date (format: MMM DD hh:mm:ss) file-path`

Return values

Table 2-416 Return values of the wormctl command

Return value	Description
0	Normal termination
1, 2	The command is specified in an incorrect format. Review and, if necessary, correct the format, and then retry the operation.
4, 5, 10, 14, 15, 17, 70, 71[#]	The specified value might not be appropriate, or there might be a problem with the system status. Solve the problem by following the instructions in the output message, and then retry the operation, as necessary. If this error occurs repeatedly, contact maintenance personnel.
65, 66, 67	The system might be busy or a temporary error might have occurred. Wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
71[#]	The system might be temporarily disabled for communication. After checking the communication status, wait a while and then retry the operation. If this error occurs repeatedly, contact maintenance personnel.
97, 99	The error cannot be handled by the system administrator. Contact maintenance personnel.

\#

   The command ended abnormally due to multiple causes.

Examples

To set up a WORM task with the following configuration:

- The file system name is `FS_1`.
- The WORM task is executed at 17:00 on weekdays.
- The autocommit period is 96 hours (four days).
- Both the autocommit and auto-dispose functions are executed.

```
$ sudo wormctl -S W-Mon,Tue,Wed,Thu,Fri-1700 --file-system FS_1 -o all -c
96
```

To delete a WORM task that is set up for the file system FS_1:

```
$ sudo wormctl --delete --file-system FS_1
KAQM37303-Q Do you still want to delete the WORM task schedule? (y/n) y
```

Command Reference

Hitachi Data Ingestor CLI Administrator's Guide

3

Command Operations

This chapter describes the operation procedures that use commands. For the syntax of commands, see .

☐ Public key management

☐ Changing the password of the management server

☐ Cluster management

☐ Controlling the OS on a node

☐ Services management

☐ Configuring the system

☐ Managing the real-time scan function

☐ Local user and local group management

☐ File system management

☐ Managing NFS shares

☐ Managing CIFS shares

☐ Managing ACLs

☐ Managing the quotas for each file system

☐ Managing subtree quotas

☐ Management of system settings

☐ Linking to an HCP system

☐ Managing a data import from another file server

☐ Managing data import settings

☐ Managing the NDMP server

☐ Managing tape drives

Public key management

This section explains how to manage public keys.

Registering a public key

This section explains how to use the `sshkeyadd` command to register a public key that will be used for SSH authentication. Public keys are registered for the SSH account `nasroot`. Make sure that there are no more than 128 public keys per node for the SSH2 protocol.

The procedure assumes that a public key is registered under the following conditions:

- The public key file is created on a UNIX machine.
- The name of the public key file is `sshkey.pub`.
- The comment on the public key is `nasroot-key`.
- The host name of the node for which the public key is to be registered is `fshost01`.

1. Use the key creation tool to create the keys (private and public) used for SSH authentication.

   For details on how to perform installation and create keys, see the relevant documentation.

2. Use the `scp` command to transfer the public key file to the SSH account home directory (`/home/nasroot`).

```
$ scp /home/admin/.ssh/sshkey.pub nasroot@fshost01:
sshkey.pub                                       100%  229
0.2KB/s   00:00
```

   Note:
   > A public key file cannot use a name that is already being used by a directory or file name under the home directory of the SSH account.

3. Log in to the target node by using SSH.

```
$ ssh -2 nasroot@fshost01
```

4. Execute the `sshkeyadd` command to register the public key.

   The public key is registered and the specified public key file is deleted from the `/home/nasroot` directory.

```
$ sudo sshkeyadd -2 -c nasroot-key sshkey.pub
```

5. Execute the `sshkeylist` command to confirm that the public key has been registered correctly.

```
$ sudo sshkeylist
User    Ver.    Comment
...
nasroot SSH2    nasroot-key
```

6. Perform steps 2 through 5 on the other node in the cluster.

Note:

If you have transferred the wrong file to the `/home/nasroot` directory, you can use the `rmfile` command to delete the file.

```
$ sudo rmfile ssh-key-nasroot.pub
KAQM16173-Q Do you want to delete the specified file? (y/n) y
```

Changing the password of the management server

This section explains how to change the password of the management server.

To change the authentication password:

1. Execute the `hnasmpasswd` command to change the authentication password that the management server uses for communicating with nodes.
   You are required to enter the new password twice.

```
$ sudo hnasmpasswd
KAQM21005-Q New password:
KAQM21006-Q Re-enter new password:
KAQM21007-I The password was changed successfully.
```

Note:

The character strings you entered in `New password` and `Re-enter new password` will not be displayed.

2. Repeat the first step on the other node so that the password is the same within the cluster.

After completing the settings in the cluster, use the Edit Node dialog box to register the new password with the management server. GUI operations will result in an authentication error unless the same password is registered with the management server and the node.

Cluster management

This section explains how to manage a cluster, nodes, and resource groups.

You can stop and start a cluster during maintenance or troubleshooting. When a cluster is stopped and started, there is no need to stop and start each node in the cluster. If a resource group has been stopped when the cluster is stopped, start the resource group after the cluster is started.

After stopping a cluster while a resource group is running, if you restart the cluster, the resource group will restart automatically. In such a case, the status of the resource group changes in the following order: `Online Ready`, `Initializing`, `Discovery (exclusivity)`, `Online Pending`, and `Online`. If many resources have been registered, it takes several tens of minutes until the status of the resource group changes to `Online/No error`.

Before starting cluster operation:

After the following operations, you must confirm whether a partial blockage has occurred in the resource group:

- When starting a cluster that was stopped while the resource group was running
- When starting a node that was stopped while the resource group was running
- When starting a resource group
- When changing an executing node of a resource group

For details on partial resource group blockage, see Notes on operations (required reading before using commands) on page 1-49.

Stopping a cluster

This section explains how to use the `clstop` command to stop a cluster.

Before performing this procedure, check the information in *Before starting cluster operation:* in Cluster management on page 3-4.

To stop a cluster:

1. Execute the `clstatus` command to check the status of the cluster and resource groups.
   Confirm that the status of the cluster and resource groups is as follows:

   - Cluster status is ACTIVE.

   - Resource group status is Online/No error, Offline/No error, or Online Maintenance/No error.

   ```
   $ sudo clstatus

   --Cluster Status--
   Cluster name     : cluster01
   Cluster status   : ACTIVE

   --Node Status--
   node 0(D710000031)
   Node name        : node0
   Node status      : UP

   node 1(D710000035)
   Node name        : node1
   Node status      : UP

   --Resource Group Status--
   Resource group name     : node0
   Resource group status   : Online/No error
   Running node            : node0

   Resource group name     : node1
   Resource group status   : Online/No error
   Running node            : node1
   ```

2. Execute the `clstop` command to stop the cluster.
   A confirmation message appears. Enter `y` to stop the cluster.

When the `clstop` command is executed, all nodes comprising the cluster and all resource groups running on the nodes are stopped.

```
$ sudo clstop
KAQM06133-Q Performing this operation will stop the services on both
nodes. Are you sure you want to stop the cluster? (y/n) y
```

3. Execute the `clstatus` command to confirm that the cluster is stopped.

   Confirm that `Cluster status` is `INACTIVE`. Note that if you stop the cluster while a resource group is running, `Resource group status` is `Online Ready`.

```
$ sudo clstatus

--Cluster Status--
Cluster name    : cluster01
Cluster status  : INACTIVE
...
--Resource Group Status--
Resource group name      : node0
Resource group status    : Online Ready/No error
Running node              :

Resource group name      : node1
Resource group status    : Online Ready/No error
Running node              :
```

Starting a cluster

This section explains how to use the `clstart` command to start a cluster.

Before performing this procedure, check the information in *Before starting cluster operation:* in [Cluster management on page 3-4](#).

To start a cluster:

1. Execute the `clstatus` command to confirm that the target cluster is stopped.
   Confirm that `Cluster status` is `INACTIVE`.

```
$ sudo clstatus

--Cluster Status--
Cluster name    : cluster01
Cluster status  : INACTIVE

--Node Status--
node 0(D710000031)
Node name       : node0
Node status     : INACTIVE

node 1(D710000035)
Node name       : node1
Node status     : INACTIVE

--Resource Group Status--
Resource group name      : node0
Resource group status    : Online Ready/No error
Running node              :
```

```
Resource group name      : node1
Resource group status    : Online Ready/No error
Running node             :
```

2. Execute the `clstart` command to start the cluster.

   When the `clstart` command is executed, all nodes comprising the cluster are started. When a node is started, its resource groups can also be started.

```
$ sudo clstart
```

3. Start resource groups.

   This step is necessary if resource groups had been stopped when the cluster was stopped. For details on how to start resource groups, see .

4. Execute the `clstatus` command to confirm that the cluster, nodes, and resource groups are running correctly.

   Confirm that the status of the cluster, nodes, and resource groups are as follows:

   ○ `Cluster status` is `ACTIVE`.

   ○ `Node status` is `UP`.

   ○ `Resource group status` is `Online/No error`.

```
$ sudo clstatus

--Cluster Status--
Cluster name     : cluster01
Cluster status   : ACTIVE

--Node Status--
node 0(D710000031)
Node name        : node0
Node status      : UP

node 1(D710000035)
Node name        : node1
Node status      : UP

--Resource Group Status--
Resource group name      : node0
Resource group status    : Online/No error
Running node             : node0

Resource group name      : node1
Resource group status    : Online/No error
Running node             : node1
```

Stopping a node

This section explains how to use the `ndstop` command to stop a node.

The procedure assumes that the node `node1` is stopped.

To stop a node:

1. Execute the `clstatus` command to check the status of the target node and the resource groups on the node.
   Confirm that the status of the nodes and resource groups are as follows:

   - `Node status` of the target node is `UP`.

   - `Resource group status` of each resource group on the target node is `Online/No error`, `Offline/No error`, or `Online Maintenance/No error`.

```
$ sudo clstatus

--Cluster Status--
Cluster name     : cluster01
Cluster status   : ACTIVE

--Node Status--
node 0(D710000031)
Node name        : node0
Node status      : UP

node 1(D710000035)
Node name        : node1
Node status      : UP

--Resource Group Status--
Resource group name      : node0
Resource group status    : Online/No error
Running node              : node0

Resource group name      : node1
Resource group status    : Online/No error
Running node              : node1
```

2. Execute the `ndstop` command to stop the node.

   A confirmation message appears. Enter `y` to stop the node.

   When the `ndstop` command is executed, the node is stopped, and the resource groups running on the node are failed over to the other node. However, when a node for which two resource groups are running is stopped, the resource groups moved over due to failover are stopped, and the previously running resource groups are failed over to the other node.

```
$ sudo ndstop node1
KAQM06134-Q Performing this operation might stop the services on the node.
Are you sure you want to stop the node? (y/n) y
```

3. Execute the `clstatus` command to confirm that the node is stopped.

   Confirm that `Node status` is `INACTIVE`.

```
$ sudo clstatus

...

--Node Status--
...
node 1(D710000035)
Node name        : node1
Node status      : INACTIVE
```

Command Operations

```
--Resource Group Status--
...

Resource group name    : node1
Resource group status  : Online/No error
Running node            : node0
```

Starting a node

This section explains how to use the `ndstart` command to start a node.

This procedure assumes that the name of the node you want to start is `node1`.

To start a node:

1. If the node you want to start is not the node that the user is logged in to, execute the `peerstatus` command, and then verify that the node OS is running normally.
   Verify that `BOOT COMPLETE` is displayed.

   ```
   $ sudo peerstatus
   BOOT COMPLETE
   ```

2. Execute the `ndstatus` command to confirm that the target node is stopped.
   Confirm that `Node status` is `INACTIVE`.

   ```
   $ sudo ndstatus node1

   --Node Status--
   node 1(D710000035)
   Node name      : node1
   Node status    : INACTIVE
   ```

3. Execute the `ndstart` command to start the node.

   ```
   $ sudo ndstart node1
   ```

4. Execute the `ndstatus` command to confirm that the node is running correctly.
   Confirm that `Node status` is `UP`.

   ```
   $ sudo ndstatus node1

   --Node Status--
   node 1(D710000035)
   Node name      : node1
   Node status    : UP
   ```

Stopping a resource group

This section explains how to use the `rgstop` command to stop a resource group.

The procedure assumes that the resource group `node1` is stopped.

To stop a resource group:

1. Execute the `rgstatus` command to view the status of the target resource group.
   Confirm that `Resource group status` is `Online/No error`, `Online Ready/No error`, or `Online Maintenance/No error`.

```
$ sudo rgstatus node1

--Resource Group Status--
Resource group name     : node1
Resource group status   : Online/No error
Running node            : node1
```

2. Execute the `rgstop` command to stop the resource group.
   A confirmation message appears. Enter `y` to stop the resource group.

```
$ sudo rgstop node1
KAQM06135-Q Performing this operation will stop the services. Are you sure
you want to stop the resource group? (y/n) y
```

3. Execute the `rgstatus` command to confirm that the resource group is stopped.
   Confirm that `Resource group status` is `Offline/No error`.

```
$ sudo rgstatus node1

--Resource Group Status--
Resource group name     : node1
Resource group status   : Offline/No error
Running node            :
```

Starting a resource group

This section explains how to use the `rgstart` command to start a resource group.

Before performing this procedure, check the information in *Before starting cluster operation:* in . The procedure assumes that the resource group `node1` is started.

To start a resource group:

1. Execute the `clstatus` command to confirm that the status of the cluster, nodes, and resource groups are as follows:

   ○ `Cluster status` is `ACTIVE`.

   ○ `Node status` of the node that contains the resource group to be started is `UP`.

   ○ `Resource group status` of the resource group to be started is `Offline/No error` or `Online Ready/No error`.

```
$ sudo clstatus

--Cluster Status--
Cluster name     : cluster01
Cluster status   : ACTIVE

--Node Status--
node 0(D710000031)
Node name         : node0

Node status       : UP

node 1(D710000035)
Node name         : node1
Node status       : UP

--Resource Group Status--
Resource group name      : node0
Resource group status    : Online/No error
Running node              : node0

Resource group name      : node1
Resource group status    : Offline/No error
Running node              :
```

2. Execute the `rgstart` command to start the target resource group.

   If many resources have been registered, it may take tens of minutes until the resource group is placed in the `Online/No error` status and becomes available.

   ```
   $ sudo rgstart node1
   ```

3. Execute the `rgstatus` command to confirm that the resource group is running correctly.

   Confirm that `Resource group status` is `Online/No error`.

   ```
   $ sudo rgstatus node1

   --Resource Group Status--
   Resource group name      : node1
   Resource group status    : Online/No error
   Running node              : node1
   ```

Changing the execution node of a resource group

This section explains how to use the `rgmove` command to perform a failover or failback that changes the resource group execution node for node maintenance or troubleshooting.

To change the resource group execution node when an NFS share has been created, the NFS service must be running on the other node, which will become the execution node.

Before performing this procedure, check the information in *Before starting cluster operation:* in .

The procedure assumes that the execution node is changed for the resource group node1.

To change the resource group execution node:

1. Execute the `clstatus` command to check the status of the node that will become the resource group execution node, and the status of the target resource group.

   Confirm that the node status and the resource group status are as follows:

   ○ `Node status` of the node that will become the execution node is `UP`.

   ○ `Resource group status` of the target resource group is `Online/No error` or `Online Maintenance/No error`.

```
$ sudo clstatus

--Cluster Status--
Cluster name    : cluster01
Cluster status  : ACTIVE

--Node Status--
node 0(D710000031)
Node name       : node0
Node status     : UP

node 1(D710000035)
Node name       : node1
Node status     : UP

--Resource Group Status--
Resource group name     : node0
Resource group status   : Online/No error
Running node             : node0

Resource group name     : node1
Resource group status   : Online/No error
Running node             : node1
```

2. Execute the `rgmove` command to change the resource group execution node.

   A confirmation message appears. Enter `y` to change the node the resource group is executed on.

   If many resources have been registered, it may take tens of minutes until the processing is completed.

```
$ sudo rgmove node1
KAQM06136-Q Performing this operation will temporarily stop the services.
Are you sure you want to change the execution node of the resource group?
(y/n) y
```

3. Execute the `clstatus` command to confirm that the resource group execution node has been changed.

   Confirm that the name of the new resource group execution node is displayed as `Running node` of the target resource group.

```
$ sudo clstatus

...
--Resource Group Status--
...
Resource group name     : node1
```

```
Resource group status   : Online/No error
Running node             : node0
```

Disabling resource group monitoring

This section explains how to use the `rgmon` command to disable monitoring of a resource group.

The procedure assumes that monitoring is disabled for the resource group `node1`.

To disable resource group monitoring:

1. Execute the `rgstatus` command to check the status of the resource group for which you want to disable monitoring.
   Confirm that `Resource group status` is `Online/No error`.

   ```
   $ sudo rgstatus node1

   --Resource Group Status--
   Resource group name      : node1
   Resource group status    : Online/No error
   Running node             : node1
   ```

2. Execute the `rgmon` command to disable monitoring of the resource group.

   ```
   $ sudo rgmon -off node1
   ```

3. Execute the `rgstatus` command to confirm that monitoring of the resource group has been disabled.
   Confirm that `Resource group status` is `Online Maintenance/No error`.

   ```
   $ sudo rgstatus node1

   --Resource Group Status--
   Resource group name      : node1
   Resource group status    : Online Maintenance/No error
   Running node             : node1
   ```

Restarting resource group monitoring

This section explains how to use the `rgmon` command to restart monitoring of a resource group.

The procedure assumes that monitoring is restarted for the resource group `node1`.

To restart resource group monitoring:

1. Execute the `rgstatus` command to check the status of the resource group for which you want to restart monitoring.
   Confirm that `Resource group status` is `Online Maintenance/No error`.

```
$ sudo rgstatus node1

--Resource Group Status--
Resource group name      : node1
Resource group status    : Online Maintenance/No error
Running node              : node1
```

2. Execute the `rgmon` command to restart monitoring of the resource group.

```
$ sudo rgmon -on node1
```

3. Execute the `rgstatus` command to confirm that monitoring of the
   resource group has been restarted.
   Confirm that `Resource group status` is `Online/No error`.

```
$ sudo rgstatus node1

--Resource Group Status--
Resource group name      : node1
Resource group status    : Online/No error
Running node              : node1
```

Changing failover-related timeout values

This section explains how to use the `clctl` command to change the timeout
values related to failing over or failing back.

The examples provided assume that the current timeout values are changed
as follows:

- Startup timeout value is to be changed to 45 minutes.
- Stoppage timeout value is to be changed to 45 minutes.

To change the timeout values:

1. Execute the `clctl` command to check the current timeout values.

```
$ sudo clctl
Timeout value for the processing to start the resource group during
failover: 0
Timeout value for the processing to stop the resource group during
failover: 60
Time until a failover starts after a failure is detected on the heartbeat
LAN: 60
Time until a failover starts after a link-down error is detected: 60
Resource group start policy if an error occurs with a resource:
ignore_resource_error
```

2. Execute the `clctl` command to change the timeout values for failing over
   or failing back.

```
$ sudo clctl -s 45 -e 45
```

3. Execute the `clctl` command to confirm that the timeout values have
   been changed correctly.

```
$ sudo clctl
Timeout value for the processing to start the resource group during
failover: 45
Timeout value for the processing to stop the resource group during
failover: 45
Time until a failover starts after a failure is detected on the heartbeat
LAN: 60
Time until a failover starts after a link-down error is detected: 60
Resource group start policy if an error occurs with a resource:
ignore_resource_error
```

4. Perform step 3 on the other node in the cluster.

Controlling the OS on a node

This section explains how to control the OS on a node.

Stopping the OS on a node

This section explains how to use the `nasshutdown` command to stop the OS on a node.

The procedure assumes that the following conditions regarding the OS of the node to be stopped

- The name of the node for which the OS is to be stopped is `node0`.
- The name of the other node in the cluster is `node1`.

To stop the OS:

1. Execute the `rgmove` command to change the execution node of the resource group to `node1`.

   For details on how to change the execution node of a resource group, see Changing the execution node of a resource group on page 3-11.

2. Use the `ndstop` command to stop the node.

   For details on how to stop the node, see Stopping a node on page 3-7.

3. Execute the `ndstatus` command to check the status of the node.

   Confirm that `Node status` is `INACTIVE` or `UNKNOWN`.

```
$ sudo ndstatus node0

--Node Status--
node 0(D710000031)
Node name       : node0
Node status     : INACTIVE
```

4. Execute the `nasshutdown` command to stop the OS on the node.

   A confirmation message appears. Enter `y` to stop the OS.

```
$ sudo nasshutdown
KAQM25413-Q Do you want to stop the OS? (y/n) y
```

If the OS of the node was stopped and then restarted the OS, use the `ndstart` command to start `node0`. Then make the necessary changes, such as changing the execution node by using the `rgmove` command. For details on how to start a node, see Starting a node on page 3-9.

Restarting the OS on a node

This section explains how to use the `nasreboot` command to restart the OS on a node.

The procedure assumes that the following conditions regarding the OS of the node to be restarted

- The name of the node for which the OS is to be restarted is `node0`.
- The name of the other node in the cluster is `node1`.

To restart the OS:

1. Execute the `rgmove` command to change the execution node of the resource group to `node1`.

   For details on how to change the execution node of a resource group, see Changing the execution node of a resource group on page 3-11.

2. Use the `ndstop` command to stop the node.

   For details on how to stop the node, see Stopping a node on page 3-7.

3. Execute the `ndstatus` command to check the status of the node.

   Confirm that `Node status` is `INACTIVE` or `UNKNOWN`.

   ```
   $ sudo ndstatus node0

   --Node Status--
   node 0(D710000031)
   Node name       : node0
   Node status     : INACTIVE
   ```

4. Execute the `nasreboot` command to restart the OS on the node.

   A confirmation message appears. Enter `y` to restart the OS.

   ```
   $ sudo nasreboot
   KAQM25414-Q Do you want to restart the OS? (y/n) y
   ```

5. After the OS restarts, execute the `ndstart` command to start `node0`.

   For details on how to start a node, see Starting a node on page 3-9.

6. Execute the `rgmove` command to change the execution node of the resource group to `node0`.

Starting the OS on the other node in the cluster

This section explains how to use the `nasboot` command to start the OS on the other node in the cluster from the node you are logged in to.

For details on the `nasboot` command, see nasboot (Start the OS on the other node in the cluster) on page 2-473.

To start the OS on the other node:

1. Execute the `peerstatus` command to confirm that the hardware on the other node has been turned off.
   Confirm that `OFF` is displayed.

```
$ sudo peerstatus
OFF
```

2. Execute the `nasboot` command to start the OS on the other node in the cluster.

```
$ sudo nasboot
```

3. Execute the `peerstatus` command to check the node status.

   Make sure that `BOOT COMPLETE` is displayed for the node status. After the OS starts, the node status will change in the order `OFF`, `STOP`, `BOOT START`, and then `BOOT COMPLETE`. If `OFF`, `STOP`, or `BOOT START` is displayed, wait a while, and then check the node status again.

```
$ sudo peerstatus
BOOT COMPLETE
```

Note:

    You can also use the GUI to check whether the OS on the node has started normally. Note, however, that when using the GUI, you need to refresh the displayed information.

Services management

This section explains how to manage services.

Stopping a service

This section explains how to use the `svctl` command to stop a service.

For services that you want to stop, you must request the clients using those services to stop accessing the file share.

The procedure assumes that the CIFS service is stopped.

To stop a service:

1. Execute the `svstatus` command to check the operating status of a CIFS service.
   Confirm that `Status` is `Running`, `Down`, `Failover` or `Offline`.

```
$ sudo svstatus -s cifs
Service name : CIFS
Status       : Running
Information  : -
```

2. Execute the `svctl` command to stop the CIFS service.

A confirmation message appears. Enter `y` to stop the CIFS service.

```
$ sudo svctl -s cifs --stop
KAQM16130-Q Are you sure you want to stop the specified service? (y/n) y
```

3. Execute the `svstatus` command to confirm that the CIFS service has been stopped.
   Confirm that `Status` is `Stopped`.

```
$ sudo svstatus -s cifs
Service name : CIFS
Status       : Stopped
Information  : -
```

Starting a service

This section explains how to use the `svctl` command to start a service.

The procedure assumes that the CIFS service is started.

To start a service:

1. Execute the `svstatus` command to check the operating status of a CIFS service.
   Confirm that `Status` is `Stopped`.

```
$ sudo svstatus -s cifs
Service name : CIFS
Status       : Stopped
Information  : -
```

2. Execute the `svctl` command to start the CIFS service.

```
$ sudo svctl -s cifs --start
```

3. Execute the `svstatus` command to confirm that the CIFS service has been started.
   Confirm that `Status` is `Running`.

```
$ sudo svstatus -s cifs
Service name : CIFS
Status       : Running
Information  : -
```

Restarting a service

This section explains how to use the `svctl` command to restart a service.

For services that you want to restart, you must request the clients using those services to stop accessing the file share.

The procedure assumes that the CIFS service is restarted.

To restart a service:

1. Execute the `svctl` command to restart a CIFS service.

    A confirmation message appears. Enter `y` to restart the CIFS service.

    ```
    $ sudo svctl -s cifs --restart
    KAQM16131-Q Are you sure you want to restart the specified service? (y/n) y
    ```

2. Execute the `svstatus` command to confirm that the CIFS service has been started.

    Confirm that `Status` is `Running`.

    ```
    $ sudo svstatus -s cifs
    Service name : CIFS
    Status       : Running
    Information  : -
    ```

Switching the automatic startup settings for a service

This section explains how to use the `svstartupset` command to switch the automatic startup settings for a service.

To switch the automatic startup settings for a service:

1. Execute the `svstartuplist` command to check the automatic startup settings for the CIFS service.

    Confirm that `Automatic startup` is `Off`.

    ```
    $ sudo svstartuplist -s cifs
    Service name      : CIFS
    Automatic startup : Off
    ```

2. Execute the `svstartupset` command to switch the automatic startup settings for the CIFS service.

    ```
    $ sudo svstartupset -s cifs --on
    KAQM16189-I An automatic start setting for a service on this node was
    changed. Confirm that the setting is consistent in the cluster.
    ```

3. Execute the `svstartuplist` command to make sure that the automatic startup settings for the CIFS service have changed.

    Confirm that `Automatic startup` is `On`.

    ```
    $ sudo svstartuplist -s cifs
    Service name      : CIFS
    Automatic startup : On
    ```

4. Perform steps 1 through 3 on the other node in the cluster.

Changing the FTP service configuration

This section explains how to use the `ftpset` command to change the FTP service configuration.

The procedure assumes that the FXP function is enabled.

To change the FTP service configuration:

1. Execute the `ftpget` command to check the current FTP service configuration.
   Make sure that `Off` is displayed for `FXP`.

   ```
   $ sudo ftpget
   FXP : Off
   ```

2. Execute the `ftpset` command to enable the FXP function.

   ```
   $ sudo ftpset --fxp on
   ```

3. Execute the `ftpget` command to make sure that the FTP service configuration has changed.
   Make sure that `On` is displayed for `FXP`.

   ```
   $ sudo ftpget
   FXP : On
   KAQM16169-I The configuration for the FTP service has been modified.
   Restart the FTP service. Rebooting the OS will not apply the changes.
   ```

4. Restart the FTP service.
5. Perform steps 1 to 4 on the other node in the cluster.

Configuring the system

This section explains how to configure the system.

Before managing an interface:

Before managing an interface, be aware of the following:

- Whenever interface settings are to be changed, all clients accessing the HDI system via 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 via that interface, even if you do not change the virtual IP address. Also, for an interface that uses both IPv4 and IPv6 concurrently, you will be temporarily unable to communicate or use any services via that interface if either IPv4 or IPv6 IP addresses are changed.
- Make sure that the OS is running on both nodes, and the cluster is either is running normally or was stopped without any problems.
- Before managing the interface of a data port, you must do the following:

  When adding or changing the 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 the running 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.

When changing the fixed IP address, netmask, or MTU value:

You need to stop the resource groups on both nodes.

- To change the fixed IP address of the management port interface, you must first stop the resource groups on both nodes and the cluster.

  After you have edited the interface, start the cluster and resource groups that you stopped.

  For details on how to stop resource groups, see Stopping a resource group on page 3-9. For details on how to start resource groups, see Starting a resource group on page 3-10.

  For details on how to stop a cluster, see Stopping a cluster on page 3-5. For details on how to start a cluster, see Starting a cluster on page 3-6.

- Even if there are no virtual IP addresses for the running resource groups, the CIFS service will not stop but CIFS access is no longer available. To access CIFS, specify a virtual IP address.

- 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, be sure to also change the peripheral equipment and client MTU values to the same values. For details on 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 you change the switch settings, 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 on how to disable the monitoring of resource groups, see Disabling resource group monitoring on page 3-13. For details on how to restart the monitoring of resource groups, see Restarting resource group monitoring on page 3-13.

- If an interface IP address is changed 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.

- If you change the IP address for a management port or data port being used for a connection, upon the command being executed without any problems, the SSH connection will be disconnected. Use the IP address

that was just set and re-establish the connection. Because the old IP address will no longer be available for connection, you must be careful when changing the IP address.

Adding an interface

This section explains how to use the `ifadd` command to add an interface to a data port.

The procedure assumes that an interface for the data port `eth12` is added under the following conditions:

- The fixed IP addresses are `10.200.100.1` and `10.200.100.2`.
- The virtual IP addresses are `10.200.100.3` and `10.200.100.4`.
- The netmask is `255.255.255.0`.
- The MTU value is `2000`.

To add an interface:

1. Execute the `iflist` command to check the current interface configuration.
   Make sure that `(Not used)` appears in the name field of the interface you want to add.

```
$ sudo iflist -v
Interface        : eth12(Not used)

Interface        : eth13(Not used)

Interface        : eth14(Not used)

Interface        : eth15(Not used)

Interface        : mng0
node 0(D79RMPBX)
 [IPv4]
 Fixed IP addr   : 192.168.3.100
 Service IP addr : 192.168.3.101
 Netmask         : 255.255.0.0
node 1(DJ8RMPBX)
 [IPv4]
 Fixed IP addr   : 192.168.3.110
 Service IP addr : 192.168.3.111
 Netmask         : 255.255.0.0
MTU              : 1500
```

2. Execute the `ifadd` command to add the interface.

```
$ sudo ifadd -a 10.200.100.1:10.200.100.2 -s 10.200.100.3:10.200.100.4 -n
255.255.255.0 -m 2000 eth12
```

3. Execute the `iflist` command to confirm that the interface has been added correctly.

```
$ sudo iflist eth12
Interface        : eth12
node 0(D79RMPBX)
 [IPv4]
```

```
 Fixed IP addr   : 10.200.100.1
 Service IP addr : 10.200.100.3
 Netmask         : 255.255.255.0
node 1(DJ8RMPBX)
 [IPv4]
 Fixed IP addr   : 10.200.100.2
 Service IP addr : 10.200.100.4
 Netmask         : 255.255.255.0
MTU              : 2000
```

Changing an interface

This section explains how to use the `ifedit` command to change an interface set for a data port or a management port.

To change the fixed IP addresses of a data port used when connecting to the management server, first reconnect the management server to the management port or to another data port, and then change the fixed IP addresses.

The procedure assumes that the interface for the data port `eth12` is changed as follows:

- Change the fixed IP addresses to `172.19.23.31` and `172.19.23.32`.
- Change the virtual IP addresses to `172.19.23.33` and `172.19.23.34`.
- Change the MTU value to `9,216`.

To change an interface:

1. Execute the `iflist` command to check the settings for the interface you are changing.

```
$ sudo iflist eth12
Interface        : eth12
node 0(D79RMPBX)
 [IPv4]
 Fixed IP addr   : 10.200.100.1
 Service IP addr : 10.200.100.3
 Netmask         : 255.255.255.0
node 1(DJ8RMPBX)
 [IPv4]
 Fixed IP addr   : 10.200.100.2
 Service IP addr : 10.200.100.4
 Netmask         : 255.255.255.0
MTU              : 2000
```

2. Execute the `ifedit` command to change the interface.

```
$ sudo ifedit -a 172.19.23.31:172.19.23.32 -s 172.19.23.33:172.19.23.34 -m
9216 eth12
```

Note:

If you are changing the settings for the interface being used for an SSH connection, you are disconnected when you execute the `ifedit` command. Log in again by using the SSH account to perform the next steps.

3. Execute the `iflist` command to confirm that the interface has been changed correctly.

```
$ sudo iflist eth12
Interface       : eth12
node 0(D79RMPBX)
 [IPv4]
 Fixed IP addr   : 172.19.23.31
 Service IP addr : 172.19.23.33
 Netmask         : 255.255.255.0
node 1(DJ8RMPBX)
 [IPv4]
 Fixed IP addr   : 172.19.23.32
 Service IP addr : 172.19.23.34
 Netmask         : 255.255.255.0
MTU             : 9216
```

If you have changed the fixed IP address of the data port used for connection with the management server, re-register the new IP address by using the Edit Node dialog box.

If you change the MTU value, execute `ping` or other commands from the client, to make sure that the client can communicate with the node at the MTU value.

If the client cannot communicate with the node even though the MTU value is set correctly, there might be a problem with the peripherals or the client. Check the settings of the peripherals and the client.

Adding routing information

This section explains how to use the `routeadd` command to add routing information to the interfaces of the management ports and the data ports.

The same routing information is set on all nodes in the cluster. Do not set more than 512 routes, including both IPv4 and IPv6 routes, in a cluster.

The procedure assumes that the following routing information is added to the data port `eth12`:

- The routing target address is `172.16.3.0`.
- The netmask is `255.255.255.0`.
- The gateway address is `172.16.3.1`.

To add routing information:

1. Execute the `routelist` command to check the current routing information.

```
$ sudo routelist
[IPv4]
Target          Netmask         Gateway         Method Type    MSS    Iface
default         0.0.0.0         192.168.3.1     Allow  default  -      mng0
```

2. Execute the `routeadd` command to add the routing information.

```
$ sudo routeadd -t net -d 172.16.3.0 -n 255.255.255.0 -g 172.16.3.1 eth12
```

3. Execute the `routelist` command to confirm that the routing information has been added correctly.

```
$ sudo routelist
[IPv4]
Target          Netmask        Gateway        Method Type    MSS   Iface
172.16.3.0      255.255.255.0  172.16.3.1     Allow  net     -     eth12
default         0.0.0.0        192.168.3.1    Allow  default -     mng0
```

Changing the setting for reverse path filtering

This section explains how to use the `routefilterctl` command to change the setting for reverse path filtering.

The procedure assumes that the reverse path filtering function is disabled.

To change the setting for reverse path filtering:

1. Execute the `routefilterctl` command to check the current setting for reverse path filtering.

```
$ sudo routefilterctl
On
```

2. Execute the `routefilterctl` command to disable the reverse path filtering function.

```
$ sudo routefilterctl --off
```

3. Execute the `routefilterctl` command to make sure that the setting for reverse path filtering has changed.

```
$ sudo routefilterctl
Off
```

Editing the interface information for BMC ports

This section explains how to use the `bmcctl` command to set and change the interfaces for BMC ports.

The procedure assumes that the interface for BMC port `bmc0` is set under the following conditions:

- The fixed IP addresses are `172.19.23.31` and `172.19.23.32`.
- The netmask is `255.255.255.0`.

To set an interface for a BMC port:

1. Execute the `bmcctl` command to set an interface for the BMC port.

```
$ sudo bmcctl -a 172.19.23.31:172.19.23.32 -n 255.255.255.0
```

2. Execute the `bmcctl` command to confirm that the interface for the BMC port has been set correctly.

```
$ sudo bmcctl
Interface         : bmc0
node 0(D710000031)
 Fixed IP addr    : 172.19.23.31
 Netmask          : 255.255.255.0
 Gateway          : 0.0.0.0
node 1(D710000035)
 Fixed IP addr    : 172.19.23.32
 Netmask          : 255.255.255.0
 Gateway          : 0.0.0.0
```

Editing the interface information for private maintenance ports

This section explains how to use the `pmctl` command to set and change interfaces of the private maintenance ports.

The procedure assumes that the interface for private maintenance port `pm0` is set under the following conditions:

- The fixed IP addresses are `172.23.211.31` and `172.23.211.32`.
- The netmask is `255.255.255.0`.

To edit the interface information for private maintenance ports:

1. Execute the `pmctl` command to set an interface for the private maintenance port.

```
$ sudo pmctl -a 172.23.211.31 -n 255.255.255.0 pm0
```

2. Execute the `pmctl` command to confirm that the interface for the private maintenance port has been set correctly.

```
$ sudo pmctl -p v4
Interface         : pm0
 [IPv4]
 Fixed IP addr    : 172.23.211.31
 Netmask          : 255.255.255.0
```

3. Log in to the other node.

4. Execute the `pmctl` command to set an interface for the private maintenance port.

```
$ sudo pmctl -a 172.23.211.32 -n 255.255.255.0 pm0
```

5. Execute the `pmctl` command to confirm that the interface for the private maintenance port has been set correctly.

```
$ sudo pmctl
Interface         : pm0
 [IPv4]
 Fixed IP addr    : 172.23.211.32
 Netmask          : 255.255.255.0
```

Viewing the network settings

This section explains how to use the `nasnetstat` command to view the network settings.

The procedure assumes that the settings for all network interfaces are checked.

To check the network settings:

1. Execute the `nasnetstat` command to view the network settings.

   The displayed information is added to the beginning of the log file. If the addition of information causes the log file to exceed 1 MB, some entries at the end of the log file are deleted so that the log file size does not exceed 1 MB.

```
$ sudo nasnetstat -i
Kernel Interface table
Iface    MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR
Flg
49-04-tap  1500 0       176       0       0 0          171       0
1        0 BMRU
49-05-tap  1500 0         8       0       0 0          749       0
2        0 BMRU
agr0       9000 0  404357751       0       0 0    124192563       0
0        0 BMPmRU
agr0-br    9000 0  218938495       0       0 0    124127221       0
0        0 BMRU
agr0-br:0  9000 0       - no statistics available -
BMRU
eth12      1500 0         0       0       0 0            0       0
0        0 BMU
eth13      1500 0         0       0       0 0            0       0
0        0 BMU
eth14      1500 0         0       0       0 0            0       0
0        0 BMU
eth15      1500 0    241636       0       0 0         8147       0
0        0 BMPRU
eth16      9000 0  106634677       0       0 0     30325494       0
0        0 BMsRU
eth17      9000 0  102402784       0       0 0     29671240       0
0        0 BMsRU
eth18      9000 0  100621296       0       0 0     32322717       0
0        0 BMsRU
eth19      9000 0   94698994       0       0 0     31873112       0
0        0 BMsRU
eth15-br   1500 0    240578       0       0 0         7956       0
0        0 BMRU
eth15-br:0 1500 0       - no statistics available
-                     BMRU
hb0        1500 0   2426789       0       0 0      2427610       0
0        0 BMRU
hb0-br     1500 0     15690       0       0 0        15197       0
0        0 BMRU
lo        16436 0   7753309       0       0 0      7753309       0
0        0 LRU
mng0       1500 0   5405874       0       0 0      4212525       0
0        0 BMPRU
mng0-br    1500 0   5368029       0       0 0      4212517       0
0        0 BMRU
mng0-br:0  1500 0       - no statistics available -
BMRU
pm0        1500 0         0       0       0 0            0       0
0        0 BMU
```

2. From the **List of RAS Information** page (for `Batch-download`) of the Check for Errors dialog box, acquire the log file.

   This step is necessary if you want to save the log file output when the `nasnetstat` command is executed. Download all log data to acquire the log files. For details on how to download log files, see the *Troubleshooting Guide*.

   Note:
   The `eraselog` command can be used to delete log files.

```
$ sudo eraselog
```

Checking the connection with a specified host

This section explains how to use the `nasping` command to check the connection between the node that you are logged in to and a specified host.

The procedure assumes that the connection to the host `host01` is checked.

To check the connection to a specified host:

1. Execute the `nasping` command to confirm the connection to the host specified in the command.

   The displayed information is added to the beginning of the log file. If the addition of information causes the log file to exceed 1 MB, some entries at the end of the log file are deleted so that the log file size does not exceed 1 MB.

```
$ sudo nasping host01
PING host01 (10.213.89.211) 56(84) bytes of data.
64 bytes from host01 (10.213.89.211): icmp_seq=1 ttl=64 time=0.373 ms
64 bytes from host01 (10.213.89.211): icmp_seq=2 ttl=64 time=0.402 ms
64 bytes from host01 (10.213.89.211): icmp_seq=3 ttl=64 time=0.272 ms
64 bytes from host01 (10.213.89.211): icmp_seq=4 ttl=64 time=0.249 ms
64 bytes from host01 (10.213.89.211): icmp_seq=5 ttl=64 time=0.418 ms
64 bytes from host01 (10.213.89.211): icmp_seq=6 ttl=64 time=0.331 ms
64 bytes from host01 (10.213.89.211): icmp_seq=7 ttl=64 time=0.252 ms
64 bytes from host01 (10.213.89.211): icmp_seq=8 ttl=64 time=0.483 ms
64 bytes from host01 (10.213.89.211): icmp_seq=9 ttl=64 time=0.402 ms
64 bytes from host01 (10.213.89.211): icmp_seq=10 ttl=64 time=0.264 ms

--- host01 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9007ms
rtt min/avg/max/mdev = 0.249/0.344/0.483/0.081 ms
```

2. From the **List of RAS Information** page (for `Batch-download`) of the Check for Errors dialog box, acquire the log file and packet dump file.

   This step is necessary if you want to save the log file output when the `nasping` command is executed. Download all log data to acquire the log files. For details on how to download log files, see the *Troubleshooting Guide*.

   Note:
   The `eraselog` command can be used to delete log files.

```
$ sudo eraselog
```

Viewing the path that leads to a specified host

This section explains how to use the `nastraceroute` command to view the path to a specified host from the node that you are logged in to.

The procedure assumes that the path to the host `host01` is displayed with IP addresses only.

To check the path to a specified host:

1. Execute the `nastraceroute` command to view information about the path to the host specified in the command.

    The displayed information is added to the beginning of the log file. If the addition of information causes the log file to exceed 1 MB, some entries at the end of the log file are deleted so that the log file size does not exceed 1 MB.

    ```
    $ sudo nastraceroute -n host01
    traceroute to host01 (10.213.89.211), 30 hops max, 40 byte packets
     1  10.213.89.211  0.333 ms  0.328 ms  0.325 ms
    ```

2. From **List of RAS Information** page (for `Batch-download`) of the Check for Errors dialog box, acquire the log file and packet dump file.

    This step is necessary if you want to save the log file output when the `nastraceroute` command is executed. Download all log data to acquire the log files. For details on how to download log files, see the *Troubleshooting Guide*.

Note:

The `eraselog` command can be used to delete log files.

```
$ sudo eraselog
```

Checking the correspondence between IP addresses and MAC addresses

This section explains how to use the `nasipneigh` command to check the correspondence between IP addresses and MAC addresses.

1. To check the correspondence between IP addresses and MAC addresses, execute the `nasipneigh` command.

    The displayed information is added to the beginning of the log file and stored. If the addition of information causes the log file to exceed 1 MB, some entries at the end of the log file will be deleted to keep the log file from exceeding 1 MB.

    ```
    $ sudo nasipneigh
    10.213.89.209 dev mng0-br lladdr 6c:f0:49:5d:cc:31 REACHABLE
    ```

```
10.0.1.25 dev hb0 lladdr 6c:f0:49:5d:c5:70 REACHABLE
10.213.88.10 dev mng0-br lladdr 00:09:41:6a:aa:80 DELAY
10.213.89.211 dev mng0-br lladdr 00:15:17:dd:f3:27 REACHABLE
```

2. Using the **List of RAS Information** page (for `Batch-download`) of the Check for Errors dialog box, acquire the log file and packet dump file.

   This step is necessary if you want to save the log file output when the `nasipneigh` command is executed. To acquire the log file, download all the log data. For details on how to download log files, see the *Troubleshooting Guide*.

   Note:
   You can also use the `eraselog` command to delete log files.

```
$ sudo eraselog
```

Switching the status of an FC path to Online

This section explains how to use the `fponline` command to switch the status of an FC path to `Online`.

The procedure assumes that the status of `path000-0002-0A` is changed from `Offline` to `Online`.

To switch the status of an FC path:

1. Execute the `fpstatus` command to check the current status of the FC path.
   Confirm that `Status` is `Offline`.

   If the status of the FC path is neither `Online` nor `Offline`, see the *Troubleshooting Guide* and restore the status of the FC path.

```
$ sudo fpstatus path000-0002-0A
Path            Target   HostPort HostPortWWN       ArrayPort
ArrayPortWWN     Status
path000-0002-0A N0-T000   fc0002   10000000c9951dec 0A
50060e801046ed00 Offline
```

2. Execute the `fponline` command to switch the status of the FC path.

```
$ sudo fponline path000-0002-0A
```

3. Execute the `fpstatus` command to confirm that the status of the FC path has been switched.
   Confirm that `Status` is `Online`.

```
$ sudo fpstatus path000-0002-0A
Path            Target   HostPort HostPortWWN       ArrayPort
ArrayPortWWN     Status
path000-0002-0A N0-T000   fc0002   10000000c9951dec 0A
50060e801046ed00 Online
```

Changing the setting for automatic switching of an FC path status to Online

This section explains how to use the `fpctl` command to change the setting for automatically switching an FC path to `Online` when the FC path is recovered from an error.

The procedure assumes that the automatic switching of FC paths to `Online` is enabled.

To change the setting:

1. Execute the `fpctl` command to check the current setting.
   Confirm that `Off` is displayed.

   ```
   $ sudo fpctl -e auto-online
   Off
   ```

2. Execute the `fpctl` command to change the setting.

   ```
   $ sudo fpctl -e auto-online --on
   ```

3. Execute the `fpctl` command to confirm that the setting has been changed.
   Confirm that `On` is displayed.

   ```
   $ sudo fpctl -e auto-online
   On
   ```

4. Perform steps 1 through 3 on the other node in the cluster.

Changing the setting for the load balancing function

This section explains how to use the `fpctl` command to change the load balancing function setting.

The procedure assumes that the load balancing function is used and that the Extended Round Robin algorithm is used for switching FC paths.

To change the load balancing function setting:

1. Execute the `fpctl` command to check the current setting.
   Confirm that `On(extended lio)` is displayed.

   ```
   $ sudo fpctl -e load-balance
   On(extended lio)
   ```

2. Execute the `fpctl` command to change the setting.

   ```
   $ sudo fpctl -e load-balance --on --type exrr
   ```

3. Execute the `fpctl` command to confirm that the setting has been changed.
   Confirm that `On(extended round-robin)` is displayed.

```
$ sudo fpctl -e load-balance
On(extended round-robin)
```

4. Perform steps 1 through 3 on the other node in the cluster.

Changing the setting for automatically assigning LDEV numbers to user LUNs

This section explains how to use the `lumapctl` command to change the setting for automatically assigning LDEV numbers to user LUNs.

The procedure assumes that the setting is changed from normal operation mode, in which LDEV numbers in the storage system are automatically assigned to user LUNs, to maintenance mode, in which the LDEV numbers are not assigned automatically.

To change the assignment setting of user LUNs:

1. Execute the `lumapctl` command to check the current setting.
   Confirm that `Off` is displayed.

```
$ sudo lumapctl -t m
Off
```

2. Execute the `lumapctl` command to change the setting.

```
$ sudo lumapctl -t m --on
```

3. Execute the `lumapctl` command to confirm that the setting has been changed.
   Confirm that `On` is displayed.

```
$ sudo lumapctl -t m
On
```

Assigning an LDEV number to a user LUN

This section explains how to use the `lumapadd` command to assign an LDEV number in the storage system to a user LUN.

The procedure assumes that LDEV number `1`, whose model is `AMS` and whose serial number is `83018368`, is assigned to the user LUN `03`.

To assign the LUN to the user LUN:

1. Execute the `lumapctl` command to confirm that the maintenance mode is enabled.
   Confirm that `On` is displayed.

```
$ sudo lumapctl -t m
On
```

2. Execute the `lumaplist` command to check the information of the user LUN.

```
$ sudo lumaplist -a
LUN    Target    Model      serial    LDEV(    hex)    type             size
 00    N0-T002   AMS        83016764     1(   0001)    SATA         20.000GB
 01    N0-T002   AMS        83016764     2(   0002)    SATA         20.000GB
 02    N0-T002   AMS        83016764     3(   0003)    SATA         20.000GB
 03    -         -                 -     -(      -)    -                   -
 04    N0-T000   AMS        83018368     2(   0002)    SATA         20.000GB
 05    N0-T000   AMS        83018368     3(   0003)    SATA         20.000GB
 06    N0-T000   AMS        83018368     4(   0004)    SATA         20.000GB
...
```

3. Execute the `lumapadd` command to assign the LDEV number to the user LUN.

```
$ sudo lumapadd -m AMS -s 83018368 03=1
```

4. Execute the `lumaplist` command to confirm that the LDEV number has been assigned to the user LUN.

```
$ sudo lumaplist -n 03
LUN    Target    Model      serial    LDEV(    hex)    type             size
 03    N0-T000   AMS        83018368     1(   0001)    SATA         20.000GB
```

Setting up an NTP server

This section explains how to use the `timeset` command to set up an NTP server.

The procedure assumes that an NTP server is set up whose IP address is 10.208.193.53.

To set up the NTP server:

1. Execute the `timeset` command to set up the NTP server.

```
$ sudo timeset -s 10.208.193.53
KAQM05153-Q If you change the node time, you must then restart the OS on
both nodes. Do you want to continue? (y/n) y
```

2. Execute the `timeget` command to confirm that the NTP server has been set up correctly.

```
$ sudo timeget -s
NTP server : 10.208.193.53
```

3. Restart the OS on both nodes in the cluster.

   For details on how to restart the OS on a node, see <u>Restarting the OS on a node on page 3-16</u>.

4. Make sure that the time is correctly synchronized with the NTP server that you set up.

   On the **List of RAS Information** page (for `List of messages`) of the Check for Errors dialog box, confirm that the KAQM05154-I system message has been output.

For details on how to check the system messages, see the *Administrator's Guide*.

Setting the node time

This section explains how to use the `timeset` command to set the time on a node.

The following procedure, which explains how to set the time for a node, assumes that the time 11:40 February 13, 2011 is to be set to the node.

To set the node time:

1. Stop the node for which you set the time.
   For details on how to stop the node, see Stopping a node on page 3-7.

2. Execute the `timeset` command to set the time.

   ```
   $ sudo timeset 201102131140
   KAQM05153-Q If you change the node time, you must then restart the OS on
   both nodes. Do you want to continue? (y/n) y
   ```

3. Execute the `timeget` command to confirm that the time has been set correctly.

   ```
   $ sudo timeget
   Sun Feb 13 11:40:12 EST 2011
   ```

4. Restart the OS on the stopped node.
   For details on how to restart the OS on a node, see Restarting the OS on a node on page 3-16.
   It takes approximately five minutes to restart the OS.

5. If an NTP server is set up, to make sure that the time is correctly synchronized with the NTP server after the OS has been restarted, on the **List of RAS Information** page (for `List of messages`) of the Check for Errors dialog box, confirm that the KAQM05154-I system message has been output.
   For details on how to check the system messages, see the *Administrator's Guide*.

6. Restart the stopped node.
   For details on how to start a node, see Starting a node on page 3-9.

7. Fail back the resource group.
   For details on how to fail back a resource group, see Changing the execution node of a resource group on page 3-11.

8. Perform steps 1 through 7 on the other node in the cluster.

Changing the message displayed at login by using SSH

This section explains how to use the `welcomemsgchange` command to change the message displayed at login by using SSH.

The procedure assumes that the default message is changed.

To change the message displayed at SSH login:

1. Execute the `welcomemsgchange` command to check the current message.

```
$ sudo welcomemsgchange
 Warning Notice!

 This is a {Company Name Here} computer system, which may be accessed and
used only for authorized {Company Name Here} business by authorized
personnel. Unauthorized access or use of this computer system may subject
violators to criminal, civil, and/or administrative action.

 All information on this computer system may be intercepted, recorded,
read, copied, and disclosed by and to authorized personnel for official
purposes, including criminal investigations. Such information includes
sensitive data encrypted to comply with confidentiality and privacy
requirements. Access or use of this computer system by any person, whether
authorized or unauthorized, constitutes consent to these terms. There is
no right of privacy in this system.
```

2. Execute the `welcomemsgchange` command to change the message.

```
$ sudo welcomemsgchange -m 'Warning Notice!
> This is a Hitachi computer system, which may be accessed and used only
for authorized Hitachi business by authorized personnel. Unauthorized
access or use of this computer system may subject violators to criminal,
civil, and/or administrative action.'
```

3. Log out from the node, and then log in again.

4. Execute the `welcomemsgchange` command to confirm that the message has been changed.

```
$ sudo welcomemsgchange
Warning Notice!
This is a Hitachi computer system, which may be accessed and used only for
authorized Hitachi business by authorized personnel. Unauthorized access
or use of this computer system may subject violators to criminal, civil,
and/or administrative action.
```

Managing the real-time scan function

This section explains how to manage the real-time scan function.

Registering the scan software to be used

This section explains how to use the `avascanengineset` command to register the scan software to be used.

The procedure assumes that Symantec scan software is to be registered.

To register the scan software to be used:

1. Execute the `avascanengineset` command to register the Symantec scan software.

```
$ sudo avascanengineset SPE
KAQV30072-Q If a different scanning software is chosen, the scan
conditions will be re-initialized and the scan server information will be
```

```
deleted.
Are you sure you want to change the scanning software? (y/n)
```

2. Execute the `avaservicestatus` command to confirm that the Symantec scan software has been registered.

```
$ sudo avaservicestatus
ScanEngine    : SPE/SSE
RealTimeScan   : Stopped
List of Scanner Servers
--------------------------------------------------
```

3. Perform steps 1 through 2 on the other node in the cluster.

Registering scan server information

This section explains how to use the `avaserveradd` command to register scan server information.

The procedure assumes that the scan server information will be registered under the following conditions.

- The scan server name is `scanserver`.
- The scan server port number is `1024`.

To register scan server information:

1. Execute the `avaserveradd` command to register the scan server information.

```
$ sudo avaserveradd scanserver:1024
```

2. Execute the `avaservicestatus` command to confirm that the scan server information has been registered.

```
$ sudo avaservicestatus
ScanEngine    : SPE/SSE
RealTimeScan   : Stopped
List of Scanner Servers
--------------------------------------------------
scanserver    1024    -
```

3. Perform steps 1 through 2 on the other node in the cluster.

Setting scan conditions

This section explains how to use the `avaconfedit` command to set scan conditions.

The procedure assumes that the following scan conditions will be set.

- A scan will be performed when a CIFS client updates a file.
- The polling interval for checking the status of the scan server is 900 seconds.

To set scan conditions:

1. Execute the `avaconfedit` command to set the scan conditions.

   ```
   $ sudo avaconfedit --set AccessType:W,PollingInterval:900
   ```

2. Execute the `avaconfedit` command to confirm that the scan conditions have been set.

   ```
   $ sudo avaconfedit --list ALL
   AccessType    : W
   ScanType      : ALL
   EnableLimitSize : ENABLE
   LimitSize (MB)    : 2047
   OverSizeAccess    : ENABLE
   InfectedAction    : DELETE
   Notify    : DISABLE
   NotifyType    : OFF
   NotifyTime    : 05:00
   ScanWorm    : DISABLE
   ScanStub    : ENABLE
   Timeout (s)    : 30
   ScanTimeout (s)    : 60
   StubScanTimeout (s)    : 900
   Retry    : 1
   ScanningFailsProcedure    : ALLOW
   PollingInterval (s)    : 900
   ScanCacheSize (MB)    : 8
   StatInfo    : OFF
   ```

3. Perform steps 1 through 2 on the other node in the cluster.

Enabling the real-time scan service

This section explains how to use the `avaservicestart` command to enable the real-time scan service.

To enable the real-time scan service:

1. Execute the `avaservicestart` command to enable the real-time scan service.

   When a message asking you whether you want to enable the real-time scan service appears, enter `y`.

   ```
   $ sudo avaservicestart
   KAQV30071-I Real-time scanning was not performed for the clients connected
   to the current CIFS share.
   Restart the CIFS service, or ask the clients to reconnect to the CIFS
   service.
   ```

2. Execute the `avaservicestatus` command to make sure that the real-time scan service has been enabled.

   Confirm that `RealTimeScan` is `Running`.

   ```
   $ sudo avaservicestatus
   ScanEngine    : SPE/SSE
   RealTimeScan    : Running
   List of Scanner Servers
   --------------------------------------------------
   scanserver    1024    Normal
   ```

3. Restart the CIFS service.

4. Perform steps 1 through 3 on the other node in the cluster.

Local user and local group management

This section explains how to manage user information and group information.

Registering a user

This section explains how to use the `usradd` command to register a user.

The procedure assumes that the user that is registered satisfies the following conditions:

- The user name is `user03`.
- The user ID is `1003`.
- The primary group to which the user belongs is `unit03` (group ID: `3000`).
- The password is `password`.
- `SubLeader` is set as a comment.
- CIFS shares are used.

To register a user:

1. Execute the `usrlist` command to view the currently registered users. Make sure that the user name and user ID you are registering are not in use.

```
$ sudo usrlist
List of users:
The number of users(1)
User name : user01
UID       : 1001
GID       : 1000
Comment   : Leader

The number of users(2)
User name : user02
...
```

2. Execute the `usradd` command to register the user.

```
$ sudo usradd -u 1003 -g unit03 -p password -c "SubLeader" -C user03
```

3. Execute the `usrlist` command to confirm that the user has been registered correctly.

```
$ sudo usrlist user03
List of users:
The number of users(1)
User name : user03
UID       : 1003
GID       : 3000
Comment   : SubLeader
```

Command Operations

Hitachi Data Ingestor CLI Administrator's Guide

Batch-registering users

This section explains how to use the `usradd` command to batch-register users.

The procedure assumes that the users that are registered satisfy the following conditions:

- The CSV file is created on a UNIX machine.
- The CSV file name is `useradd100.csv`.
- The result file name is `result_adduser.txt`.
- The host name of the node for which you are registering the users is `fshost01`.
- You are using SSH protocol version 2.

To batch-register users:

1. Create a CSV file for batch registration.
   For details on the CSV file format, see [Format of a CSV file used for batch registration or batch deletion of user information on page B-2](#).

2. Use the `scp` command to transfer the created CSV file to the `/home/nasroot` directory.

   ```
   $ scp /home/admin/useradd100.csv nasroot@fshost01:useradd100.csv
   ```

   Note:
   > You cannot use the name of a directory or file in the home directory of the SSH account (`/home/nasroot`) as the file name of the CSV file.

3. Log in to the node using the SSH account.

   ```
   $ ssh -2 nasroot@fshost01
   ```

4. Execute the `usradd` command to batch-register the users.

   ```
   $ sudo usradd -F useradd100.csv -o result_adduser.txt
   ```

5. On a UNIX machine, use the `scp` command to download the result file from the `/home/nasroot` directory, and confirm that the users have been correctly registered.
   Make sure that `#Completed` appears in all the execution classification fields in the `result_adduser.txt` file. For details on the format of the result file, see [Format of result file used for batch registration or batch deletion of user information on page B-5](#).

   ```
   $ scp nasroot@fshost01:result_adduser.txt /home/admin/result_adduser.txt
   ```

6. Execute the `usrlist` command to confirm that the users have been registered correctly.

   ```
   $ sudo usrlist
   List of users:
   ```

```
The number of users(1)
User name : user01
UID       : 1001
GID       : 1000
Comment   : Leader

The number of users(2)
User name : user02
...
```

7. Execute the `rmfile` command to delete the CSV file and result file.

```
$ sudo rmfile useradd100.csv
KAQM16173-Q Do you want to delete the specified file? (y/n) y
$ sudo rmfile result_adduser.txt
KAQM16173-Q Do you want to delete the specified file? (y/n) y
```

Note:
    Also delete any files that you transferred inadvertently.

Registering a group

This section explains how to use the `grpadd` command to register a group.

The procedure assumes that the group that is registered satisfies the following conditions:

*   The group name is `unit03`.
*   The group ID is `3000`.
*   ACLs are used for accessing CIFS shares.

To register a group:

1. Execute the `grplist` command to view the currently registered groups.
    Make sure that the group name and group ID you are registering are not in use.

```
$ sudo grplist
List of groups:
The number of groups(1)
Group name : unit01
GID        : 1000

The number of groups(2)
Group name : unit02
...
```

2. Execute the `grpadd` command to register the group.

```
$ sudo grpadd -g 3000 -C unit03
```

3. Execute the `grplist` command to confirm that the group has been registered correctly.

```
$ sudo grplist unit03
List of groups:
The number of groups(1)
```

Command Operations
Hitachi Data Ingestor CLI Administrator's Guide

```
Group name : unit03
GID       : 3000
```

Batch-registering groups

This section explains how to use the `grpadd` command to batch-register groups.

The procedure assumes that the groups that are registered satisfy the following conditions:

- The CSV file is created on a UNIX machine.
- The CSV file name is `groupadd100.csv`.
- The result file name is `result_addgroup.txt`.
- The host name of the node for which you are registering the groups is `fshost01`.
- You are using SSH protocol version 2.

To batch-register groups:

1. Create a CSV file for batch registration.
   For details on the format of the CSV file, see Format of a CSV file used for batch registration or batch deletion of group information on page B-8.

2. Use the `scp` command to transfer the created CSV file to the `/home/nasroot` directory.

   ```
   $ scp /home/admin/groupadd100.csv nasroot@fshost01:groupadd100.csv
   ```

   Note:
   You cannot use the name of a directory or file in the home directory of the SSH account (`/home/nasroot`) as the file name of the CSV file.

3. Log in to the node using the SSH account.

   ```
   $ ssh -2 nasroot@fshost01
   ```

4. Execute the `grpadd` command to batch-register the groups.

   ```
   $ sudo grpadd -F groupadd100.csv -o result_addgroup.txt
   ```

5. On a UNIX machine, use the `scp` command to download the result file from the `/home/nasroot` directory, and confirm that the groups have been correctly registered. For details on the format of the result file, see Format of result file used for batch registration or batch deletion of group information on page B-10.

   ```
   $ scp nasroot@fshost01:result_addgroup.txt /home/admin/result_addgroup.txt
   ```

6. Execute the `grplist` command to confirm that the groups have been registered correctly.

```
$ sudo grplist
List of groups:
The number of groups(1)
Group name : unit01
GID        : 1000

The number of groups(2)
Group name : unit02
...
```

7. Execute the `rmfile` command to delete the CSV file and result file.

```
$ sudo rmfile groupadd100.csv
KAQM16173-Q Do you want to delete the specified file? (y/n) y
$ sudo rmfile result_addgroup.txt
KAQM16173-Q Do you want to delete the specified file? (y/n) y
```

Note:
   Also delete any files that you transferred inadvertently.

File system management

This section explains how to manage a file system.

Before operating a file system:

In File Services Manager, you can create a file system from multiple device files. When you use multiple device files, use a logical volume manager. For File Services Manager, use an LVM as a volume manager.

When you create a file system, you must carefully consider such factors as the purpose of the file system and the characteristics of the drive. For details on how a file system should be created, see the *Installation and Configuration Guide*.

Creating a file system

This section explains how to use the `fscreate` command to create a file system. The maximum size of a file system is 1 PB, which is the total size of device files.

The procedure assumes that the file system is created under the following conditions:

• The name of the file system to be created is `filesystem01`.

• `/dev/enas/lu0A`, `/dev/enas/lu0B`, and `/dev/enas/lu0C` are used as device files.

• The ACL type of the file system to be created is Advanced ACL.

To create a file system:

1. Execute the `lulist` command to check the information about device files to be used.

```
$ sudo lulist -v
Device files for use:
 /dev/enas/lu0A FC/SAS 20.000GB - N0-T003 AMS 85011261 -
 /dev/enas/lu0B FC/SAS 20.000GB - N0-T003 AMS 85011261 -
 /dev/enas/lu0C FC/SAS 20.000GB - N0-T003 AMS 85011261 -
 /dev/enas/lu0D FC/SAS 20.000GB - N0-T003 AMS 85011261 -
 /dev/enas/lu0E FC/SAS 20.000GB - N0-T003 AMS 85011261 -
...
```

2. Execute the `fscreate` command to create a file system.

```
$ sudo fscreate -t advanced filesystem01 lu0A,lu0B,lu0C
```

3. Execute the `fslist` command to confirm that the file system has been created correctly.

```
$ sudo fslist -m -t filesystem01
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem01
 Total disk capacity(GB) : 60.000
 Device status           : normal
 Device files            : lu0A lu0B lu0C
 Block used(GB)          :
 Block free(GB)          :
 I-node used             :
 I-node free             :
 Volume manager          : use
 Mount status            : --
 Quota                   : --
 ACL type                : Advanced ACL
 Model                   : AMS
 Serial number           : 85011261
```

The created file system is not automatically mounted. You must use the `fsmount` command to mount the created file system.

Mounting a file system

This section explains how to use the `fsmount` command to mount a file system.

File systems are mounted at the following *mount point* directory:

`/mnt/`*file-system-name*

In an HDI system, the mount status is maintained even if a resource group providing the file system services fails over or if the services are restarted. The HDI system allows full-time access to the file system by maintaining the mount status.

The procedure assumes that the file system `filesystem01` is mounted under the following conditions:

- Permit writing.
- Enable the quota functionality.

To mount a file system:

1. Execute the `fslist` command to view the mount status of the target file system.

   Confirm that `Mount status` is `--`.

```
$ sudo fslist filesystem01
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem01
 Total disk capacity(GB) : 30.000
 Device status           : normal
 Device files            : lu0A lu0B lu0C
 Block used(GB)          :
 Block free(GB)          :
 I-node used             :
 I-node free             :
 Volume manager          : use
 Mount status            : --
 Quota                   : --
```

2. Execute the `fsmount` command to mount the file system.

```
$ sudo fsmount -w -q on filesystem01
```

3. Execute the `fslist` command to confirm that the file system has been mounted correctly.

```
$ sudo fslist filesystem01
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem01
...
 Block used(GB)          : 0.000
 Block free(GB)          : 29.891
 I-node used             : 8
 I-node free             : 31358968
...
 Mount status            : rw
 Quota                   : on
```

Unmounting a file system

This section explains how to use the `fsumount` command to unmount a file system.

Before unmounting a file system, you must do the following:

- Delete all NFS shares and CIFS shares.

  If you attempt to unmount a file system without deleting NFS shares and CIFS shares, an error occurs. Use the `nfsdelete` command to delete the NFS shares. Use the `cifsdelete` command to delete the CIFS shares.

- Inform clients using the service of the file system to be unmounted that the service will be stopped.

  When the file system is unmounted, the service of the file system for which the unmount command was executed is stopped.

- If you are using Backup Restore, check the connection between the NDMP server and the backup server, and between the NDMP server and the media server to make sure that backup or restore operations are not being performed.

  If you unmount a file system during a backup or restore operation, the backup or restore operation ends with an error. Use the `ndmpcontrol` command to check the connection between the NDMP server and the backup server, and between the NDMP server and the media server.

The procedure assumes that the file system `filesystem01` is unmounted.

To unmount a file system:

1. Execute the `fslist` command to view the mount status of the target file system.

   Confirm that `Mount status` is `rw` or `ro`.

```
$ sudo fslist filesystem01
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem01
 Total disk capacity(GB) : 30.000
 Device status           : normal
 Device files            : lu0A lu0B lu0C
 Block used(GB)          : 0.000
 Block free(GB)          : 29.891
 I-node used             : 8
 I-node free             : 31358968
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
```

2. Execute the `fsumount` command to unmount the file system.

```
$ sudo fsumount filesystem01
```

3. Execute the `fslist` command to confirm that the file system has been unmounted correctly.

   Confirm that `Mount status` is `--`.

```
$ sudo fslist filesystem01
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem01
...
 Block used(GB)          :
 Block free(GB)          :
 I-node used             :
 I-node free             :
...
 Mount status            : --
 Quota                   : --
```

Expanding a file system

This section explains how to use the `fsexpand` command to expand a file system that was created using a volume manager. The expanded file system must be no more than 1 PB, which is the total size of device files. For details

on the relationship between the initial capacity of a created file system and the capacity of file systems that can be expanded, see <u>Table 2-180 Initial capacity of a created file system and the maximum capacity after expansion on page 2-323</u>.

The procedure assumes that the file system is expanded under the following conditions:

- The file system name is `filesystem01`.

- `/dev/enas/lu06` and `/dev/enas/lu07` are used as device files.

To expand a file system:

1. Execute the `lulist` command to check the information about device files to be used.

```
$ sudo lulist -v
Device files for use:
 /dev/enas/lu06 FC/SAS 20.000GB - N0-T003 AMS 85011261 -
 /dev/enas/lu07 FC/SAS 20.000GB - N0-T003 AMS 85011261 -
 /dev/enas/lu0D FC/SAS 20.000GB - N0-T003 AMS 85011261 -
 /dev/enas/lu0E FC/SAS 20.000GB - N0-T003 AMS 85011261 -
 /dev/enas/lu0F FC/SAS 20.000GB - N0-T003 AMS 85011261 -
...
```

2. Execute the `fslist` command to confirm the current information about the file system.
   Confirm that `use` is displayed for `Volume manager`.

```
$ sudo fslist -m filesystem01
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem01
 Total disk capacity(GB) : 60.000
 Device status           : normal
 Device files            : lu0A lu0B lu0C
 Block used(GB)          : 0.004
 Block free(GB)          : 59.872
 I-node used             : 8
 I-node free             : 62816248
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
 Model                   : AMS
 Serial number           : 85011261
```

3. Execute the `fsexpand` command to expand the file system.

```
$ sudo fsexpand filesystem01 lu06,lu07
```

4. Execute the `fslist` command to confirm that the file system has been expanded correctly.

```
$ sudo fslist filesystem01
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem01
 Total disk capacity(GB) : 100.000
 Device status           : normal
 Device files            : lu06 lu07 lu0A lu0B lu0C
 Block used(GB)          : 0.004
```

```
Block free(GB)          : 99.810
I-node used             : 8
I-node free             : 104693752
Volume manager          : use
Mount status            : rw
Quota                   : on
```

Changing file system settings

This section explains how to use the `fsedit` command to change the settings of a file system.

The procedure assumes that the file system settings are changed under the following conditions:

- The target file system is a WORM file system.
- The file system name is `filesystem05`.
- The maximum retention period is to be changed from one year to 30 years (10,950 days).
- The minimum retention period is to be changed from 0 minute to 30 minutes.

1. Execute the `fslist` command to confirm the information about the file system whose settings you want to change.
   Confirm that `rw` is displayed for `Mount status`.

   ```
   $ sudo fslist -w filesystem05
   List of File Systems:
   The number of file systems(1)
    File system(used by)    : filesystem05(WORM)
    Total disk capacity(GB) : 10.000
    Block used(GB)          : 0.004
    Block free(GB)          : 9.985
    I-node used             : 84
    I-node free             : 10485676
    Mount status            : rw
    Quota                   : on
    Max retention           : 365-0-0
    Min retention           : 0-0-0
    Auto commit             : off
      Commit mode           : --
    Auto commit period      : --
    Default retention       : --
    Rename empty directories: deny
   ```

2. Execute the `fsedit` command to change the file system settings.

   ```
   $ sudo fsedit -w -M 10950-0-0 -m 0-0-30 filesystem05
   ```

3. Execute the `fslist` command to confirm that the file system settings have been changed.

   ```
   $ sudo fslist -w filesystem05
   List of File Systems:
   The number of file systems(1)
    File system(used by)    : filesystem05(WORM)
    Total disk capacity(GB) : 10.000
   ```

```
Block used(GB)          : 0.004
Block free(GB)          : 9.985
I-node used             : 84
I-node free             : 10485676
Mount status            : rw
Quota                   : on
Max retention           : 10950-0-0
Min retention           : 0-0-30
Auto commit             : off
   Commit mode          : --
Auto commit period      : --
Default retention       : --
Rename empty directories: deny
```

Enabling a warning notification related to file system usage

This section explains how to use the `fsfullmsg` command or the `fsctl` command to enable functionality that generates a warning notification if a file system usage exceeds the threshold. When the system is first installed, warnings are issued if the file system usage exceeds the default warning threshold.

The procedure assumes that a warning notification is generated in either of the following cases:

- When the block usage for the file system (`filesystem02`) exceeds 50 GB

- When the number of used inodes for the file system (`filesystem02`) exceeds 50,000

To enable the warning notification:

1. Execute the `fslist` command to confirm that the target file system has been mounted with the write permission set.
   Confirm that Mount status is rw.

```
$ sudo fslist filesystem02
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem02
 Total disk capacity(GB) : 835.211
 Device status           : normal
 Device files            : lu02 lu0C lu0E lu10
 Block used(GB)          : 0.196
 Block free(GB)          : 834.772
 I-node used             : 9
 I-node free             : 875659255
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
```

2. Execute the `fsfullmsg` command or the `fsctl` command to view the warning notification settings.
   Confirm that the file system name is followed by the string Off.

```
$ sudo fsfullmsg filesystem02
 filesystem02     Off(0,0)
```

```
$ sudo fsctl -m filesystem02
 filesystem02      Off(0,0)
```

3. Execute the `fsfullmsg` command or the `fsctl` command to enable warning notifications.

```
$ sudo fsfullmsg -s -o blimit=50G,ilimit=50000 filesystem02
BlockLimit=50GB, InodeLimit=50000 (filesystem02)
```

```
$ sudo fsctl -m -s -o blimit=50G,ilimit=50000 filesystem02
BlockLimit=50GB, InodeLimit=50000 (filesystem02)
```

4. Execute the `fsfullmsg` command or the `fsctl` command to confirm that warning notifications have been configured correctly.
   Confirm that the file system name is followed by the string `On`.

```
$ sudo fsfullmsg filesystem02
 filesystem02      On(50G,50000)
```

```
$ sudo fsctl -m filesystem02
 filesystem02      On(50G,50000)
```

Enabling automatic failover that is performed when a file system is blocked

This section explains how to use the `fsautofo` command or the `fsctl` command to enable the functionality that automatically performs a failover if a file system is blocked. When the HDI system is first installed, automatic failover is enabled so that failover occurs if the file system becomes blocked.

The procedure assumes that an automatic failover occurs if the file system `filesystem02` is blocked.

To enable automatic failover:

1. Execute the `fslist` command to confirm that the target file system has been mounted with the write permission set.
   Confirm that `Mount status` is `rw`.

```
$ sudo fslist filesystem02
List of File Systems:
The number of file systems(1)
 File system(used by)   : filesystem02
 Total disk capacity(GB) : 835.211
 Device status           : normal
 Device files            : lu02 lu0C lu0E lu10
 Block used(GB)          : 0.196
 Block free(GB)          : 834.772
 I-node used             : 9
 I-node free             : 875659255
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
```

2. Execute the `fsautofo` command or the `fsctl` command to view the automatic failover settings.
   Confirm that the file system name is followed by the string `Off`.

```
$ sudo fsautofo filesystem02
 filesystem02     Off
```

```
$ sudo fsctl -f filesystem02
 filesystem02     Off
```

3. Execute the `fsautofo` command or the `fsctl` command to enable automatic failovers.

```
$ sudo fsautofo -s filesystem02
```

```
$ sudo fsctl -f -s filesystem02
```

4. Execute the `fsautofo` command or the `fsctl` command to confirm that automatic failovers have been configured correctly.
   Confirm that the file system name is followed by the string `On`.

```
$ sudo fsautofo filesystem02
 filesystem02     On
```

```
$ sudo fsctl -f filesystem02
 filesystem02     On
```

Changing the settings to enable recording of the file creation time

This section explains how to use the `fsctl` command to change the settings to enable or disable recording of the time that a file is created for existing file systems.

Note:

For a file system for which recording of the file creation time is disabled, if a CIFS client views the file system attribute, the oldest of the last access time (`atime`), last modified time (`ctime`), and last edited time (`mtime`) is displayed as the creation time. Note that even if recording of the file creation time is enabled, NFS clients cannot view the creation time.

The procedure assumes that the settings for the file system `filesystem02` are changed.

To enable recording of the file creation time:

1. Execute the `fslist` command to confirm that the target file system has been mounted with the write permission set.
   Confirm that `Mount status` is `rw`.

```
$ sudo fslist filesystem02
List of File Systems:
The number of file systems(1)
```

```
File system(used by)     : filesystem02
Total disk capacity(GB) : 835.211
Device status            : normal
Device files             : lu02 lu0C lu0E lu10
Block used(GB)           : 0.196
Block free(GB)           : 834.772
I-node used              : 9
I-node free              : 875659255
Volume manager           : use
Mount status             : rw
Quota                    : on
```

2. Execute the `fsctl` command to view the file creation time settings.
   Confirm that the file system name is followed by the string `Off`.

```
$ sudo fsctl -c -o create_time filesystem02
 filesystem02     Off
```

3. Execute the `fsctl` command to change the settings so that the file creation time is recorded.

```
$ sudo fsctl -c -s -o create_time filesystem02
```

4. Execute the `fsctl` command to confirm that the settings have been specified correctly.
   Confirm that the file system name is followed by the string `On`.

```
$ sudo fsctl -c -o create_time filesystem02
 filesystem02     On
```

5. If necessary, execute the `fsctl` command to set the file creation time for all existing files.
   The oldest of the last access time (`atime`), the last change time (`ctime`), and the last modification time (`mtime`) is set as the file creation time. If this step is performed for a file system or directory that contains 100,000 files, about one minute is required for the processing to finish.

```
$ sudo fsctl -c -x filesystem02
filesystem02: Wait ............. Success
```

Managing NFS shares

This section explains how to manage NFS shares.

Creating an NFS share

This section explains how to use the `nfscreate` command to create an NFS share. Note that you can create a maximum of 1,024 NFS shares per cluster.

When you create an NFS share for a file system of the Advanced ACL type, the access control does not operate according to the permission that can be viewed by the client but to the set ACL. For this reason, when you use only NFS shares, use the file systems of the Classic ACL type. For the same

reason, when you use file systems of the Advanced ACL type, do not set inherited ACEs to directories for which you create NFS shares.

If an error occurs during NFS share creation, the previous status is restored. The entered settings do not change if a failover or restart occurs once NFS shares have been created.

The procedure assumes that an NFS share is created under the following conditions:

- A new directory is created with the name `/mnt/filesystem01/unit01` as a shared directory (owner: `sys01`, owner group: `unit01`).

- The `/mnt/filesystem01/unit01` directory will be made public only to `host01`.

To create an NFS share:

1. Execute the `fslist` command to confirm that the file system in which you want to create a shared directory has been mounted.

   If you want to create an NFS share in a newly created shared directory or with the write permission set, confirm that `Mount status` is `rw`.

```
$ sudo fslist -t filesystem01
List of File Systems:
The number of file systems(1)
 File system(used by)     : filesystem01
 Total disk capacity(GB) : 30.000
 Device status            : normal
 Device files             : lu0A lu0B lu0C
 Block used(GB)           : 0.000
 Block free(GB)           : 29.891
 I-node used              : 8
 I-node free              : 31358968
 Volume manager           : use
 Mount status             : rw
 Quota                    : on
 ACL type                 : Classic ACL
```

2. Execute the `dircreate` command to create a public directory.

   This step is necessary when you create a new shared directory.

```
$ sudo dircreate -u sys01 -g unit01 /mnt/filesystem01/unit01
```

3. Execute the `dirlist` command to confirm that the shared directory has been created correctly.

   This step is necessary when you have created a new shared directory.

```
$ sudo dirlist -d /mnt/filesystem01/unit01
0755 sys01            unit01            /mnt/filesystem01/unit01
```

4. Execute the `nfscreate` command to create an NFS share.

```
$ sudo nfscreate -d /mnt/filesystem01/unit01 -H host01
```

5. Execute the `nfslist` command to confirm that the NFS share has been created correctly.

```
$ sudo nfslist -d /mnt/filesystem01/unit01
List of File Shares:
The number of NFS share(1)
    Shared directory                        : /mnt/filesystem01/unit01
        Public destination host/network    : host01
        Permission mode / Synchronous writing : rw_sync
        Anonymous mapping                   : root_only
        Anonymous UID                       : 65534
        Anonymous GID                       : 65534
        Transmission port restriction       : do_not_perform
        Subtree check                       : do_not_perform
        Access check with lock request      : do_not_perform
```

Editing information about an NFS share

This section explains how to use the `nfsedit` command to edit information about an NFS share.

The procedure assumes that the information is edited under the following conditions:

- An NFS share with the write permission set has been created in the `/mnt/filesystem01/unit01` directory and made public on `host01`.

- The write permissions are removed from the NFS share in the `/mnt/filesystem01/unit01` directory.

To edit information about an NFS share:

1. Execute the `nfslist` command to view the current information about the target NFS share.

```
$ sudo nfslist -d /mnt/filesystem01/unit01
List of File Shares:
The number of NFS share(1)
    Shared directory                        : /mnt/filesystem01/unit01
        Public destination host/network    : host01
        Permission mode / Synchronous writing : rw_sync
        Anonymous mapping                   : root_only
        Anonymous UID                       : 65534
        Anonymous GID                       : 65534
        Transmission port restriction       : do_not_perform
        Subtree check                       : do_not_perform
        Access check with lock request      : do_not_perform
```

2. Execute the `nfsedit` command to edit information about the NFS share.

```
$ sudo nfsedit -d /mnt/filesystem01/unit01 -H host01 -p ro
```

3. Execute the `nfslist` command to confirm that information about the NFS share has been changed.

```
$ sudo nfslist -d /mnt/filesystem01/unit01
List of File Shares:
The number of NFS share(1)
    Shared directory                        : /mnt/filesystem01/unit01
        Public destination host/network    : host01
        Permission mode / Synchronous writing : ro
...
```

Backing up information about NFS shares

This section explains how to use the `nfsbackup` command to back up information about the NFS shares for each file system. The backed-up information about NFS shares can be restored by using the `nfsrestore` command.

The procedure assumes that the information is backed up under the following conditions:

- The target file system is `filesystem01`.
- The information definition file name is `filesystem01_nfsshares.xml`.

To back up information about an NFS share:

1. Execute the `nfslist` command to check the current NFS share information.

```
$ sudo nfslist -O m,s
List of File Shares:
The number of NFS share(1)
    Shared directory                        : /mnt/filesystem01/unit01
        Public destination host/network     : host01
        Permission mode / Synchronous writing : rw_sync
        Anonymous mapping                    : root_only
        Anonymous UID                        : 65534
        Anonymous GID                        : 65534
        Transmission port restriction        : do_not_perform
        Subtree check                        : do_not_perform
        Access check with lock request       : do_not_perform
        Maximum rwsize(KB)                   : --
        Security flavor                      : sys

The number of NFS share(2)
    Shared directory                        : /mnt/filesystem01/unit02
        Public destination host/network     : host02
...
```

2. Execute the `nfsbackup` command to back up the NFS share information.

```
$ sudo nfsbackup filesystem01 filesystem01_nfsshares.xml
```

3. Execute the `nfsrestore` command with the `--list` option specified to check the contents of the information definition file.

```
$ sudo nfsrestore --list filesystem01_nfsshares.xml
Backup date and time: 2009-04-13T10:04:26-0400
List of Backed-up File Shares:
The number of NFS share(1)
    Shared directory                        : /mnt/filesystem01/unit01
        Public destination host/network     : host01
        Permission mode / Synchronous writing : rw_sync
        Anonymous mapping                    : root_only
        Anonymous UID                        : 65534
        Anonymous GID                        : 65534
        Transmission port restriction        : do_not_perform
        Subtree check                        : do_not_perform
        Access check with lock request       : do_not_perform
        Maximum rwsize(KB)                   : --
        Security flavor                      : sys

The number of NFS share(2)
```

```
     Shared directory                             : /mnt/filesystem01/unit02
         Public destination host/network         : host02
...
```

Note:

> If you do not restore the backed-up information soon after the backup
> finishes, use the `scp` command on the remote host to move and save the
> information definition file stored in the `/home/nasroot` directory to a
> remote host.

```
scp nasroot@host-name-of-node:information-definition-file-name path-for-
the-file-to-save
```

> After the file is sent to the remote host, execute the `rmfile` command to
> delete the information definition file stored in the `/home/nasroot`
> directory.

```
sudo rmfile information-definition-file-name
```

Restoring information about NFS shares

This section explains how to use the `nfsrestore` command to restore
information about NFS shares. However, you must first mount the file system
associated with the NFS shares. NFS share information backed up by using
the `nfsbackup` command can be restored.

The procedure assumes that the information is restored under the following
conditions:

- The target file system is `filesystem01`.

- The target information definition file is `filesystem01_nfsshares.xml`.

To restore information about an NFS share:

1. Execute the `nfsrestore` command with the `--list` option specified to
   check the contents of the information definition file.

```
$ sudo nfsrestore --list filesystem01_nfsshares.xml
Backup date and time: 2009-04-13T10:04:26-0400
List of Backed-up File Shares:
The number of NFS share(1)
    Shared directory                             : /mnt/filesystem01/unit01
        Public destination host/network         : host01
        Permission mode / Synchronous writing : rw_sync
        Anonymous mapping                        : root_only
        Anonymous UID                            : 65534
        Anonymous GID                            : 65534
        Transmission port restriction            : do_not_perform
        Subtree check                            : do_not_perform
        Access check with lock request           : do_not_perform
        Maximum rwsize(KB)                       : --
        Security flavor                          : sys

The number of NFS share(2)
    Shared directory                             : /mnt/filesystem01/unit02
```

```
            Public destination host/network       : host02
...
```

2. If the target file system has not been mounted yet, execute the `fsmount` command to mount it.

```
$ sudo fsmount -w filesystem01
```

3. Execute the `nfsrestore` command to restore the information about NFS shares.

```
$ sudo nfsrestore filesystem01_nfsshares.xml
```

4. Execute the `nfslist` command to make sure the information about NFS shares has been properly restored.

```
$ sudo nfslist -O m,s
List of File Shares:
The number of NFS share(1)
    Shared directory                       : /mnt/filesystem01/unit01
        Public destination host/network       : host01
        Permission mode / Synchronous writing : rw_sync
        Anonymous mapping                     : root_only
        Anonymous UID                         : 65534
        Anonymous GID                         : 65534
        Transmission port restriction         : do_not_perform
        Subtree check                         : do_not_perform
        Access check with lock request        : do_not_perform
        Maximum rwsize(KB)                    : --
        Security flavor                       : sys

The number of NFS share(2)
    Shared directory                       : /mnt/filesystem01/unit02
        Public destination host/network       : host02
...
```

5. Execute the `rmfile` command to delete the information definition file.

```
$ sudo rmfile filesystem01_nfsshares.xml
KAQM16173-Q Do you want to delete the specified file? (y/n) y
```

Adding a keytab file for Kerberos authentication

This section explains how to use the `nfskeytabadd` command to add the keytab file for Kerberos authentication to the keytab files managed by the node.

The procedure assumes that a file is added under the following conditions:

- The name of the file to be added is `nfs.keytab`.
- The host name of the node for which you are registering the file is `fshost01`.
- The SSH protocol version 2 is used.

To add a keytab file for Kerberos authentication:

1. Use the `scp` command to transfer the file to the SSH account home directory (`/home/nasroot`).

```
$ scp /tmp/nfs.keytab nasroot@fshost01:
nfs.keytab                                   100%  166     0.2KB/s   00:00
```

Note:

> You cannot use the name of a directory or file that already exists in the home directory of the SSH account (`/home/nasroot`) as the name of the file.

2. Log in to the target node by using SSH.

```
$ ssh -2 nasroot@fshost01
```

3. Execute the `nfskeytabadd` command to add the keytab file for Kerberos authentication.

    The contents of the file is added and the specified file is deleted from the `/home/nasroot` directory.

    Confirm that the contents of the added file are displayed.

```
$ sudo nfskeytabadd -i /home/nasroot/nfs.keytab
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
----
--------------------------------------------------------------------------
   3 nfs/node0.ad2003.skyu1.local@AD2003.SKYU1.LOCAL
   3 nfs/node1.ad2003.skyu1.local@AD2003.SKYU1.LOCAL
```

Managing CIFS shares

This section explains how to manage CIFS shares.

Multiple CIFS share names can be assigned to the same share directory by creating multiple CIFS shares for the same share directory. Note the following in regards to share operations:

*   We recommend using commands to create and edit CIFS shares.
*   In the GUI, information about only the first CIFS share created for each share directory is displayed.

Creating a CIFS share

This section explains how to use the `cifscreate` command to create CIFS shares.

The maximum number of CIFS shares that you can create depends on whether the configuration definition of the CIFS service is set to automatically reload the CIFS share setting and apply it in the CIFS client environment. For details about the maximum number of CIFS shares, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

Note:

> If you create a new shared directory, the settings information specified for the shared directory will differ between the Classic ACL type file system and the Advanced ACL type file system.

> When the file system is the Advanced ACL type, ACL settings information is provided according to the permission mode specified by the `dircreate` command. You can check the ACL settings information by executing the `dirgetacl` command. If you want to change the ACL settings information, use the `dirsetacl` command.

> When the file system is the Classic ACL type, only the permission mode is set but not the ACL settings information.

The procedure assumes that a CIFS share is created under the following conditions:

- A new directory is created with the name `/mnt/filesystem04/unit20` as a shared directory (owner: `sys02`, owner group: `unit10`).

- `user00` is not allowed to write data to the CIFS share.

- A new CIFS share is created with the name `unit20`.

To create a CIFS share:

1. Execute the `fslist` command to confirm that the file system in which you want to create a shared directory has been mounted.

   If you want to create a CIFS share in a newly created shared directory or with the write permission set, confirm that `Mount status` is `rw`.

```
$ sudo fslist -t filesystem04
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem04
 Total disk capacity(GB) : 80.000
 Device status           : normal
 Device files            : lu02 lu03 lu04 lu05
 Block used(GB)          : 0.000
 Block free(GB)          : 79.960
 I-node used             : 8
 I-node free             : 83886072
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
 ACL type                : Advanced ACL
```

2. Execute the `dircreate` command to create a shared directory.

   This step is necessary when you create a new shared directory. If you create a new directory, by default, the directory will be created with the `0755` mode. Before all the information of the CIFS share has been applied, it is possible that another user could write data to the CIFS share. For this reason, we recommend that you create a shared directory with permission settings that permit only the owner to write, create a CIFS share, and then set write permissions for the shared directory.

```
$ sudo dircreate -u sys02 -g unit10 -m 700 /mnt/filesystem04/unit20
```

3. Execute the `dirlist` command to confirm that the shared directory has been created correctly.

   This step is necessary when you have created a new shared directory.

   ```
   $ sudo dirlist -d /mnt/filesystem04/unit20
   0700 sys02            unit10           /mnt/filesystem04/unit20
   ```

4. Execute the `cifscreate` command to create a CIFS share.

   ```
   $ sudo cifscreate -x unit20 -d /mnt/filesystem04/unit20 -D add:user00
   ```

5. Execute the `cifslist` command to confirm that the CIFS share has been created correctly.

   ```
   $ sudo cifslist -x unit20 -v
   List of File Shares:
   The number of CIFS share(1)
     Name of file share              : unit20
     Shared directory                : /mnt/filesystem04/unit20
     Use ACL                         : use
     Server specification            : --
     Comment for file share          :
     Permission mode                 : rw
     Browse permission               : permit
     File access permissions         : --
     Directory access permissions    : --
     Write disallowed users          : user00
     Write disallowed groups         : --
     Write allowed users             : --
     Write allowed groups            : --
   ```

6. Execute the `diredit` command to change the attributes of the shared directory.

   ```
   $ sudo diredit -m 777 /mnt/filesystem04/unit20
   ```

7. Execute the `dirlist` command to confirm that the attributes of the shared directory have been changed.

   ```
   $ sudo dirlist -d /mnt/filesystem04/unit20
   0777 sys02            unit10           /mnt/filesystem04/unit20
   ```

Editing information about a CIFS share

This section explains how to use the `cifsedit` command to edit information about a CIFS share.

The procedure assumes that the information is edited under the following conditions:

- The name of the CIFS share whose attributes are to be changed is `unit20`.

- A comment is to be set for the CIFS share.

To edit information about a CIFS share:

1. Execute the `cifslist` command to view the current information about the target CIFS share.

```
$ sudo cifslist -x unit20
List of File Shares:
The number of CIFS share(1)
  Name of file share            : unit20
  Shared directory              : /mnt/filesystem04/unit20
  Use ACL                       : use
  Server specification          : --
  Comment for file share        :
  Permission mode               : rw
  Browse permission             : permit
  File access permissions       : --
  Directory access permissions  : --
```

2. Execute the `cifsedit` command to edit information about the CIFS share.

```
$ sudo cifsedit -x unit20 -c "cifs comment"
```

3. Execute the `cifslist` command to confirm that information about the CIFS share has been changed.

```
$ sudo cifslist -x unit20
List of File Shares:
The number of CIFS share(1)
  Name of file share            : unit20
...
  Comment for file share        : cifs comment
...
```

Backing up information about CIFS shares

This section explains how to use the `cifsbackup` command to back up information about the CIFS shares for each file system. The backed-up information about CIFS shares can be restored by using the `cifsrestore` command.

The procedure assumes that the information is backed up under the following conditions:

- The target file system is `filesystem01`.
- The information definition file name is `filesystem01_cifsshares.xml`.

To back up information about CIFS shares:

1. Execute the `cifslist` command to check the current CIFS share information.

```
$ sudo cifslist -v -O all
List of File Shares:
The number of CIFS share(1)
  Name of file share            : unit20
  Shared directory              : /mnt/filesystem01/unit20
  Use ACL                       : use
  Server specification          : --
  Comment for file share        :
```

```
    Permission mode            : rw
    Browse permission          : permit
    File access permissions    : rw,rw,rw
    Directory access permissions : rw,rw,rw
    Write disallowed users     : usr001
    Write disallowed groups    : --
    Write allowed users        : --
    Write allowed groups       : --
    Guest account access       : default
    Disk synchronization policy : default
    CIFS client cache          : default
    File timestamp changeable  : default
    Home directory             : do_not_use
    CIFS access log (success)  : none
    CIFS access log (failure)  : none
    ACL type                   : Classic ACL
    Client access policy       : parallel
    Volume Shadow Copy Service : default
    Modified files check (VSS) : default
    Read-only cache for conflicts : default
    Access Based Enumeration   : default
    Offline attribute          : do_not_use
    Home directory roaming     : do_not_use
    Retry file modify (HDR)    : do_not_use
    SMB encryption             : default

The number of CIFS share(2)
  Name of file share          : unit21
  Shared directory            : /mnt/filesystem01/unit21
...
```

2. Execute the `cifsbackup` command to back up the information about the CIFS shares.

```
$ sudo cifsbackup filesystem01 filesystem01_cifsshares.xml
```

3. Execute the `cifsrestore` command with the `--list` option specified to check the contents of the information definition file.

```
$ sudo cifsrestore --list filesystem01_cifsshares.xml
Backup date and time: 2016-01-19T09:02:15-0500
List of Backed-up File Shares:
The number of CIFS share(1)
  Name of file share          : unit20
  Shared directory            : /mnt/filesystem01/unit20
  Use ACL                     : use
  Server specification        : --
  Comment for file share      :
  Permission mode             : rw
  Browse permission           : permit
  File access permissions     : rw,rw,rw
  Directory access permissions : rw,rw,rw
  Write disallowed users      : usr001
  Guest account access        : default
  Disk synchronization policy : default
  CIFS client cache           : default
  File timestamp changeable   : default
  Home directory              : do_not_use
  CIFS access log (success)   : none
  CIFS access log (failure)   : none
  Client access policy        : parallel
  Volume Shadow Copy Service  : default
  Modified files check (VSS)  : default
  Read-only cache for conflicts : default
  Access Based Enumeration    : default
  Offline attribute           : do_not_use
```

```
   SMB encryption             : default
   Retry file modify (HDR)    : do_not_use

List of Backed-up File Shares:
The number of CIFS share(2)
   Name of file share         : unit21
   Shared directory           : /mnt/filesystem01/unit21
...
```

Note:

If you do not restore the backed-up information soon after the backup finishes, use the `scp` command on the remote host to move and save the information definition file stored in the `/home/nasroot` directory to a remote host.

```
scp nasroot@host-name-of-node:information-definition-file-name path-for-
the-file-to-save
```

After the file is sent to the remote host, execute the `rmfile` command to delete the information definition file stored in the `/home/nasroot` directory.

```
sudo rmfile information-definition-file-name
```

Restoring information about CIFS shares

This section explains how to use the `cifsrestore` command to restore information about an CIFS share. However, you must first mount the file system associated with the CIFS shares. CIFS share information backed up by using the `cifsbackup` command can be restored.

The procedure assumes that the information is restored under the following conditions:

- The target file system is `filesystem01`.
- The target information definition file is `filesystem01_cifsshares.xml`.

To restore information about CIFS shares:

1. Execute the `cifsrestore` command with the `--list` option specified to check the contents of the information definition file.

```
$ sudo cifsrestore --list filesystem01_cifsshares.xml
Backup date and time: 2016-01-19T09:02:15-0500
List of Backed-up File Shares:
The number of CIFS share(1)
   Name of file share         : unit20
   Shared directory           : /mnt/filesystem01/unit20
   Use ACL                    : use
   Server specification       : --
   Comment for file share     :
   Permission mode            : rw
   Browse permission          : permit
   File access permissions    : rw,rw,rw
   Directory access permissions : rw,rw,rw
   Write disallowed users     : usr001
   Guest account access       : default
```

```
   Disk synchronization policy  : default
   CIFS client cache            : default
   File timestamp changeable    : default
   Home directory               : do_not_use
   CIFS access log (success)     : none
   CIFS access log (failure)     : none
   Client access policy          : parallel
   Volume Shadow Copy Service    : default
   Modified files check (VSS)    : default
   Read-only cache for conflicts : default
   Access Based Enumeration      : default
   Offline attribute             : do_not_use
   SMB encryption                : default
   Retry file modify (HDR)       : do_not_use

List of Backed-up File Shares:
The number of CIFS share(2)
  Name of file share            : unit21
  Shared directory              : /mnt/filesystem01/unit21
...
```

2. If the target file system has not been mounted yet, execute the `fsmount` command to mount it.

```
$ sudo fsmount -w filesystem01
```

3. Execute the `cifsrestore` command to restore the information about the CIFS shares.

```
$ sudo cifsrestore filesystem01_cifsshares.xml
```

4. Execute the `cifslist` command to make sure the information about the CIFS shares has been properly restored.

```
$ sudo cifslist -v -O all
List of File Shares:
The number of CIFS share(1)
  Name of file share            : unit20
  Shared directory              : /mnt/filesystem01/unit20
  Use ACL                       : use
  Server specification          : --
  Comment for file share        :
  Permission mode               : rw
  Browse permission             : permit
  File access permissions       : rw,rw,rw
  Directory access permissions  : rw,rw,rw
  Write disallowed users        : usr001
  Write disallowed groups       : --
  Write allowed users           : --
  Write allowed groups          : --
  Guest account access          : default
  Disk synchronization policy   : default
  CIFS client cache             : default
  File timestamp changeable     : default
  Home directory                : do_not_use
  CIFS access log (success)     : none
  CIFS access log (failure)     : none
  ACL type                      : Classic ACL
  Client access policy          : parallel
  Volume Shadow Copy Service    : default
  Modified files check (VSS)    : default
  Read-only cache for conflicts : default
  Access Based Enumeration      : default
  Offline attribute             : do_not_use
```

```
   Home directory roaming        : do_not_use
   Retry file modify (HDR)       : do_not_use
   SMB encryption                : default

The number of CIFS share(2)
  Name of file share            : unit21
  Shared directory              : /mnt/filesystem01/unit21
...
```

5. Execute the `rmfile` command to delete the information definition file.

```
$ sudo rmfile filesystem01_cifsshares.xml
KAQM16173-Q Do you want to delete the specified file? (y/n) y
```

Setting the directory used for saving the CIFS access log

This section explains how to use the `cifslogctl` command to set the directory used for saving the CIFS access log. When the directory is set and a new access log is swapped in, the existing CIFS access log is saved to the file system under the following file name:

cifsaccesslog_*host-name-of-node_YYYYMMDD_hhmmss*.log

If a file with the same file name already exists in the directory, that file is overwritten. For details on the information output to the CIFS access log, see the *Installation and Configuration Guide*.

To prevent the saved CIFS access log from affecting the file system capacity, we recommend that you set up the system to generate a warning when file system usage by the access log files exceeds a set threshold. For details on how to set up warning notification, see Enabling a warning notification related to file system usage on page 3-48.

The procedure assumes that a new directory (`/mnt/filesystem04/cifslog`) is created in a file system of the Advanced ACL type in order to save the CIFS access log to that directory.

To set the directory used for saving the CIFS access log:

1. Execute the `fslist` command to confirm that the file system containing the directory has been mounted.
   Confirm that the `Mount status` is `rw`.

```
$ sudo fslist -t filesystem04
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem04
 Total disk capacity(GB) : 40.000
 Device status           : normal
 Device files            : lu0C lu0D lu0E lu0F
 Block used(GB)          : 0.000
 Block free(GB)          : 39.855
 I-node used             : 8
 I-node free             : 41811960
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
 ACL type                : Advanced ACL
```

2. Execute the `dircreate` command to create a directory used for saving the CIFS access log.

   This step is necessary when you create a new directory. Specify `root` as both the directory owner and group name. Specify `700` as the mode for the owner, owner group, and other users.

   ```
   $ sudo dircreate -u root -g root -m 700 /mnt/filesystem04/cifslog
   ```

3. Execute the `dirlist` command to confirm that the directory has been created correctly.

   This step is necessary whenever you create a new directory.

   ```
   $ sudo dirlist -d /mnt/filesystem04/cifslog
   0700 root              root              /mnt/filesystem04/cifslog
   ```

4. If the file system is the Advanced ACL type, execute the `dirsetacl` command to set an ACL for the directory.

   Specify the settings so that only the `root` user can access the directory.

   ```
   $ sudo dirsetacl -t advanced --allow root:u:a:a:f /mnt/filesystem04/cifslog
   ```

5. If the file system is the Advanced ACL type, execute the `dirgetacl` command to check the ACL that is set for the directory.

   ```
   $ sudo dirgetacl /mnt/filesystem04/cifslog
   /mnt/filesystem04/cifslog
   root:u:a:a:ALLOW:f
   ```

6. Execute the `cifscreate` command to create a CIFS share in the new directory.

   Set the `-b` option to ensure that the share name of the directory in which the CIFS access log is saved will not be displayed in the CIFS client environment.

   ```
   $ sudo cifscreate -x cifslog -d /mnt/filesystem04/cifslog -b do_not_permit
   ```

7. Execute the `cifslist` command to confirm that the CIFS share has been created correctly.

   ```
   $ sudo cifslist -x cifslog
   List of File Shares:
   The number of CIFS share(1)
     Name of file share            : cifslog
     Shared directory              : /mnt/filesystem04/cifslog
     Use ACL                       : use
     Server specification          : --
     Comment for file share        :
     Permission mode               : rw
     Browse permission             : do_not_permit
     File access permissions       : --
     Directory access permissions  : --
   ```

8. Execute the `cifslogctl` command to check the current setting for the CIFS access log directory.

```
$ sudo cifslogctl --display
Directory for saving : Unsetting
```

9. Execute the `cifslogctl` command to set the directory used for saving the CIFS access log.

```
$ sudo cifslogctl --setdir /mnt/filesystem04/cifslog
```

10. Execute the `cifslogctl` command to confirm that the directory used for saving the CIFS access log has been set correctly.

```
$ sudo cifslogctl --display
Directory for saving : /mnt/filesystem04/cifslog
```

Saving the latest CIFS access log information

This section explains how to use the `cifslogctl` command to save all of the latest CIFS access log information at the same time.

The procedure assumes that a directory (`/mnt/filesystem04/cifslog`) has already been set for where the CIFS access log information is saved.

1. Execute the `cifslogctl` command to confirm the directory in which the CIFS access log information is saved.

```
$ sudo cifslogctl --display
Directory for saving : /mnt/filesystem04/cifslog
```

2. Execute the `cifslogctl` command to save the latest CIFS access log information.

```
$ sudo cifslogctl --save
```

Managing ACLs

This section explains how to manage the ACLs of shared directories.

Setting an ACL (for a file system of the Advanced ACL type)

This section explains how to use the `dirsetacl` command to set an ACL for a shared directory created in a file system of the Advanced ACL type.

Note that the maximum number of ACEs for a directory is 700.

The procedure assumes that an ACL is set for the `/mnt/filesystem04/unit20` directory under the following conditions:

- *Full Control* permission is granted to the user `user01`. The application destination is *This folder only*.

- *List Folder / Read Data* and *Read Attributes* permissions are granted to the group `Everyone`.

- The application destination is *This folder, subfolders, and files*.
- The inheritance range is all folders and files under this folder.

To set an ACL:

1. Execute the `fslist` command to make sure of the following:

   - `Mount status` is `rw`.

   - `ACL type` is `Advanced ACL`.

```
$ sudo fslist -t filesystem04
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem04
 Total disk capacity(GB) : 80.000
 Device status           : normal
 Device files            : lu7B lu7C lu7D lu7E
 Block used(GB)          : 0.256
 Block free(GB)          : 79.744
 I-node used             : 5
 I-node free             : 83623931
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
 ACL type                : Advanced ACL
```

2. Execute the `dirsetacl` command to set an ACL.

```
$ sudo dirsetacl -t advanced --allow user01:u:o:o:f --allow
Everyone:g:a:a:r::a /mnt/filesystem04/unit20
```

3. Execute the `dirgetacl` command to confirm that the ACL has been correctly set for the directory.

```
$ sudo dirgetacl /mnt/filesystem04/unit20
/mnt/filesystem04/unit20
user01:u:o:o:ALLOW:f
Everyone:g:a:a:ALLOW:r::a
```

Setting an ACL (for a file system of the Classic ACL type)

This section explains how to use the `dirsetacl` command to set an ACL for a shared directory created in a file system of the Classic ACL type.

Note that the maximum number of ACEs for a directory is 128 (that is, a maximum of 64 ACEs each for access ACLs and default ACLs).

Note that ACL settings are not inherited to subdirectories and files in a directory for which an ACL is set. Use a CIFS client to set ACLs for the subdirectories and files in a shared directory.

When creating a CIFS share for a directory for which an ACL has been set, if you set that the ACL is not used, the ACL settings cannot be viewed and the ACL cannot be set from a CIFS client even though the ACL permissions are still enabled.

The procedure assumes that an ACL is set for the `/mnt/filesystem02/unit10` directory under the following conditions:

- Read and write permissions are granted to the user `user01`.
- Read permissions are granted to the group `unit02`.

To set an ACL:

1. Execute the `fslist` command to make sure of the following:

   - `Mount status` is `rw`.
   - `ACL type` is `Classic ACL`.

```
$ sudo fslist -t filesystem02
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem02
 Total disk capacity(GB) : 80.000
 Device status           : normal
 Device files            : lu7B lu7C lu7D lu7E
 Block used(GB)          : 0.256
 Block free(GB)          : 79.744
 I-node used             : 5
 I-node free             : 83623931
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
 ACL type                : Classic ACL
```

2. Execute the `dirsetacl` command to set an ACL.

```
$ sudo dirsetacl -m u:user01:rw,g:unit02:r /mnt/filesystem02/unit10
```

3. Execute the `dirgetacl` command to confirm that the ACL has been correctly set for the directory.

```
$ sudo dirgetacl /mnt/filesystem02/unit10/
# file: /mnt/filesystem02/unit10
# owner: sys02
# group: unit10
user::rwx
user:user01:rw-
group::rwx
group:unit02:r--
mask::rwx
other::rwx
```

Managing the quotas for each file system

This section explains how to manage the quotas for each file system.

For other cautionary notes on managing quotas, see the *Installation and Configuration Guide*.

Setting quotas for users for each file system

This section explains how to use the `quotaset` command to set quotas for users for each file system.

The procedure assumes that a quota is set under the following conditions:

- The target file system is `filesystem02`.
- A quota is assigned to the user `sys02`.
- The soft limit on block usage is set to 1 GB, and the hard limit is set to 2 GB.

To set a quota for a user:

1. Execute the `fslist` command to confirm that the target file system is mounted with the quota functionality enabled.
   Confirm that `Quota` is `on`.

   ```
   $ sudo fslist filesystem02
   List of File Systems:
   The number of file systems(1)
    File system(used by)     : filesystem02
    Total disk capacity(GB) : 40.000
    Device status            : normal
    Device files             : lu00 lu01 lu02 lu03
    Block used(GB)           : 0.004
    Block free(GB)           : 39.860
    I-node used              : 8
    I-node free              : 41811960
    Volume manager           : use
    Mount status             : rw
    Quota                    : on
   ```

2. Execute the `quotaset` command to set the quota for the user.

   ```
   $ sudo quotaset -u sys02 -b 1G,2G filesystem02
   ```

3. Execute the `quotaget` command to confirm that the quota for the user has been correctly set.

   ```
   $ sudo quotaget -u sys02 filesystem02
   List of Quota Information of File System(filesystem02):
   The number of quota information(1)
   User name : sys02
   UID       : 2002
   Block     Used capacity : 0MB(0MB)
             Soft limit    : 1GB(1024MB)
             Hard limit    : 2GB(2048MB)
             Grace period  : -
   i-node    Used count    : 0
             Soft limit    : 0
             Hard limit    : 0
             Grace period  : -
   ```

Setting quotas for groups for each file system

This section explains how to use the `quotaset` command to set quotas for groups for each file system.

The procedure assumes that a quota is set under the following conditions:

- The target file system is `filesystem02`.
- A quota is assigned to the group `unit10`.
- The soft limit on block usage is set to 15 GB, and the hard limit is set to 20 GB.

To set a quota for the group:

1. Execute the `fslist` command to confirm that the target file system is mounted with the quota functionality enabled.

   Confirm that `Quota` is `on`.

   ```
   $ sudo fslist filesystem02
   List of File Systems:
   The number of file systems(1)
    File system(used by)    : filesystem02
    Total disk capacity(GB) : 40.000
    Device status           : normal
    Device files            : lu00 lu01 lu02 lu03
    Block used(GB)          : 0.004
    Block free(GB)          : 39.860
    I-node used             : 8
    I-node free             : 41811960
    Volume manager          : use
    Mount status            : rw
    Quota                   : on
   ```

2. Execute the `quotaset` command to set the quota for the group.

   ```
   $ sudo quotaset -g unit10 -b 15G,20G filesystem02
   ```

3. Execute the `quotaget` command to confirm that the quota for the group has been correctly set.

   ```
   $ sudo quotaget -g unit10 filesystem02
   List of Quota Information of File System(filesystem02):
   The number of quota information(1)
   Group name : unit10
   GID        : 1010
   Block      Used capacity : 0MB(0MB)
              Soft limit    : 15GB(15360MB)
              Hard limit    : 20GB(20480MB)
              Grace period  : -
   i-node     Used count    : 0
              Soft limit    : 0
              Hard limit    : 0
              Grace period  : -
   ```

Setting the default quota for a file system

This section explains how to use the `quotaset` command to set the default quota for a file system.

The procedure assumes that a default quota is set for the `filesystem02` file system. For the default quota, the soft limit on block usage is set to 1 GB, and the hard limit is set to 2 GB.

To set the default quota:

1. Execute the `fslist` command to confirm that the target file system is mounted with the quota functionality enabled.
   Confirm that `Quota` is `on`.

```
$ sudo fslist filesystem02
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem02
 Total disk capacity(GB) : 40.000
 Device status           : normal
 Device files            : lu00 lu01 lu02 lu03
 Block used(GB)          : 0.004
 Block free(GB)          : 39.860
 I-node used             : 8
 I-node free             : 41811960
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
```

2. Execute the `quotaset` command to set the default quota.

```
$ sudo quotaset -d -b 1g,2g filesystem02
```

3. Execute the `quotaget` command to confirm that the default quota has been correctly set.

```
$ sudo quotaget -d filesystem02
Default Quota Information of File System(filesystem02):
Block      Soft limit(default) : 1GB(1024MB)
           Hard limit(default) : 2GB(2048MB)
i-node     Soft limit(default) : 0
           Hard limit(default) : 0
```

Setting a quota grace period for a file system

This section explains how to use the `quotaset` command to set a quota grace period for a file system.

Set a grace period for each file system. The grace period you set applies to all users and groups that use that file system.

If you later change the current grace period, the new setting will not apply to the users or groups which are in the grace period because their inode usage or block usage has already exceeded the soft limit.

The procedure assumes that the grace period for block usage is set to 10 days for the quota set for the `filesystem02` file system.

To set a grace period:

1. Execute the `fslist` command to confirm that the target file system is mounted with the quota functionality enabled.
   Confirm that `Quota` is `on`.

```
$ sudo fslist filesystem02
List of File Systems:
```

```
The number of file systems(1)
 File system(used by)    : filesystem02
 Total disk capacity(GB) : 40.000
 Device status           : normal
 Device files            : lu00 lu01 lu02 lu03
 Block used(GB)          : 0.004
 Block free(GB)          : 39.860
 I-node used             : 8
 I-node free             : 41811960
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
```

2. Execute the `quotaset` command to set the quota grace period.

```
$ sudo quotaset -t -b 10 filesystem02
```

3. Execute the `quotaget` command to confirm that the quota grace period
   has been correctly set.

```
$ sudo quotaget -t filesystem02
Grace Period Information of File System(filesystem02):
Block grace period  : 10 days
i-node grace period : 7 days
```

Setting the quota monitoring method for a file system

This section explains how to use the `quotaset` command to set the quota
monitoring method for a file system.

The procedure assumes that a quota monitoring method is set for the
`filesystem02` file system under the following conditions:

- Quota monitoring begins at 04:30.
- If users or groups that have exceeded the soft limit or grace period are
  detected, summary information is sent via an SNMP trap.

To set the quota monitoring method:

1. Execute the `fslist` command to confirm that the target file system is
   mounted with the quota functionality enabled.
   Confirm that `Quota` is `on`.

```
$ sudo fslist filesystem02
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem02
 Total disk capacity(GB) : 40.000
 Device status           : normal
 Device files            : lu00 lu01 lu02 lu03
 Block used(GB)          : 0.004
 Block free(GB)          : 39.860
 I-node used             : 8
 I-node free             : 41811960
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
```

2. Execute the `quotaset` command to set the quota monitoring method for the file system.

```
$ sudo quotaset -m -s 0430 -n summary filesystem02
```

3. Execute the `quotaget` command to confirm that the quota monitoring method is properly set for the file system.

```
$ sudo quotaget -m filesystem02
Monitoring Time of File System(filesystem02):
SNMP notification mode : Use a summary notification
04:30
```

Managing subtree quotas

This section describes how to manage subtree quotas.

Setting a quota for a directory

This section explains how to use the `stquotaset` command to set a quota for a directory.

The procedure assumes that a quota is set under the following conditions:

- A new directory is created with the name `/mnt/filesystem03/dir01` as a shared directory, and a quota is to be assigned to this directory (owner: `sys05`, owner group: `unit15`).

- The soft limit on block usage is set to 18 GB, and the hard limit is set to 20 GB.

To set a quota for the directory:

1. Execute the `fslist` command to confirm that the target file system is mounted with the quota functionality enabled.
   Confirm that `Quota` is `on`.

```
$ sudo fslist filesystem03
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem03
 Total disk capacity(GB) : 835.211
 Device status           : normal
 Device files            : lu02 lu0C lu0E lu10
 Block used(GB)          : 0.437
 Block free(GB)          : 834.530
 I-node used             : 10
 I-node free             : 875659254
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
```

2. Execute the `dircreate` command to create a shared directory.

```
$ sudo dircreate -u sys05 -g unit15 /mnt/filesystem03/dir01
```

3. Execute the `dirlist` command to confirm that the shared directory has been correctly created.

```
$ sudo dirlist -d /mnt/filesystem03/dir01
0755 sys05          unit15           /mnt/filesystem03/dir01
```

4. Execute the `stquotaset` command to set the quota for the shared directory.

```
$ sudo stquotaset -b 18G -B 20G filesystem03/dir01
```

5. Execute the `stquota` command to confirm that the quota has been correctly set for the shared directory.

```
$ sudo stquota filesystem03
*** Report for subtree quotas on file system filesystem03
              Block limits                            i-node limits
Directory        Used    Soft    Hard  Grace        Used    Soft    Hard
Grace
-------------------------------------------------------------------------
-----
dir01      --       0    18G     20G                   1      0       0
```

Setting quotas for users for each directory

This section explains how to use the `stquotaset` command to set quotas for users for each directory.

The procedure assumes that a user quota is set under the following conditions:

- The target directory is `/mnt/filesystem03/dir01/dir02`.
- A quota is assigned to users `sys03` and `sys04`.
- The soft limit on block usage is set to 900 MB, and the hard limit is set to 1 GB.

To set a quota for the users:

1. Execute the `fslist` command to confirm that the target file system is mounted with the quota functionality enabled.
   Confirm that `Quota` is `on`.

```
$ sudo fslist filesystem03
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem03
 Total disk capacity(GB) : 100.000
 Device status           : normal
 Device files            : lu11
 Block used(GB)          : 0.004
 Block free(GB)          : 99.915
 I-node used             : 13
 I-node free             : 104824819
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
```

2. Execute the `stquotaset` command to set the quota for the users.

```
$ sudo stquotaset -u -b 900M -B 1G filesystem03/dir01/dir02 sys03 sys04
```

3. Execute the `stquota` command or the `stquotalist` command to confirm that the quota for the users has been correctly set.

```
$ sudo stquota -u filesystem03 sys03 sys04
*** Report for subtree user quotas on file system filesystem03
*** User: sys03
                 Block limits                         i-node limits
Directory       Used    Soft    Hard  Grace          Used    Soft    Hard
Grace
-------------------------------------------------------------------------
-----
dir01/dir02
               --       0    900M    1.0G                0       0       0

*** User: sys04
                 Block limits                         i-node limits
Directory       Used    Soft    Hard  Grace          Used    Soft    Hard
Grace
-------------------------------------------------------------------------
-----
dir01/dir02
               --       0    900M    1.0G                0       0       0
```

```
$ sudo stquotalist -u filesystem03/dir01/dir02
*** Report for subtree user quotas on directory filesystem03/dir01/dir02
                 Block limits                         i-node limits
User            Used    Soft    Hard  Grace          Used    Soft    Hard
Grace
-------------------------------------------------------------------------
-----
sys03    --       0    900M    1.0G                0       0       0
sys04    --       0    900M    1.0G                0       0       0
```

Setting quotas for groups for each directory

This section explains how to use the `stquotaset` command to set quotas for groups for each directory.

The procedure assumes that a group quota is set under the following conditions:

- The target directory is `/mnt/filesystem03/dir01/dir02/dir03`.
- A quota is assigned to groups `unit20` and `unit21`.
- The soft limit on block usage is set to 9 GB, and the hard limit is set to 10 GB.

To set a quota for the groups:

1. Execute the `fslist` command to confirm that the target file system is mounted with the quota functionality enabled.
   Confirm that `Quota` is `on`.

```
$ sudo fslist filesystem03
List of File Systems:
```

```
The number of file systems(1)
 File system(used by)    : filesystem03
 Total disk capacity(GB) : 100.000
 Device status           : normal
 Device files            : lu11
 Block used(GB)          : 0.004
 Block free(GB)          : 99.915
 I-node used             : 13
 I-node free             : 104824819
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
```

2. Execute the `stquotaset` command to set the quota for the groups.

```
$ sudo stquotaset -g -b 9G -B 10G filesystem03/dir01/dir02/dir03 unit20
unit21
```

3. Execute the `stquota` command or `stquotalist` command to confirm that the quota for the groups has been correctly set.

```
$ sudo stquota -g filesystem03 unit20 unit21
*** Report for subtree group quotas on file system filesystem03
*** Group: unit20
                Block limits                        i-node limits
Directory       Used    Soft    Hard  Grace         Used    Soft    Hard
Grace
-----------------------------------------------------------------------------
-----
dir01/dir02/dir03
         --        0     9.0G     10G                  0       0       0

*** Group: unit21
                Block limits                        i-node limits
Directory       Used    Soft    Hard  Grace         Used    Soft    Hard
Grace
-----------------------------------------------------------------------------
-----
dir01/dir02/dir03
         --        0     9.0G     10G                  0       0       0
```

```
$ sudo stquotalist -g filesystem03/dir01/dir02/dir03
*** Report for subtree group quotas on directory filesystem03/dir01/dir02/
dir03
                Block limits                        i-node limits
Group           Used    Soft    Hard  Grace         Used    Soft    Hard
Grace
-----------------------------------------------------------------------------
-----
unit20    --        0     9.0G     10G                  0       0       0
unit21    --        0     9.0G     10G                  0       0       0
```

Setting the default quota for a directory

This section explains how to use the `stquotaset` command to set the default quota for a directory.

The procedure assumes that the default quota is set under the following conditions:

- The target directory is `/mnt/filesystem03/dir01/dir02/dir03`.

Command Operations

Hitachi Data Ingestor CLI Administrator's Guide

- The soft limit on block usage is set to 700 MB, and the hard limit is set to 750 MB.

To set the default quota for a directory:

1. Execute the `fslist` command to confirm that the target file system is mounted with the quota functionality enabled.

   Confirm that `Quota` is `on`.

```
$ sudo fslist filesystem03
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem03
 Total disk capacity(GB) : 100.000
 Device status           : normal
 Device files            : lu11
 Block used(GB)          : 0.004
 Block free(GB)          : 99.915
 I-node used             : 14
 I-node free             : 104824818
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
```

2. Execute the `stquotaset` command to set the default quota.

```
$ sudo stquotaset -d -b 700M -B 750M filesystem03/dir01/dir02/dir03
```

3. Execute the `stquota` command to confirm that the default quota has been correctly set.

```
$ sudo stquota -d filesystem03
*** Report for subtree user quotas on file system filesystem03
                Default block limits    Default i-node limits
Directory               Soft    Hard    Soft    Hard
-----------------------------------------------------------------------------
-----
dir01/dir02/dir03       700M    750M    0       0
```

Applying a quota to an existing directory

This section explains how to use the `stquotaset` command to apply a quota to an existing directory. When a quota is applied, the inode usage and block usage under the target directory are used to calculate the quota usage.

The procedure assumes that a quota is applied under the following conditions:

- A quota is applied to an existing directory with the name `/mnt/filesystem00/dir01/dir02`.
- The soft limit on block usage is set to 18 GB, and the hard limit is set to 20 GB.

To apply a quota to an existing directory:

1. Execute the `stquotaset` command to set the size of the target directory.

```
$ sudo stquotaset -b 18G -B 20G filesystem00/dir01/dir02
```

2. Execute the `stquotaset` command to apply the quota to the existing directory.

   The inode usage and block usage for the directories and files under the target directory will be recorded as the quota usage. When this command is executed for a directory that contains 100,000 files, about 30 seconds is required for the processing to finish.

```
$ sudo stquotaset -x filesystem00/dir01/dir02
filesystem00/dir01/dir02: Wait ............. Success
```

3. Execute the `stquota` command to confirm that the quota has been applied to the existing directory.

```
$ sudo stquota filesystem00
*** Report for subtree quotas on file system filesystem00
              Block limits                              i-node limits
Directory       Used    Soft    Hard  Grace          Used    Soft    Hard
Grace
-----------------------------------------------------------------------------
-----
dir01/dir02
              --     3.7M     18G     20G            100002      0       0
```

Setting a quota grace period for a directory

This section explains how to use the `stquotaset` command to set a quota grace period for a directory.

There are three types of grace periods for a subtree quota: directory grace period, user grace period, and group grace period. A user grace period applies to all users who use the directory. A group grace period applies to all groups that use the directory. You cannot set different grace periods for individual users or groups.

If you later change the current grace period, the new setting will not apply to the users or groups which are in the grace period because their inode usage or block usage has already exceeded the soft limit.

The procedure assumes that a grace period is set under the following conditions:

- The target directory is `/mnt/filesystem03/dir01/dir02`.
- A user grace period is set.
- The grace period for block usage is set to 10 days.

To set a grace period:

1. Execute the `fslist` command to confirm that the target file system is mounted with the quota functionality enabled.
   Confirm that `Quota` is `on`.

```
$ sudo fslist filesystem03
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem03
 Total disk capacity(GB) : 100.000
 Device status           : normal
 Device files            : lu11
 Block used(GB)          : 0.004
 Block free(GB)          : 99.915
 I-node used             : 10
 I-node free             : 104824822
 Volume manager          : use
 Mount status            : rw
 Quota                   : on
```

2. Execute the `stquotaset` command to set the quota grace period.

```
$ sudo stquotaset -t -u -b 10 filesystem03/dir01/dir02
```

3. Execute the `stquota` command to confirm that the grace period for the quota has been correctly set.

```
$ sudo stquota -t -u filesystem03
*** Report for subtree user quotas on file system filesystem03
Directory               Block grace time    i-node grace time
-------------------------------------------------------------------------------
-----
dir01/dir02                         10days                  7days
```

Setting the quota monitoring method for each directory

This section explains how to use the `stquotaset` command to set quota monitoring methods for each directory.

The subtree quota monitoring method can be set for each file system or directory. If you set the monitoring method for a file system, all directories immediately under the mount point for which subtree quota is set are monitored.

The procedure assumes that the monitoring method is set under the following conditions:

- The target directory is `/mnt/filesystem03/dir01/dir02`.
- Quota monitoring begins at 01:05 and 13:15.

To set quota monitoring method:

1. Execute the `fslist` command to confirm that the target file system is mounted with the quota functionality enabled.
   Confirm that `Quota` is `on`.

```
$ sudo fslist filesystem03
List of File Systems:
The number of file systems(1)
 File system(used by)    : filesystem03
 Total disk capacity(GB) : 100.000
```

```
Device status         : normal
Device files          : lu11
Block used(GB)        : 0.004
Block free(GB)        : 99.915
I-node used           : 13
I-node free           : 104824819
Volume manager        : use
Mount status          : rw
Quota                 : on
```

2. Execute the `stquota` command to confirm that the quota has been set for the directory.

```
$ sudo stquota filesystem03
*** Report for subtree quotas on file system filesystem03
            Block limits                           i-node limits
Directory        Used    Soft     Hard  Grace       Used    Soft     Hard
Grace
--------------------------------------------------------------------------
-----
dir01/dir02
          --        0     18G      20G               1       0        0
```

3. Execute the `stquotaset` command to set the quota monitoring method for the directory.

```
$ sudo stquotaset -m -s 0105,1315 -n individual filesystem03/dir01/dir02
```

4. Execute the `stquota` command to confirm that the quota monitoring method is properly set for the directory.

```
$ sudo stquota -m filesystem03
*** Report for the monitoring start time on file system filesystem03
*** Settings for the file system
KAQG91214-I There is no item to display.
*** Settings for the directory dir01/dir02
SNMP notification mode : Use individual notifications
SNMP notification time : 01:05
                         13:15
```

Management of system settings

This section explains how to manage system settings.

The cluster management LU takes approximately three minutes to save, and the OS disks take approximately one minute each.

If a load is placed on the node, the processing to save the system LUs might time out and stop while the load on the node is being reduced. If this occurs, after the load on the node has lessened and become stable, save the system LUs again. To periodically save the system LUs, set up a schedule that executes the save process on a date and time when the load on the node is low.

Hitachi Data Ingestor CLI Administrator's Guide

Before saving the system LUs:

You cannot save the system LUs 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.

If you want to output the system settings file to the home directory of the SSH account (`/home/nasroot`), make sure that the system settings file is not in the `/home/nasroot` directory.

To output the system settings file to a shared directory in a file system, the file system must be mounted as read/write-enabled for the node on which you want to perform manual saving or periodic saving. We also recommend that only system administrators be permitted to access a file share or shared directory to which the system settings file is to be output.

Saving system LUs and outputting the system settings file to the home directory

This subsection describes how to use the `syslusave` command to save system LUs and output the system settings file to the SSH account home directory (`/home/nasroot`).

Before performing this procedure, review the information in *Before saving the system LUs:* in .

The procedure assumes that the system LUs containing the system settings file `sysbk_FC-GW4230NC0-T108000063_20110911_0638.tgz` are to be saved.

To save the system LUs:

1. Execute the `syslusavestatus` command to check the save status of the system LUs.
   Make sure that `Normal` is displayed for `Save status` under `Cluster management LU save status` and that `Normal` is displayed for `Save status` for both nodes under `OS disk save status`.

```
$ sudo syslusavestatus
Setting save status
Transfer all system settings : 2011/09/11 05:45
Download all system settings : 2011/09/11 06:24

Cluster management LU save status
 Save status     : Normal
 Last save date : 2011/09/11 06:25

OS disk save status
 node 0(DT108000063)
 Save status     : Normal
 Last save date : 2011/09/11 06:24

 node 1(DT108000064)
 Save status     : Normal
 Last save date : 2011/09/11 06:24
```

2. Execute the `syslusave` command to save the system settings file in the home directory of the SSH account (`/home/nasroot`).

```
$ sudo syslusave -o
KAQM13128-I The settings were successfully saved. Transfer the settings
file to an external location, and then erase the file stored in the
system. (output file = sysbk_FC-GW4230NC0-T108000063_20110911_0638.tgz)
```

3. Execute the `syslusavestatus` command to confirm that the system LUs have been saved correctly.

   Make sure that `Normal` is displayed for `Save status` under `Cluster management LU save status` and that `Normal` is displayed for `Save status` for both nodes under `OS disk save status`. Also confirm that the date and time displayed for `Download all system settings` have been updated.

```
$ sudo syslusavestatus
Setting save status
Transfer all system settings : 2011/09/11 05:45
Download all system settings : 2011/09/11 06:38

Cluster management LU save status
 Save status     : Normal
 Last save date : 2011/09/11 06:40

OS disk save status
 node 0(DT108000063)
 Save status     : Normal
 Last save date : 2011/09/11 06:39

 node 1(DT108000064)
 Save status     : Normal
 Last save date : 2011/09/11 06:39
```

4. On the remote host, use the `scp` command to transfer the system settings file from the `/home/nasroot` directory to the remote host.

```
$ scp nasroot@fshost01:sysbk_FC-GW4230NC0-
T108000063_20110911_0638.tgz .sysbk_FC-GW4230NC0-T10800
sysbk_FC-GW4230NC0-
T108000063_20110911_0638.tgz                              100%
695KB 694.7KB/s   00:00
```

5. Execute the `rmfile` command to delete the system settings file from the `/home/nasroot` directory.

```
$ sudo rmfile sysbk_FC-GW4230NC0-T108000063_20110911_0638.tgz
KAQM16173-Q Do you want to delete the specified file? (y/n) y
```

Saving system LUs and outputting the system settings file to a file system

This subsection describes how to use the `syslusave` command to save system LUs and output the system settings file to a shared directory in a file system.

Before performing this procedure, review the information in *Before saving the system LUs:* in Management of system settings on page 3-80.

The procedure assumes that the system LUs are saved under the following conditions:

- The name of the shared directory to which the system settings file is to be output is `/mnt/filesystem01/backup`.
- The system settings file name is `sysbk_FC-GW4230NC0-T108000063_20110911_1223.tgz`.

To manually save the system settings file in the file system:

1. Execute the `syslusavestatus` command to check the save status of the system LUs.

   Make sure that `Normal` is displayed for `Save status` under `Cluster management LU save status` and that `Normal` is displayed for `Save status` for both nodes under `OS disk save status`.

   ```
   $ sudo syslusavestatus
   Setting save status
   Transfer all system settings : 2011/09/11 05:45
   Download all system settings : 2011/09/11 06:38

   Cluster management LU save status
    Save status     : Normal
    Last save date : 2011/09/11 06:40

   OS disk save status
    node 0(DT108000063)
    Save status     : Normal
    Last save date : 2011/09/11 06:39

    node 1(DT108000064)
    Save status     : Normal
    Last save date : 2011/09/11 06:39
   ```

2. Execute the `syslusave` command to save the system settings file in the shared directory of the file system.

   ```
   $ sudo syslusave -d /mnt/filesystem01/backup
   KAQM13128-I The settings were successfully saved. Transfer the settings
   file to an external location, and then erase the file stored in the
   system. (output file = sysbk_FC-GW4230NC0-T108000063_20110911_1223.tgz)
   ```

3. Execute the `syslusavestatus` command to confirm that the system LUs have been saved correctly.

   Make sure that `Normal` is displayed for `Save status` under `Cluster management LU save status` and that `Normal` is displayed for `Save status` for both nodes under `OS disk save status`. Also confirm that the date and time displayed for `Download all system settings` have been updated.

   ```
   $ sudo syslusavestatus
   Setting save status
   Transfer all system settings : 2011/09/11 05:45
   Download all system settings : 2011/09/11 12:23

   Cluster management LU save status
   ```

```
 Save status    : Normal
 Last save date : 2011/09/11 12:25

OS disk save status
 node 0(DT108000063)
 Save status    : Normal
 Last save date : 2011/09/11 12:23

 node 1(DT108000064)
 Save status    : Normal
 Last save date : 2011/09/11 12:23
```

4. Use a command provided by the file share client to transfer the system settings file to a location external to the file system.

5. Use a command provided by the file share client to delete the system settings file in the shared directory.

Changing the settings for periodic saving for the system LU

This section explains how to use the `sysluscheduleset` command to change the settings for periodically saving the system LUs.

The procedure assumes that the settings are changed as follows:

- The periodic saving interval for the system LUs is to be changed to daily at 12:30 on Sunday through Tuesday.

- The system settings file is to be output to the directory `/mnt/FS01/dir`.

To change the settings for periodically saving the system LUs:

1. Execute the `sysluscheduleget` command to view the settings for periodically saving the system LUs.

```
$ sudo sysluscheduleget
Schedule settings for saving all system settings
Schedule setting status : On
Schedule interval      : Daily
Schedule time          : 00:07
Output setting         : -
```

2. Execute the `sysluscheduleset` command to change the settings for periodically saving the system LUs.

```
$ sudo sysluscheduleset -S W-Sun,Mon,Tue-1230 -d /mnt/FS01/dir
```

3. Execute the `sysluscheduleget` command to confirm that the settings for periodically saving the system LUs has been changed.

```
$ sudo sysluscheduleget
Schedule settings for saving all system settings
Schedule setting status : On
Schedule interval      : Weekly
                         Day of week : Sun,Mon,Tue
Schedule time          : 12:30
Output setting         : /mnt/FS01/dir
```

Restoring the system LUs

This section explains how to use the `syslurestore` command to restore the system LUs. For details on how to restore the system LUs, see the *Troubleshooting Guide*.

For details on how to restore system LUs from the system settings file saved on an HCP system, see the applicable usage example in syslurestore (Restore system LUs) on page 2-620.

The examples in the procedure assume that the system LUs are restored under the following conditions:

- The system LUs are to be restored in a batch operation.
- The system settings file is to be transferred from the remote host to the home directory of the SSH account (`/home/nasroot`).
- The system settings file name is `sysbk_FC-GW79RMPBX_20101117_1330.tgz`.

To restore the system LUs:

1. On the remote host, use the `scp` command to transfer the system settings file from the remote host to the `/home/nasroot` directory.

```
$ scp sysbk_FC-GW79RMPBX_20101117_1330.tgz nasroot@fshost01:/home/nasroot
sysbk_FC-
GW79RMPBX_20101117_1330.tgz
100%  518KB 517.7KB/s   00:00
```

2. Log in to the target node by using SSH.

```
$ ssh -2 nasroot@fshost01
```

3. Execute the `syslurestore` command to restore the system LUs.
   A confirmation message appears. Enter `y` to restore the system LUs.

```
$ sudo syslurestore -f sysbk_FC-GW79RMPBX_20101117_1330.tgz
KAQM13133-Q Processing might take a while. Do you want to restore the
system settings by using the specified file (saved date and time =
2010/11/17 13:30)? (y/n)y
```

4. Execute the `rmfile` command to delete the system settings file.

```
$ sudo rmfile sysbk_FC-GW79RMPBX_20101117_1330.tgz
KAQM16173-Q Do you want to delete the specified file? (y/n) y
```

Linking to an HCP system

This section explains how to specify the settings for linking to an HCP system.

Changing the information of the migration destination HCP system

This section explains how to use the `archcpset` command to change the information about the migration-destination HCP system.

The procedure assumes that the information is changed under the following conditions:

- The information is to be specified interactively.
- The HCP host name (as a fully qualified domain name) is `hcp.example.com`, and will not be changed.
- The HCP host name (as a fully qualified domain name) is not set, but will be set to `hcp.example2.com`.
- The HCP tenant name will be changed from `tenant01` to `tenant02`.
- The data access account (user name: `user02`) used to access all namespaces in the new tenant is to be specified, and the password is to be changed to the one for that account.
- The IP address that has been made external and is used to connect to the HCP system is not set, but will be set to `123.45.67.89`.
- The IP address that has been made external and is used to connect to the replica HCP system is not set, but will be set to `123.45.67.99`.

To change the information of the migration destination HCP system:

1. Execute the `archcpget` command to check the currently registered HCP system information.

   ```
   $ sudo archcpget
   HCP host name          : hcp.example.com
   Replica HCP host name :
   HCP tenant name        : tenant01
   HCP account user       : user01
   External host          :
   External replica host :
   ```

2. Execute the `archcpset` command to change the information of the migration destination HCP system.

   Enter the new value for each item. Enter the value for the item that is not to be changed (host name) as well.

   ```
   $ sudo archcpset
   HCP host name : hcp.example.com
   Replica HCP host name (If replica HCP is not used, simply press the
   [Enter] key.) : hcp.example2.com
   HCP tenant name : tenant02
   HCP account user : user02
   HCP account password :
   confirm password :
   External HCP host name (To communicate with HCP directly, press the
   [Enter] key.) : 123.45.67.89
   External replica HCP host name (To communicate with the replica HCP
   directly, press the [Enter] key.) : 123.45.67.99
   ```

   Note:

The character strings you enter for `HCP account password` and `confirm password` are not displayed.

3. Execute the `archcpget` command to confirm that the information of the migration destination HCP system has been changed.

```
$ sudo archcpget
HCP host name         : hcp.example.com
Replica HCP host name : hcp.example2.com
HCP tenant name       : tenant02
HCP account user      : user02
External host         : 123.45.67.89
External replica host : 123.45.67.99
```

Changing the HCP communication setting

This section explains how to use the `arcsslctl` command to change the setting for communication with an HCP system.

The procedure assumes that the setting is changed to disable the use of HTTPS.

To change the HCP communication setting:

1. Execute the `arcsslctl` command to check the current HCP communication setting.

```
$ sudo arcsslctl
Protocol setting: HTTPS
```

2. Execute the `arcsslctl` command to change the setting so that HTTPS is not used for communication with HCP systems.

```
$ sudo arcsslctl --disable
```

3. Execute the `arcsslctl` command to confirm that the HCP communication setting has been changed.

```
$ sudo arcsslctl
Protocol setting: HTTP
```

Changing proxy server information

This section explains how to use the `arcproxyset` command to change the proxy server information.

The procedure assumes that the proxy server information is changed under the following conditions:

* The information is to be specified interactively.
* The host name of the proxy server is `proxy.example.com`, and is not to be changed.
* The port number used for the proxy server is to be changed to `8081`.

- The user name used for authentication on the proxy server is to be changed to `user02`, and the password is to be changed to the password for the new user name.

To change the proxy server information:

1. Execute the `arcproxyget` command to check the current proxy server information.

```
$ sudo arcproxyget
Proxy host        : proxy.example.com
Proxy port        : 8080
Proxy account user : user01
```

2. Execute the `arcproxyset` command to change the proxy server information.

   Enter the new value for each item. Do not enter anything for the item that is not to be changed (host name).

```
$ sudo arcproxyset
host:
port: 8081
user-name: user02
password:
confirm password:
```

Note:
   The character strings you entered for `password` and `confirm password` are not displayed.

3. Execute the `arcproxyget` command to confirm that the proxy server information has been changed.

```
$ sudo arcproxyget
Proxy host        : proxy.example.com
Proxy port        : 8081
Proxy account user : user02
```

Changing the stub threshold

This section explains how to use the `arcreplimitset` command to change the current stub threshold. The stub threshold is the threshold (the remaining disk capacity) at which stub processing is performed.

The procedure assumes that the threshold is changed under the following conditions:

- The file system name is `FS_1`.
- The stub threshold is changed to 100 GB.

To change the stub threshold:

1. Execute the `arcreplimitget` command to view the current stub threshold.

```
$ sudo arcreplimitget --file-system FS_1
Replication limit rest size : 10%
```

2. Execute the `arcreplimitset` command to change the stub threshold.

```
$ sudo arcreplimitset --rest-size 100g --file-system FS_1
```

3. Execute the `arcreplimitget` command to confirm that the stub threshold
   has been changed.

```
$ sudo arcreplimitget --file-system FS_1
Replication limit rest size : 100GB
```

Managing a data import from another file server

This section explains how to import data used by another file server to an
HDI system.

For details on how to import data, see the *Installation and Configuration
Guide*.

The procedure assumes that data is imported by using CIFS shares.

Adding data import definition information about another file server

This section explains how to use the `datamigrateconfadd` command to add
the data import definition information of another file server.

The procedure assumes that the data import definition information is added
under the following conditions:

- The host name of the import-source file server is `host`.
- The CIFS share name of the import-source file server is `share`.
- The directory path to the HDI system is `/mnt/fs01/share`.
- The user name of the import-source file server is `user01`.
- The password for the import-source file server is `pass01`.

1. Execute the `datamigrateconflist` command to view the data import
   definition information of other file servers.

```
$ sudo datamigrateconflist
List of CIFS Migration Definitions
```

2. Execute the `datamigrateconfadd` command to add the data import
   definition information of another file server.

```
$ sudo datamigrateconfadd --source "host\share" --destination /mnt/fs01/
share --user user01 --password pass01
```

3. Execute the `datamigrateconflist` command to confirm that the data
   import definition information of the file server has been added.

```
$ sudo datamigrateconflist --source "host\share"
List of CIFS Migration Definitions
CIFS migration definition number (1)
 Migration-source host name      : host
 Migration-source share name     : share
 User name                       : user01
 Migration-destination directory : /mnt/fs01/share
 File share migration status     : not execute
```

Starting an import from another file server

This section explains how to use the `datamigratestart` command to start a data import from another file server to an HDI system.

1. Execute the `datamigratestart` command to start an import from another file server to the HDI system.

```
$ sudo datamigratestart --source "host\share"
```

Managing data import settings

This section explains how to manage both the settings for data migrations from an HDI system to the HCP system and the settings for data imports from another file server to an HDI system.

Changing data import settings

This section explains how to use the `arcconfedit` command to change both the settings for data migrations from an HDI system to the HCP system and the settings for data imports from another file server to an HDI system.

The execution examples in the procedures below are used to change the settings for data migrations to the HCP system so that the following conditions are satisfied:

- Thread pool used for data migrations to the HCP system:

  - The maximum number of threads is changed to 60.
  - The minimum number of threads is changed to 20.

- Thread pools not used for data migrations to the HCP system:

  - The maximum number of threads is set to 50 and will not be changed.
  - The minimum number of thread is set to 20 and will not be changed.

- The maximum number of retries for communication with an HCP system is changed to 5.

- Transfer speed to an HCP system is set to 0 bytes per second and will not be changed.

- The timeout period for communication with an HCP system is changed to 10,000 seconds.

- The HCP connection timeout value is changed to 500 seconds.
- The minimum transfer speed to an HCP system is changed to 12,000 bytes per second.
- The time period for monitoring transfer speed to an HCP system is changed to 300 seconds.
- A setting is changed so that HTTP messages are compressed for communication with HCP systems.
- The maximum number of retries performed when migrating data to an HCP system is changed to 10.
- The retry interval when migrating data to an HCP system is changed to 20 seconds.

To change the data migration settings:

1. Execute the `arcconflist` command to view the current settings.

```
$ sudo arcconflist
Thread configuration
  Thread pool                 : archive
    Thread max                : 30
    Thread min                : 10
  Thread pool                 : other
    Thread max                : 50
    Thread min                : 20
HCP communication configuration
  Retry max                   : 1
  Transfer speed(byte/s)      : 0
  Timeout(s)                  : 10800
  Connect timeout(s)          : 300
  Low speed(byte/s)           : 11650
  Low speed time(s)           : 180
  Compression                 : disable
Migration configuration
  Update retry max            : 5
  Update retry interval(s)    : 10
File Server communication configuration
  Retry max                   : 1
  Timeout(s)                  : 300
```

2. Execute the `arcconfedit` command to change the settings.

```
$ sudo arcconfedit --thread-min 20 --thread-max 60 --thread-pool archive --
retry-max 5 --comm-timeout 10000 --conn-timeout 500 --low-speed 12000 --
low-speed-time 300 --comm-compression enable --update-retry-max 10 --
update-retry-interval 20
```

3. Execute the `arcconflist` command to confirm that the settings have been changed.

```
$ sudo arcconflist
Thread configuration
  Thread pool                 : archive
    Thread max                : 60
    Thread min                : 20
  Thread pool                 : other
    Thread max                : 50
    Thread min                : 20
HCP communication configuration
  Retry max                   : 5
  Transfer speed(byte/s)      : 0
```

```
   Timeout(s)                : 10000
   Connect timeout(s)        : 500
   Low speed(byte/s)         : 12000
   Low speed time(s)         : 300
   Compression               : enable
Migration configuration
   Update retry max          : 10
   Update retry interval(s)  : 20
File Server communication configuration
   Retry max                 : 1
   Timeout(s)                : 300
```

Managing the NDMP server

This section explains how to manage the NDMP server.

Controlling the NDMP server

This subsection explains how to control the NDMP server by using the `ndmpcontrol` command.

The procedure below assumes that the NDMP server is not running and will be started.

To control the NDMP server:

1. Execute the `ndmpcontrol` command to check whether the NDMP server can be started.

   In the command execution result, if S is displayed under `allowrequest`, the NDMP server can be started.

   ```
   $ sudo ndmpcontrol -l
   Aug 14 11:26:15 KAQB11500-I ndmpcontrol command execution has started.
   Aug 14 11:26:15 KAQB12201-I Operating statuses of NDMP servers:
   NDMPsvrstatus allowrequest pid   connectstatus
   ----------------------------------------------
   stopped       L,S,F,H            disconnected
   Aug 14 11:26:15 KAQB11501-I ndmpcontrol command has finished.
   ```

2. Execute the `ndmpcontrol` command to start the NDMP server.

   ```
   $ sudo ndmpcontrol -s
   ```

3. Execute the `ndmpcontrol` command to confirm that the NDMP server is up and running.

   If `running` is displayed under `NDMPsvrstatus`, the NDMP server is running.

   ```
   $ sudo ndmpcontrol -l
   ...
   NDMPsvrstatus allowrequest pid   connectstatus
   ----------------------------------------------
   running       L,R,Q,F,H    1381 disconnected
   ...
   ```

Changing the NDMP server password

This subsection explains how to change the NDMP server password by using the `ndmppasswd` command.

In the following procedure, the same password will be set for the NDMP servers on both nodes in the cluster.

To change the NDMP server password:

1. Execute the `ndmppasswd` command to change the NDMP server password.

    If the command is executed interactively, enter text when the prompt for each item is displayed.

    ```
    $ sudo ndmppasswd
    Jan 12 02:07:18 KAQB11502-Q Enter the value of the displayed parameter
    name, and then press 'Enter'.
    userid=root
    oldpasswd=
    newpasswd=
    confirmpasswd=
    Jan 12 02:07:43 KAQB11500-I ndmppasswd command execution has started.
    Jan 12 02:07:43 KAQB11705-W Items are applied only to the logged-in node.
    If necessary, log in to each node on the cluster and check each setup.
    Jan 12 02:07:43 KAQB11501-I ndmppasswd command has finished.
    ```

2. Log in again to the other node in the cluster, and then perform step 1 again for that node.

3. In the backup management software, change the settings related to the NDMP server.

    For an overview of the above tasks, see the supplementary Backup Restore documentation that is provided with HDI.

Changing the NDMP server configuration information

The system administrator can use the `ndmpconfig` command to change the NDMP server configuration information.

This subsection explains how to change the NDMP server timeout value. The example assumes the following conditions:

*   Changing the default timeout value of 480 minutes to 720 minutes.
*   Setting the same value (720 minutes) for the NDMP servers on both nodes in the cluster.

To change the timeout information for the NDMP server:

1. Execute the `ndmpconfig` command to check the current timeout value.

    Check the messages for `server_timeout`.

    ```
    $ sudo ndmpconfig -l server_timeout
    Aug 14 11:32:38 KAQB11500-I ndmpconfig command execution has started.
    Aug 14 11:32:38 KAQB12216-I NDMP server time-out information:
        server_timeout 480
    Aug 14 11:32:38 KAQB11501-I ndmpconfig command has finished.
    ```

2. Execute the `ndmpcontrol` command to make sure of the following:

- The NDMP server is running normally.

  Make sure that `running` is displayed for `NDMPsvrstatus`.

- No backup or restore operation is being performed.

  Make sure that `disconnected` is displayed for `connectstatus`.

```
$ sudo ndmpcontrol -l
Aug 14 11:34:05 KAQB11500-I ndmpcontrol command execution has started.
Aug 14 11:34:06 KAQB12201-I Operating statuses of NDMP servers:
NDMPsvrstatus allowrequest pid   connectstatus
--------------------------------------------
running       L,R,Q,F,H    1381 disconnected
Aug 14 11:34:06 KAQB11501-I ndmpcontrol command has finished.
```

3. Execute the `ndmpconfig` command to change the NDMP server timeout information.

   When the timeout information for the NDMP server is changed, the NDMP server automatically restarts.

```
$ sudo ndmpconfig -m server_timeout 720
```

4. Execute the `ndmpconfig` command to make sure that the timeout value was changed correctly.

   Make sure that the timeout value you set for `server_timeout` is displayed.

```
$ sudo ndmpconfig -l server_timeout
...
    server_timeout 720
...
```

5. Log in again to the other node in the cluster, and then perform steps 1 to 4 again for that node.

Changing the conditions for interrupting an offline backup

The system administrator can use the `ndmpfsconfig` command to change the conditions for interrupting an offline backup.

This subsection explains how to change the conditions for interrupting an offline backup. The example assumes the following conditions:

- The current conditions for interrupting an offline backup of the file system (`FS1`) are set so that offline backup processing continues even if a file is modified or deleted during the offline backup (the accuracy check of the offline backup is not enhanced).

- The conditions for interrupting an offline backup of the file system (`FS1`) are changed so that offline backup processing is interrupted if a file is modified or deleted during the offline backup (the accuracy check of the offline backup is enhanced).

To change the conditions for interrupting an offline backup:

1. Execute the `fslist` command to make sure that the file system for which the conditions for interrupting an offline backup is to be changed is mounted.

    If the file system is not mounted, mount it. If you cannot check the status from the failed-over node, execute the command on the other node in the cluster.

    ```
    $ sudo fslist -c
    FS1:1.000:normal:lu4A:0.004:0.959:8:1015800:use:rw:on
    FS2:1.000:normal:lu4B:0.004:0.959:8:1015800:use:rw:on
    fstest:1.000:normal:lu50:::::use:--:--
    ```

2. Execute the `ndmpfsconfig` command to check the currently set conditions for interrupting an offline backup.

    You can see that offline backup processing is set to continue even if a file is modified or deleted during the offline backup because `Off` is displayed for `Improved backup data accuracy check`.

    ```
    $ sudo ndmpfsconfig -l FS1
    Mar  8 09:31:48 KAQB11500-I ndmpfsconfig command execution has started.
    The number of file systems(1)
     File system                       : FS1
     Improved backup data accuracy check : Off
    Mar  8 09:31:49 KAQB11501-I ndmpfsconfig command has finished.
    ```

3. Execute the `ndmpfsconfig` command to change the settings so that offline backup processing is interrupted if a file is updated during an offline backup of the file system (`FS1`).

    ```
    $ sudo ndmpfsconfig -a -p accurate-check FS1
    Mar  8 09:19:30 KAQB11500-I ndmpfsconfig command execution has started.
    Mar  8 09:19:31 KAQB11501-I ndmpfsconfig command has finished.
    ```

4. Execute the `ndmpfsconfig` command to make sure that the conditions for interrupting an offline backup was changed correctly.

    Make sure that `On` is displayed for `Improved backup data accuracy check`.

    ```
    $ sudo ndmpfsconfig -l FS1
    Mar  8 09:20:07 KAQB11500-I ndmpfsconfig command execution has started.
    The number of file systems(1)
     File system                       : FS1
     Improved backup data accuracy check : On
    Mar  8 09:20:08 KAQB11501-I ndmpfsconfig command has finished.
    ```

Managing tape drives

This section explains how to manage tape drives.

Registering tape drives collectively

When a tape device connected to a node via a SAN is used for the first time or after a tape device has been replaced, all tape drives need to be registered on the NDMP server. This subsection describes how to register all the tape drives at the same time.

To register tape drive information on the NDMP server:

1. Ask the SAN administrator to make sure that the target tape devices are set up (for example, the tape devices are connected, or the FC switch zones are set up).

2. Use backup management software to make sure that no backup or restore jobs are being performed on any of the nodes.

3. Execute the `tapelist` command with the `-d` option specified to confirm that the tape drives are connected to the node and that they are running.

   In the `Status` column, confirm that the first of the two letters, which indicates the connection status of a tape drive, is `D` for each drive.

```
$ sudo tapelist -d
Jan 12 05:19:40 KAQB11500-I tapelist command execution has started.
Jan 12 05:19:40 KAQB12225-I The list of tape device information will now
be displayed.
WWN              LUN Status Model            Type            Path
-----------------------------------------------------------------------
---------------
500104f000944a83   0 D,D   Ultrium 3-SCSI   Sequential-Access /dev/
500104f000944a83/nst00
500104f000944a86   0 D,D   Ultrium 3-SCSI   Sequential-Access /dev/
500104f000944a86/nst00
Jan 12 05:19:40 KAQB11501-I tapelist command has finished.
```

4. Execute the `tapeadd` command with the `-a` option specified to register all the tape drives on the NDMP server.

   The NDMP server automatically restarts after the tape drive is registered on it.

```
$ sudo tapeadd -a
```

5. Execute the `tapelist` command without any options specified to confirm that the tape drive information is registered on the NDMP server.

   In the `Status` column, confirm that the second of the two letters, which indicates the registration status of a tape drive, is `A` for each drive.

```
$ sudo tapelist
...
WWN              LUN Status Model            Type            Path
-----------------------------------------------------------------------
---------------
500104f000944a83   0 -,A   Ultrium 3-SCSI   Sequential-Access /dev/
500104f000944a83/nst00
500104f000944a86   0 -,A   Ultrium 3-SCSI   Sequential-Access /dev/
500104f000944a86/nst00
...
```

Registering tape drives individually

If you add and register a tape drive after an operation has already started that is using a tape device connected to a node via the SAN has started, register the tape drive by itself.

This subsection describes how to register an individual tape drive (`WWN: 500104f000944a86`; `LUN: 0`) on the NDMP server on which another tape drive (`WWN: 500104f000944a83`; `LUN: 0`) is already registered after operation has already started using a tape drive connected to a node via the SAN.

To register the tape drive individually on the NDMP server:

1. Use backup management software to make sure that no backup or restore jobs are being performed on any of the nodes.

2. Execute the `tapelist` command with the `-D` option specified to check the information for unregistered tape drives.

   In the `Status` column, confirm that the second of the two letters, which indicates the registration status of a tape drive, is `D` for the drive.

   ```
   $ sudo tapelist -D
   Jan 12 05:22:00 KAQB11500-I tapelist command execution has started.
   Jan 12 05:22:00 KAQB12225-I The list of tape device information will now
   be displayed.
   WWN              LUN Status Model            Type           Path
   ------------------------------------------------------------------------
   ---------------
   500104f000944a86   0 D,D   Ultrium 3-SCSI   Sequential-Access /dev/
   500104f000944a86/nst00
   Jan 12 05:22:00 KAQB11501-I tapelist command has finished.
   ```

3. Execute the `tapeadd` command with the `-t` option, *WWN*, and *LUN* to register the tape drive.

   You can register more than one tape drive by specifying a WWN and LUN for each tape drive you want to register.

   The NDMP server automatically restarts after the tape drive is registered on it.

   ```
   $ sudo tapeadd -t 500104f000944a86:0
   ```

4. Execute the `tapelist` command without any options specified to confirm that the tape drive has been registered.

   In the `Status` column, confirm that the second of the two letters, which indicates the registration status of a tape drive, is `A` for the drive. Note that in addition to the information about the newly registered tape drive (`WWN: 500104f000944a86`; `LUN: 0`), the information about the previously registered tape drive (`WWN: 500104f000944a83`; `LUN: 0`) is also displayed.

   ```
   $ sudo tapelist
   ...
   WWN              LUN Status Model            Type           Path
   ------------------------------------------------------------------------
   ---------------
   500104f000944a83   0 -,A   Ultrium 3-SCSI   Sequential-Access /dev/
   500104f000944a83/nst00
   500104f000944a86   0 -,A   Ultrium 3-SCSI   Sequential-Access /dev/
   ```

```
500104f000944a86/nst00
...
```

Unregistering tape drive information

This subsection describes how to use the `tapedel` command to unregister all tape drives that are registered on an NDMP server.

To unregister all tape drive information from the NDMP server:

1. Use the backup management software to unregister the tape drives.

2. Use backup management software to make sure that no backup or restore jobs are being performed on any of the nodes.

3. Execute the `tapelist` command without any options specified to confirm that the tape drives are registered on the NDMP server.

    In the `Status` column, confirm that the second of the two letters, which indicates the registration status of a tape drive, is `A` for each drive.

```
$ sudo tapelist
Jan 12 05:24:33 KAQB11500-I tapelist command execution has started.
Jan 12 05:24:33 KAQB12225-I The list of tape device information will now
be displayed.
WWN              LUN Status Model            Type            Path
-------------------------------------------------------------------------
---------------
500104f000944a83  0 -,A    Ultrium 3-SCSI   Sequential-Access /dev/
500104f000944a83/nst00
500104f000944a86  0 -,A    Ultrium 3-SCSI   Sequential-Access /dev/
500104f000944a86/nst00
Jan 12 05:24:33 KAQB11501-I tapelist command has finished.
```

4. Execute the `tapedel` command with the `-a` option specified to unregister all tape drive information.

    After the tape drives are unregistered, the NDMP server is automatically restarted.

```
$ sudo tapedel -a
```

5. Execute the `tapelist` command with the `-d` option specified to confirm that no tape drives are registered on the NDMP server.

    In the `Status` column, confirm that the second of the two letters, which indicates the registration status of a tape drive, is `D` for each drive.

```
$ sudo tapelist -d
...
WWN              LUN Status Model            Type            Path
-------------------------------------------------------------------------
---------------
500104f000944a83  0 D,D    Ultrium 3-SCSI   Sequential-Access /dev/
500104f000944a83/nst00
500104f000944a86  0 D,D    Ultrium 3-SCSI   Sequential-Access /dev/
500104f000944a86/nst00
...
```

6. Working with the SAN administrator, remove the FC cable.

Command Operations

This operation is required when you stop using a tape device or replace a tape device.

Command Operations

How to Identify the IDs of Processes That Lock NFS Files

This appendix explains how to identify a process ID when a unique ID is displayed by the `nfslockslist` command.

☐ [Identifying a process ID when a unique ID is displayed by the nfslockslist command](#)

Identifying a process ID when a unique ID is displayed by the nfslockslist command

If you execute the `nfslockslist` command, the file lock information for an NFS client host is displayed. If the NFS client host uses Linux kernel 2.6.9 or later, unique IDs are displayed in the file lock information, instead of process IDs.

This appendix describes how to identify a process ID from a displayed unique ID. The procedure assumes that you will view file lock information for an NFS client host (host name: `ClientHost1`) that uses Linux kernel 2.6.9 or later, and that you want to identify the process IDs that correspond to unique IDs 2 and 3. Also, the procedure assumes that you will execute the command from a remote host.

To identify a process ID from a unique ID:

1. Execute the `nfslockslist` command to view the file lock information for the NFS client host.
   Check the inode numbers and paths that correspond to the unique IDs.

   ○ The inode number that corresponds to the unique ID 3 of `ClientHost1` is 142, and the path is `/mnt/nfs1/file1`.

   ○ The inode number that corresponds to the unique ID 2 of `ClientHost1` is 143, and the path is `/mnt/nfs1/file2`.

   ```
   [ClientHost]$ ssh -2 nasroot@fshost01 'sudo nfslockslist'
   1: 254:8:142 /mnt/nfs1/file1 POSIX  ADVISORY  READ  0 EOF 3
   ClientHost1 2009/12/18 16:51:57
   2: 254:8:143 /mnt/nfs1/file2 POSIX  ADVISORY  READ  0 EOF 2
   ClientHost1 2009/12/18 16:48:52
   3: 254:9:144 /mnt/nfs2/file3 POSIX  ADVISORY  READ  0 EOF 29812
   ClientHost2 2009/12/18 16:47:18
   ```

   Note that the execution result of the `nfslockslist` command is displayed in the following format:

   ```
   number: major-number:minor-number:inode-number path POSIX  ADVISORY WRITE-
   or-READ starting-offset-of-file-lock ending-offset-of-file-lock process-ID
   host-name-or-IP-address date-and-time-at-which-the-file-lock-was-obtained-
   or-date-and-time-from-which-the-file-lock-waiting-to-be-obtained-starts
   ```

2. Check the contents of the `/proc/locks` file.
   In the `/proc/locks` file, check the inode number that matches the inode number displayed by using the `nfslockslist` command.

   If there is only one inode number that matches the displayed number:
   > In the `/proc/locks` file, check the process ID that corresponds to the inode number displayed by using the `nfslockslist` command.
   >
   > You can identify 20197 as the process ID that corresponds to the unique ID 3 because the process ID 20197 in the `/proc/locks` file corresponds to the inode number 142 for the unique ID 3.

   If there are multiple inode numbers that match the displayed number:

Go to step 3.

```
[ClientHost1]$ grep 142 /proc/locks
1: POSIX ADVISORY READ 20197 00:1a:142 0 0
[ClientHost1]$ grep 143 /proc/locks
3: POSIX ADVISORY READ 20156 00:1b:143 0 0
4: POSIX  ADVISORY  READ  20157 00:1a:143 0 0
```

Note that the format of the `/proc/locks` file differs depending on the platform of the NFS client host. For details on the display format, see the documentation for the OS being used.

3. In the `/proc/locks` file, check the process ID that corresponds to the inode number displayed by using the `nfslockslist` command.

   The process IDs in the `/proc/locks` file that corresponds to the inode number `143` are `20156` and `20157`.

4. Execute the `lsof` command to check the file used by the relevant process.

   Execute the `lsof` command with the process IDs `20156` and `20157` specified for the argument of the `-p` option. From the execution result, identify the path used by the internal processing of the HDI system.

   ○ The path that corresponds to the process ID `20156` is `/mnt/nfs1/file2`.

   ○ The path that corresponds to the process ID `20157` is `/mnt/nfs2/file3`.

```
[ClientHost1]$ lsof -p 29020,29004
COMMAND   PID   USER   FD   TYPE DEVICE   SIZE   NODE NAME
rdwr2   20156  user1   3ur  REG   0,26     20   143
/home/usr1/testdir/file2 (os:/mnt/nfs1)
rdwr2   20157  user1   3ur  REG   0,27     20   143
/home/usr2/testdir/file3 (os:/mnt/nfs2)
```

5. From the execution result, check the process ID that corresponds to the path for the unique ID.

   You can identify `20156` as the process ID that corresponds to the unique ID `2` because the process ID `20156` corresponds to the path `/mnt/nfs1/file2` for the unique ID `2` checked in step 1.

How to Identify the IDs of Processes That Lock NFS Files

B

Batch-Registering or Batch-Deleting Local Users or Groups

The system administrator can batch-register and batch-delete local users or local groups.

☐ [Format of a CSV file used for batch registration or batch deletion of user information](#)

☐ [Format of result file used for batch registration or batch deletion of user information](#)

☐ [Format of a CSV file used for batch registration or batch deletion of group information](#)

☐ [Format of result file used for batch registration or batch deletion of group information](#)

Format of a CSV file used for batch registration or batch deletion of user information

This section explains the format of a CSV file required for batch-registering or batch-deleting users. This file will contain user password information. Make sure that it is managed properly.

Specify the name of the CSV file in no more than 255 characters. You can use alphanumeric characters, hyphens (–), and underscores (_). You can also use periods (.), except at the beginning or end of the character string.

The table below describes the information you specify in the CSV file used for batch-registering or batch-deleting user information.

Table B-1 Information specified in the CSV file used for batch-registering or batch-deleting user information

Item	Specify at registration	Specify at deletion	Description
Execution classification	Yes	Yes	Specify the data-execution classification. Specify `Data`. If you specify a hash mark (#), the line will be a comment.

Data classification	Yes	Yes	Specify the data-processing classification.
			
			`UA01`
			
			　　Specify to batch-register the data.
			
			`UD01`
			
			　　Specify to batch-delete the data.
			
			You cannot specify both `UA01` and `UD01` in the same file.

Data registration destination	Yes	No	Specify the destination where the user information is to be registered.
			
			`1`
			
			　　Register in File Services Manager.
			
			`3`
			
			　　Register in File Services Manager as users who access CIFS shares.

User name	Yes	Yes	Specify each user name in no more than 16 characters, beginning with an alphanumeric character. From the second character, you can use alphanumeric characters, hyphens (–), and underscores (_). Alphabetic characters are not case sensitive in Windows. Specify a name that is unique regardless of the case. You cannot specify a name that duplicates a user name already registered by File Services

Item	Specify at registration	Specify at deletion	Description
			Manager, the NIS server, or the LDAP server for user authentication. When adding a user that accesses CIFS shares, you cannot specify a name that duplicates the name of any existing group configured to use the ACL.
			You cannot specify the following user names which are reserved in the OS on the node:
			`avahi, avahi-autoipd, backup, bin, bind, daemon, Debian-exim, enasroot, ftp, games, gdm, gnats, haldaemon, hddsroot, hplip, hsguiroot, identd, irc, libuuid, libvirt-qemu, list, lp, mail, messagebus, man, nasroot, news, nobody, ntp, postgres, proftpd, proxy, root, service, snmp, sshd, statd, sync, sys, telnetd, uucp, vde2-net, www-data, __groupowner`
UID	Yes	No	Specify the user ID in the range from 200 to 2147483147. You cannot specify a user ID that is already registered by File Services Manager, the NIS server, or the LDAP server for user authentication. You cannot specify 65534. If user mapping is used, you cannot specify a user ID within the range set for user mapping.
GID	Yes	No	Specify the ID of the primary group to which the user belongs.
Password	Yes	No	Specify the user password, using 6 to 20 characters.
			You can use alphanumeric characters, exclamation marks (!), double quotation marks ("), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), asterisks (*), plus signs (+), commas (,), hyphens (-), periods (.), forward slashes (/), colons (:), semicolons (;), left angle brackets (<), equal signs (=), right angle brackets (>), question marks (?), at marks (@), left square brackets ([), backslashes (\), right square brackets (]), carets (^), underscores (_), grave accent marks (`), left curly brackets ({), vertical bars (|), right curly brackets (}), and tildes (~).

Item	Specify at registration	Specify at deletion	Description
Comment	Optional	No	Specify a comment about the user in no more than 32 characters.
			You can use alphanumeric characters, hash marks (#), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ((), right parentheses ()), asterisks (*), plus signs (+), hyphens (-), periods (.), forward slashes (/), semicolons (;), left angle brackets (<), right angle brackets (>), question marks (?), at marks (@), left square brackets ([), right square brackets (]), carets (^), underscores (_), left curly brackets ({), vertical bars (|), right curly brackets (}), and tildes (~). You can also use spaces, except at the beginning or end of the character string.
Affiliated group	Optional	No	Use a group name or group ID to specify the other groups to which the user belongs. A user can belong to a maximum of 32 groups. To specify multiple groups, separate the group names or IDs with commas (,) and enclose all the group names and IDs with double quotation marks (").

Legend:
Yes: Specification is necessary
Optional: Specification is optional
No: Specification is unnecessary

The following shows an example of CSV coding used to batch-register user information:

```
#execution classification,data classification,data registration
destination,user name,user ID,group ID,password,comment,affiliated group
Data,UA01,3,user04,1004,1000,password,Leader,"unit01,2000"
```

The following shows an example of CSV coding used to batch-delete user information.

```
#execution classification,data classification,,user name
Data,UD01,,user04
```

Format of result file used for batch registration or batch deletion of user information

You can output, to an execution result file, the results of checking the CSV file and the results of batch registration or deletion, and can check these results.

If you are only checking the CSV file, and the user information is correct, OK is output to the user's execution classification.

```
#execution classification,data classification,data registration
destination,user name,user ID,group ID,password,comment,affiliated group
OK,UA01,3,user04,1004,1000,password,Leader,"unit01,2000"
```

If the batch registration or deletion is successful, #Completed is output to the user's execution classification.

```
#execution classification,data classification,data registration
destination,user name,user ID,group ID,password,comment,affiliated group
#Completed,UA01,3,user04,1004,1000,password,Leader,"unit01,2000"
```

If the user information specified in the CSV file contains an error, NG(*contents-of-the-error*) is output to the user's execution classification.

```
#execution classification,data classification,data registration
destination,user name,user ID,group ID,password,comment,affiliated group
NG(The specified UID is already
registered),UA01,3,user04,1004,1000,password,Leader,"unit01,2000"
```

If the user information specified in the CSV file contains even a single error, none of the users are registered or deleted. Correct all the lines to which NG was output, check the contents of the CSV file settings again, and re-execute the batch registration or deletion.

The Table B-2 Error message, cause, and action when an error occurs at batch registration of users on page B-5 and Table B-3 Error message, cause, and action when an error occurs at batch deletion of users on page B-7 describe the error message, cause, and action to be taken when an error occurs at batch registration or batch deletion of users.

Table B-2 Error message, cause, and action when an error occurs at batch registration of users

Error message	Cause	Action
The group to which the user belongs is incorrect	There is no group corresponding to the group name or group ID specified as a group to which the user belongs.	Check the affiliated group information.
The comment is invalid	The information specified as a comment is invalid. The comment contains an invalid	Check the information specified as a comment.

Error message	Cause	Action
	character or an invalid number of characters.	
The data classification value is invalid	The information specified as the data classification is invalid.	Check the information specified as the data classification.
The value for the data registration destination is invalid	The information specified as the data registration destination is invalid.	Check the information specified as the data registration destination.
The execution classification value is invalid	The information specified as the execution classification is invalid.	Check the information specified as the execution classification.
The GID value is invalid	The information specified as the group ID is invalid, or no group corresponding to the specified group ID was found. The group ID contains an invalid character or the specified value is outside the valid range.	Check the information specified as the group ID.
The number of elements is invalid	The number of elements in the registration information specified in the CSV file is invalid.	Check the number of elements in the registration information.
An invalid character is specified in the password	The information specified as the password is invalid. The password contains an invalid character or an invalid number of characters.	Check the information specified as the password.
The UID is duplicated in the CSV file	User IDs are duplicated in the CSV file.	Check the information specified as user IDs.
The user name is duplicated in the CSV file	User names are duplicated in the CSV file.	Check the information specified as the user name.
The specified UID is already registered	The ID specified as the user ID is already in use.	Check the information specified as the user ID.
The specified user is already registered	The name specified as the user name is already in use.	Check the information specified as the user name.
The UID value is invalid	The information specified as the user ID is invalid. The user ID contains an invalid character or the specified value is outside the valid range.	Check the information specified as the user ID.
The user name value is invalid	The information specified as the user name is invalid. The	Check the information specified as the user name.

Error message	Cause	Action
	user name contains an invalid character or an invalid number of characters.	
The specified user name is already specified for a group name registered in the CIFS ACL environment	The specified user name duplicates a group name registered in the CIFS (ACL) environment.	Enter a different user name.
An attempt to acquire a locked resource failed	An internal error occurred. • An attempt to acquire a locked resource (timeout) failed.	Re-execute the batch registration. If the error occurs again, download all the File Services Manager log files and contact maintenance personnel. For details on how to download log files, see the *Troubleshooting Guide*.
Registration failed	An internal error occurred. • An attempt to acquire a locked resource (reason other than timeout) failed. • An attempt to convert the group ID of a group to which the user belongs to the group name (file operation error, or group information not found) failed. • An attempt to register a user (using a command) failed.	Re-execute the batch registration. If the error occurs again, download all the File Services Manager log files and contact maintenance personnel. For details on how to download log files, see the *Troubleshooting Guide*.

Table B-3 Error message, cause, and action when an error occurs at batch deletion of users

Error message	Cause	Action
The data classification value is invalid	The information specified as the data classification is invalid.	Check the information specified as the data classification.
The execution classification value is invalid	The information specified as the execution classification is invalid.	Check the information specified as the execution classification.
The number of elements is invalid	The number of elements in the deletion information specified in the CSV file is invalid.	Check the number of elements in the deletion information.
The user name is duplicated in the CSV file	User names are duplicated in the CSV file.	Check the information specified as user names.

Error message	Cause	Action
The specified user does not exist	There is no such user corresponding to the specified user name.	Check the information specified as the user name.
The user name value is invalid	The information specified as the user name is invalid. The user name contains an invalid character or an invalid number of characters.	Check the information specified as the user name.
An attempt to acquire a locked resource failed	An internal error occurred. • An attempt to acquire a locked resource (timeout) failed.	Re-execute the batch deletion. If the error occurs again, download all the File Services Manager log files and contact maintenance personnel. For details on how to download log files, see the *Troubleshooting Guide*.
Deletion failed	An internal error occurred. • An attempt to delete a user (using a command) failed. • An attempt to acquire a locked resource (for a reason other than a timeout) failed.	Re-execute the batch deletion. If the error occurs again, download all the File Services Manager log files and contact maintenance personnel. For details on how to download log files, see the *Troubleshooting Guide*.

Format of a CSV file used for batch registration or batch deletion of group information

This section explains the format of a CSV file required for batch-registering or batch-deleting groups.

Specify the name of the CSV file in no more than 255 characters. You can use alphanumeric characters, hyphens (–), and underscores (_). You can also use periods (.), except at the beginning or end of the character string.

The table below describes the information you specify in the CSV file used for batch-registering or batch-deleting group information.

Table B-4 Information specified in the CSV file used for batch-registering or batch-deleting group information

Item	Specify at registration	Specify at deletion	Description
Execution classification	Yes	Yes	Specify the data-execution classification. Specify `Data`. If you specify a hash mark (#), the line will be a comment.

Item	Specify at registration	Specify at deletion	Description

Data classification	Yes	Yes	Specify the data-processing classification.
			
			`GA01`
			
			    Specify to batch-register the data.
			
			`GD01`
			
			    Specify to batch-delete the data.
			
			You cannot specify both `GA01` and `GD01` in the same file.

Data registration destination	Yes	No	Specify the destination where the group information is to be registered.
			
			`1`
			
			    Register in File Services Manager.
			
			`3`
			
			    Register in File Services Manager as groups that use ACLs to access CIFS shares.

Group name	Yes	Yes	Specify each group name in no more than 16 characters, beginning with an alphanumeric character. From the second character, you can use alphanumeric characters, hyphens (-), and underscores (_). Alphabetic characters are not case sensitive in Windows. Specify a name that is unique regardless of the case. When you are using the ACL function for the group being added, you cannot specify a name that duplicates the name of any user configured to access CIFS shares. You cannot specify a name that duplicates a user name already registered by File Services Manager, the NIS server, or the LDAP server used for user authentication. You cannot specify the following group names which are reserved in the OS on a node: `adm, audio, avahi, avahi-autoipd, backup, bin, bind, cdrom, crontab, daemon, Debian-exim, dialout, dip, disk, enasroot, fax, floppy, ftp, games, gdm, gnats, haldaemon, hddsroot, hsguiroot, irc, kmem, kvm, libuuid, libvirt, list, lp, lpadmin, mail, man, messagebus, mlocate, nasroot, netdev, news, nogroup, ntp, operator, plugdev, postgres, powerdev, proxy, root, sasl, scanner, service, shadow, src, ssh, ssl-cert, staff, stb-admin, sudo, sys, tape, telnetd, tty, users, utmp, uucp, vde2-`

Item	Specify at registration	Specify at deletion	Description
			`net`, `video`, `voice`, `winbindd_priv`, `www-data`
GID	Yes	No	Specify the group ID in the range from 200 to 2147483147. You cannot specify a group ID that is already registered by File Services Manager, the NIS server, or the LDAP server used for user authentication. You cannot specify 65534. If user mapping is used, you cannot specify a group ID within the range set used for user mapping.
Affiliated users	Optional	No	Specify the users belonging to each group by user name or user ID. Specify users registered with File Services Manager. Separate the user names or IDs with commas (`,`) and enclose all the user names and IDs with double quotation marks (`"`).

Legend:

Yes: Specification is necessary

Optional: Specification is optional

No: Specification is unnecessary

The following shows an example of CSV coding used to batch-register group information:

```
#Execution classification,data classification,data registration
destination,group name,group ID,affiliated users
Data,GA01,3,unit04,4000,"user01,1002"
```

The following shows an example of CSV coding used to batch-delete group information:

```
#Execution classification,data classification,,group name
Data,GD01,,unit04
```

Format of result file used for batch registration or batch deletion of group information

You can output, to an execution result file, the results of the CSV file check and the batch registration or deletion, and can confirm that the results are correct.

If you are only checking the CSV file, and the group information is correct, `OK` is output to the group execution classification.

```
#Execution classification,data classification,data registration
destination,group name,group ID,affiliated users
OK,GA01,3,unit04,4000,"user01,1002"
```

If the batch registration or deletion is successful, `#Completed` is output to the
group execution classification.

```
#Execution classification,data classification,data registration
destination,group name,group ID,affiliated users
#Completed,GA01,3,unit04,4000,"user01,1002"
```

If the group information specified in the CSV file contains an error,
`NG(`*contents-of-the-error*`)` is output to the group execution classification.

```
#Execution classification,data classification,data registration
destination,group name,group ID,affiliated users
NG(The specified GID is already registered),GA01,3,unit04,4000,"user01,1002"
```

If the group information specified in the CSV file contains even a single error,
none of the groups are registered or deleted. Correct all the lines to which `NG`
was output, check the CSV file settings again, and re-execute the batch
registration or deletion.

The Table B-5 Error message, cause, and action when an error occurs at
batch registration of groups on page B-11 and Table B-6 Error message,
cause, and action when an error occurs at batch deletion of groups on page
B-13 describe the error message, cause, and action to be taken when an error
occurs at batch registration or batch deletion of groups.

**Table B-5 Error message, cause, and action when an error occurs at batch
registration of groups**

Error message	Cause	Action
`The user who belongs to the group is incorrect`	There is no user corresponding to the user name or user ID specified as an affiliated user.	Check the affiliated user information.
`The data classification value is invalid`	The information specified as the data classification is invalid.	Check the information specified as the data classification.
`The value for the data registration destination is invalid`	The information specified as the data registration destination is invalid.	Check the information specified as the data registration destination.
`The execution classification value is invalid`	The information specified as the execution classification is invalid.	Check the information specified as the execution classification.
`The GID value is invalid`	The information specified as the group ID is invalid. The group ID contains an invalid character or the specified	Check the information specified as the group ID.

Error message	Cause	Action
	value is outside the valid range.	
The number of elements is invalid	The number of elements in the registration information specified in the CSV file is invalid.	Check the number of elements in the registration information.
The GID is duplicated in the CSV file	Group IDs are duplicated in the CSV file.	Check the information specified as group IDs.
The group name is duplicated in the CSV file	Group names are duplicated in the CSV file.	Check the information specified as group names.
The specified GID is already registered	The ID specified as the group ID is already in use.	Check the information specified as the group ID.
The specified group is already registered	The name specified as the group name is already in use.	Check the information specified as the group name.
The group name value is invalid	The information specified as the group name is invalid. The group name contains an invalid character or an invalid number of characters.	Check the information specified as the group name.
The specified group name is already specified for a user name registered in the CIFS environment	The specified group name duplicates a user name registered in the CIFS environment.	Enter a different group name.
An attempt to acquire a locked resource failed	An internal error occurred. • An attempt to acquire a locked resource (timeout) failed.	Re-execute the batch registration. If the error occurs again, download all the File Services Manager log files and contact maintenance personnel. For details on how to download log files, see the *Troubleshooting Guide*.
Registration failed	An internal error occurred. • An attempt to acquire a locked resource (for a reason other than a timeout) failed. • An attempt to convert the user ID of an affiliated user to the user name (file operation error, or user information not found) failed. • An attempt to register a group (using a command) failed.	Re-execute the batch registration. If the error occurs again, download all the File Services Manager log files and contact maintenance personnel. For details on how to download log files, see the *Troubleshooting Guide*.

Table B-6 Error message, cause, and action when an error occurs at batch deletion of groups

Error message	Cause	Action
The data classification value is invalid	The information specified as the data classification is invalid.	Check the information specified as the data classification.
The execution classification value is invalid	The information specified as the execution classification is invalid.	Check the information specified as the execution classification.
The number of elements is invalid	The number of elements in the deletion information specified in the CSV file is invalid.	Check the number of elements in the deletion information.
The group name is duplicated in the CSV file	Group names are duplicated in the CSV file.	Check the group name settings.
The specified group does not exist	There is no group corresponding to the name specified as the group name.	Check the information specified as the group name.
The group name value is invalid	The information specified as the group name is invalid. The group name contains an invalid character or an invalid number of characters.	Check the information specified as the group name.
The specified group is set up as a user's primary group	The specified group name duplicates the name of the primary group to which the user belongs.	Delete any users whose primary group is the group being deleted, and then try again.
An attempt to acquire a locked resource failed	An internal error occurred. • An attempt to acquire a locked resource (timeout) failed.	Re-execute the batch deletion. If the error occurs again, download all the File Services Manager log files and contact maintenance personnel. For details on how to download log files, see the *Troubleshooting Guide*.
Deletion failed	An internal error occurred. • An attempt to delete a group (using a command) failed. • An attempt to acquire a locked resource (for a reason other than a timeout) failed.	Re-execute the batch deletion. If the error occurs again, download all the File Services Manager log files and contact maintenance personnel. For details on how to download log files, see the *Troubleshooting Guide*.

Batch-Registering or Batch-Deleting Local Users or Groups

Hitachi Vantara