Hitachi Data Ingestor

6.4.6-02

Installation and Configuration Guide

This guide provides information you need about setting up an Hitachi Data Ingestor (HDI) system. This guide provides system configuration examples and describes required settings for external server components for HDI. This guide also describes how to link HDI with Hitachi Content Platform (HCP), and how to install and configure File Services Manager.

MK-90HDICOM002-18
March 2019

Contents

Preface

This manual contains information that you need to know before operating the Hitachi Data Ingestor (HDI) systems. This manual also explains how to set up the systems.

Intended audience

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

In addition, the user must have:

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

Product version

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

Release notes

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 (This manual)	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

Manual name	Description
	operation, as well as the environment settings for an external server.
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, MK-90HDI034	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 Command Suite products

- *Hitachi Command Suite User Guide*
- *Hitachi Command Suite CLI Reference Guide*
- *Hitachi Command Suite Messages*
- *Hitachi Command Suite Installation and Configuration Guide*
- *Hitachi Command Suite Replication Manager Configuration Guide*
- *Hitachi Command Suite Tuning Manager Installation Guide*

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 Storage Navigator Modular 2 Graphical User Interface (GUI) User's Guide*

Hitachi AMS2000 series

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

Hitachi Content Platform

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

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

Abbreviation conventions

This manual uses the following abbreviations for product names:

Abbreviation	Full name or meaning
Active Directory	Active Directory(R)
ADAM	Active Directory(R) Application Mode 1.0
Compute Systems Manager	Hitachi Compute Systems Manager
Device Manager	Hitachi Device Manager Software
Dynamic Provisioning	Hitachi Dynamic Provisioning
Dynamic Tiering	Hitachi Dynamic Tiering
File Services Manager	A generic name for the following: • Configuration Manager • Hitachi File Services Manager
Firefox	Mozilla Firefox(R)
Global Link Manager	Hitachi Global Link Manager Software
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
HUS VM	Hitachi Unified Storage VM
Internet Explorer	Windows(R) Internet Explorer(R)
OpenLDAP	OpenLDAP 2.*x*
Replication Manager	Hitachi Replication Manager Software
ShadowImage	A generic name for the following: • ShadowImage • ShadowImage in-system replication

Abbreviation	Full name or meaning
Solaris 10	Solaris 10 Operating System for SPARC Platforms
Sun Java System Directory Server	Sun Java(TM) System Directory Server 5.2
Tiered Storage Manager	Hitachi Tiered Storage Manager Software
TrueCopy	A generic name for the following: • TrueCopy • TrueCopy Asynchronous • TrueCopy Extended Distance • TrueCopy remote replication
Tuning Manager	Hitachi Tuning Manager Software
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 Server 2008	A generic name for the following: • Microsoft(R) Windows Server(R) 2008 Datacenter • Microsoft(R) Windows Server(R) 2008 Enterprise • Microsoft(R) Windows Server(R) 2008 Standard
Windows Server 2008 R2	A generic name for the following: • Microsoft(R) Windows Server(R) 2008 R2 Datacenter

Abbreviation	Full name or meaning
	• Microsoft(R) Windows Server(R) 2008 R2 Enterprise • Microsoft(R) Windows Server(R) 2008 R2 Standard
Windows Server 2012	A generic name for the following: • Microsoft(R) Windows Server(R) 2012 Datacenter • Microsoft(R) Windows Server(R) 2012 Standard
Windows Server 2012 R2	A generic name for the following: • Microsoft(R) Windows Server(R) 2012 R2 Datacenter • Microsoft(R) Windows Server(R) 2012 R2 Standard
Windows Server 2016	A generic name for the following: • Microsoft(R) Windows Server(R) 2016 Datacenter • Microsoft(R) Windows Server(R) 2016 Standard

Unless otherwise noted, this document assumes that you are using the user interface of Windows 7, Windows Server 2008, or an earlier Windows version. If you are using Windows Server 2012 or a later Windows version, the actual user interface might differ from that described in this manual. If necessary, see the documentation for the OS that you are using.

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>`

Convention	Description
	Note: Italic font is also used to indicate variables.

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

Icon	Label	Description
	Note	Calls attention to important and/or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions and/or consequences (e.g., disruptive operations).

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!

1

Overview of Hitachi Data Ingestor

This chapter describes the features of, and gives a functional overview of, Hitachi Data Ingestor (HDI).

- ☐ What is Hitachi Data Ingestor?
- ☐ Linkage with Hitachi Content Platform

What is Hitachi Data Ingestor?

An Hitachi Data Ingestor (HDI) system provides services that enable clients on different platforms to share data in storage systems. An HDI system consists of file servers called *nodes* and storage systems in which data is compacted and stored. The HDI system provides a file system service to clients by way of the network ports on the nodes.

The HDI model determines whether HDI nodes can be set up in a redundant configuration. 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*.

From a management console, the system administrator of an HDI system can set up the system, monitor operating statuses, monitor for errors, change settings, back up data, and restore data.

The following figure shows an overview of an HDI system.

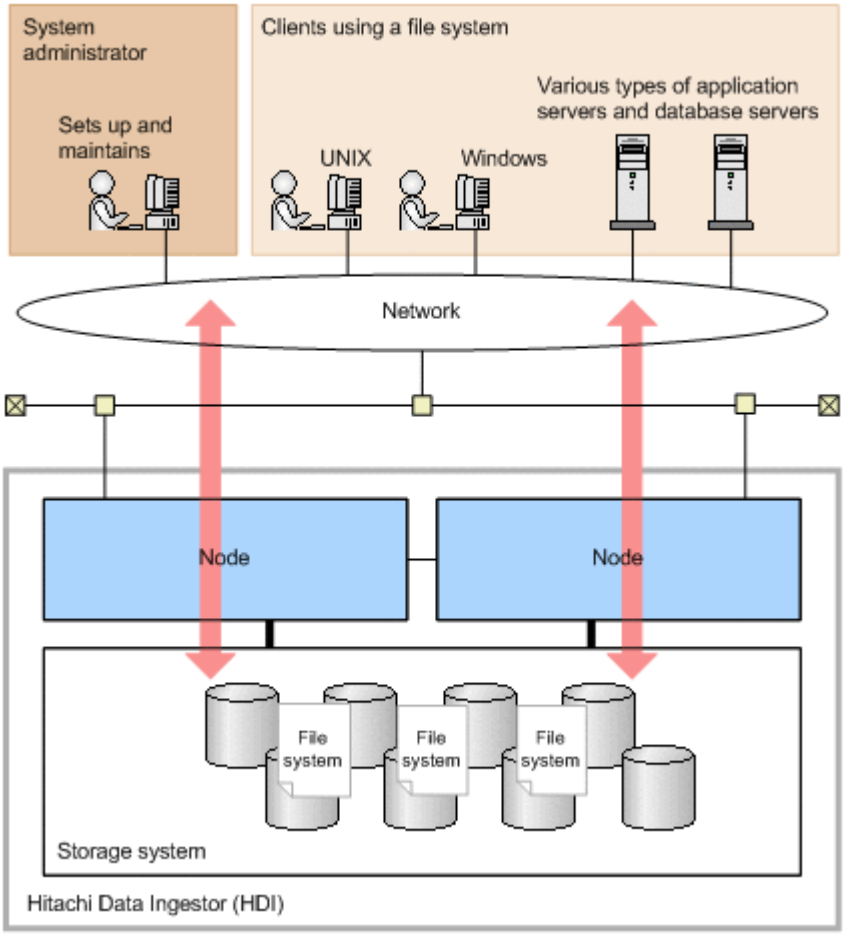


Figure 1-1 Overview of an HDI system

The main features of an HDI system are as follows.

Provides an open data-sharing environment that fully utilizes legacy systems

While fully utilizing an enterprise's already-existing LAN environment, an HDI system can achieve integrated management of data on a storage system. Data on a storage system can be shared across heterogeneous platforms.

Efficient and flexible capacity management

In an HDI system linked to Dynamic Provisioning, which provides the capacity virtualization functionality for storage systems, a virtual volume whose capacity is larger than a physical volume on a storage system can be allocated to a file system. Before a capacity shortage occurs, a disk can be added without stopping the system, thereby improving the usability of the storage system and reducing installation costs. It is also possible to efficiently use free space on a volume allocated to a file system by checking the available capacity for each shared directory according to operational preferences.

Ensures high availability in a cluster configuration

In an HDI system, two nodes are configured in a cluster to ensure the reliable delivery of services, such as NFS and CIFS services. If an error occurs in one node, services can be relocated to the other node in the cluster, ensuring service stability.

By working together with the failover functionality, the HDI system enables online maintenance of hardware, software, and the services provided by the HDI system.

Ensures safety

In an HDI system, *Anti-Virus Enabler* can perform real-time scanning to protect valuable data on a file system from viruses.

Data persistence suitable for compliance

Files on file systems that support WORM (Write Once Read Many) functionality can be changed to WORM data, thereby preventing falsification and deletion of data and providing long-term data persistence suitable for regulatory compliance.

Secure data storage by using encryption technology

Encryption on user LUs used for file systems reduces the risk of information leaks (*Local data encryption*). HDI systems use secret key cryptography (an XTS-AES cipher with a 256-bit key length). Encryption requires a corresponding license.

Backup operations

By replicating data, an HDI system can protect valuable data shared on a file system from loss due to error or malfunctions.

Linkage with Hitachi Command Suite products in a cluster configuration

An HDI system can link with the following Hitachi Command Suite products:

- Device Manager

  By linking with Device Manager, you can centrally manage the correspondence between volumes in storage systems and file

systems. You can also use single sign-on for the Hitachi Command Suite products.

- Tuning Manager

  You can view the status of file system usage and performance information for the OS on a node.

Data importing from other file servers

You can import file share data used in file servers other than HDI systems to an HDI system. The data in multiple file servers can be imported simultaneously. This allows you to integrate file server operations into an HDI system.

HDI systems can import data while the target file system is in use. Access from clients can be re-opened even if all files and directories have not yet been imported. This reduces the time that file system operation must be stopped.

Linkage with Hitachi Content Platform

Hitachi Content Platform (HCP) systems archive large amounts of data created on various systems and store them long term. HCP systems allow quick access to archived data, in addition to high capacity scalability.

An HDI system that links with an HCP system can provide high-performance file system services and, at the same time, efficiently manage the large amounts of data that accumulates daily.

For example, by making files WORM (Write Once, Read Many) files to guard against tampering or deletion, and by regularly migrating infrequently accessed files to an HCP system, you can effectively manage archived data to ensure that file systems meet compliance requirements. If you make data of a past version archived in an HCP system available to HDI clients, those clients can restore the data when necessary.

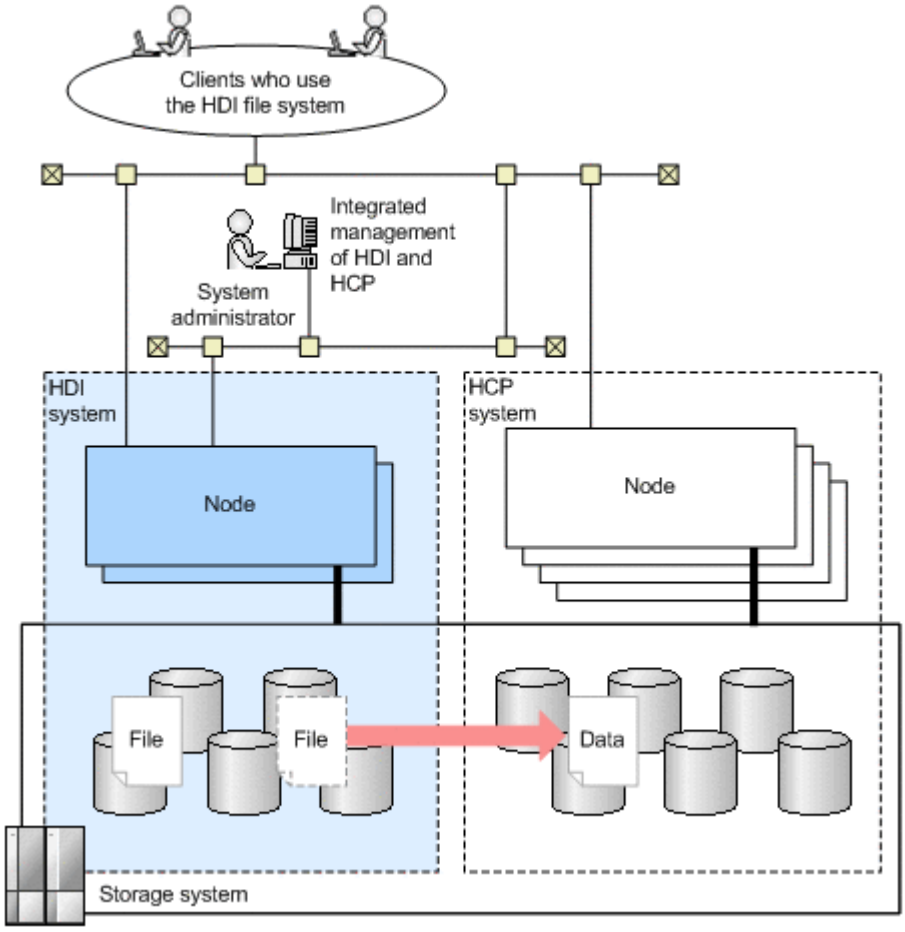


Figure 1-2 Linkage between an HDI system and an HCP system that share a storage system

In addition, migrating the file system data on HDI systems running in distributed locations to a remote HCP system by way of a network enables you to centrally control data in a large-scale system. File systems in each location are managed by HDI system administrators. The data received from each location is centrally managed by the HCP system administrator. The data centrally managed by an HCP system can be shared among HDI systems running in distributed locations.

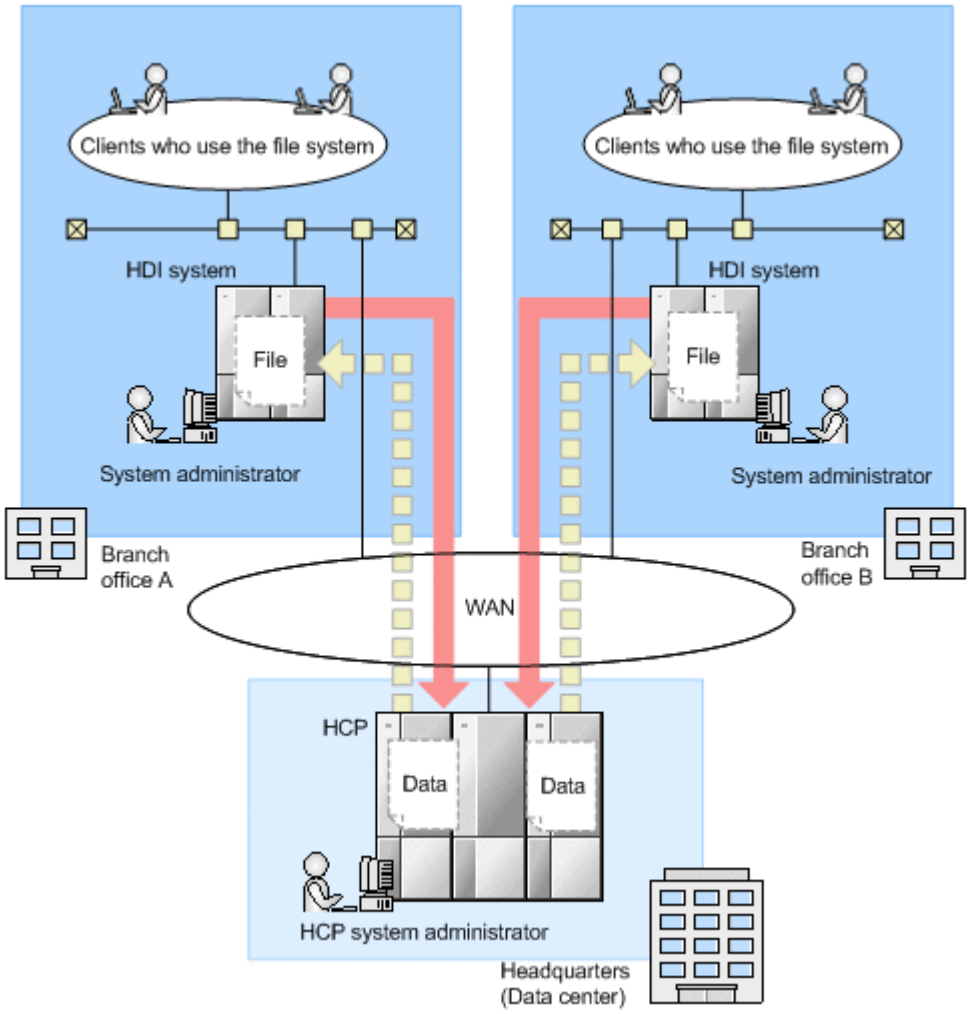


Figure 1-3 Linkage between HDI systems and a remote HCP system via a network

2

System Configuration

This chapter describes HDI system configurations. This chapter also describes system configurations in which HDI systems link with an HCP system.

- Hardware configurations
- Network configurations
- System configurations when linking with an HCP system

Hardware configurations

In addition to storage systems and nodes, an HDI system includes external servers and devices, on the network, that are required to provide file system services. This section describes HDI hardware configurations.

Configurations of storage systems and nodes

An HDI node that uses a storage system in either a cluster configuration or single-node configuration is a device connected to a storage system by way of Fibre Channel, and can include various ports (such as data ports, management ports, and BMC ports), a DVD drive, and an internal hard disk drive. For information about node hardware, see the applicable HDI manual. For the names and locations of ports, see Appendix C, Layout of Node Ports on page C-1.

External servers and devices required in an HDI system

In addition to a storage system and nodes, an HDI system also requires the following external servers and devices:

Management console

A computer required in order to use the GUI or commands. The following programs can also be used:

Storage Navigator

A program required for operating Universal Volume Manager when a VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system is used for an HDI system in a cluster configuration. This program can be used to check which drive holds the actual device files.

For details about management console environment setup, see Environment settings for a management console on page 3-9.

Management server in a cluster configuration

A computer needed to manage the HDI in a cluster configuration. Hitachi File Services Manager is installed on the management server. One management server can manage a maximum of 16 clusters.

A management server can also be used as a management console.

The following programs are required for a management server:

Hitachi File Services Manager

A program that is required for system administrators to operate or manage an HDI system by using a GUI. Hitachi File Services Manager links with Configuration Manager on the node and provides GUI functionality for managing setup and operations for an HDI system. Hitachi File Services Manager and Configuration Manager are generically called *File Services Manager*.

When multiple clusters are managed from one management server, the program installed on the management server and the programs

installed on the nodes might differ. If the program installed on a node is earlier than Hitachi File Services Manager installed on the management server, some information might not be displayed in the GUI, or some GUI items might be disabled. In such a case, see the documentation for the relevant program version installed on the node, and take corrective actions.

If multiple servers manage the same cluster, the information on the servers might be inconsistent or cluster settings might be specified unintentionally. For this reason, do not use multiple servers to manage the same cluster.

Device Manager

A program used to manage the disk resources and hardware configuration of storage systems in an integrated manner. By linking with Device Manager, you can centrally manage the correspondence between volumes in storage systems and file systems.

In a large-scale environment with a lot of file systems and file shares, if HDI is linked with Device Manager, ask the Device Manager administrator in advance to expand the maximum length of HTTP request entities permitted by the Device Manager server.

Device Manager can be installed and operated on a computer other than one on which Hitachi File Services Manager is installed. Before using Hitachi File Services Manager via the GUI for the Device Manager installed on a computer other than one on which Hitachi File Services Manager is installed, change the settings for Hitachi File Services Manager by following the procedure in Connecting to Device Manager to manage user accounts on page 7-83.

Hitachi Command Suite Common Component

A component that provides functionality common to Hitachi File Services Manager and Hitachi Command Suite products. Hitachi Command Suite Common Component is installed as part of either Hitachi File Services Manager or a Hitachi Command Suite product. This component provides functionalities such as GUI login, integrated log output on the management server, and Web services.

Hitachi Storage Navigator Modular 2

A program required to create and delete LUs taking into consideration the disk drive layout and the parity groups when the storage system being used is in the Hitachi AMS2000 series or the HUS100 series.

You can use the GUI of Hitachi Storage Navigator Modular 2 installed on the management server from Hitachi File Services Manager. To display the Hitachi Storage Navigator Modular 2 GUI from Hitachi File Services Manager when the Password Protection functionality or Account Authentication functionality has been enabled on the storage system, an account named `nasmgr` must be created beforehand in the storage system. For the `nasmgr` account password, use the authentication password for the management server on the node. (For the Password Protection functionality, use the first 12 characters of the authentication password.)

For details about management server environment setup, see Environment settings for a management server on page 3-5.

NTP server

A server that applies the correct time to each node. Make sure that an NTP server is set up. We recommend that you use two NTP servers to prepare against NTP server failures. For details about the environment settings for an NTP server, see Environment settings for the NTP server on page 3-33.

SNMP manager

A manager that is required to view system information or receive error notification by using SNMP. For details about the environment settings for an SNMP manager, see Environment settings for the SNMP manager on page 3-30.

DNS server

A server required when searching the DNS for host names.

NIS server

A server required when searching for user and host information via the NIS. For details about the NIS server environment setup, see Environment settings for the NIS server on page 3-17.

WINS server

A server required when a CIFS client that uses an HDI system resolves a host name by using WINS.

KDC server

A server required for the following purposes:

- User authentication

  Required if Kerberos authentication for the NFS service is used to authenticate users.
- System administrator account authentication

  Required if Kerberos authentication is used to authenticate system administrator accounts.

For details about the KDC server environment setup, see Environment settings for the KDC server on page 3-28.

RADIUS server

A server that is necessary for using RADIUS authentication to authenticate system administrator accounts. For details about the environment settings for a RADIUS server, see Environment settings for the RADIUS server on page 3-29.

Domain controller

A server required when an HDI system authenticates users by using Active Directory authentication or NT domain authentication. If an Active Directory domain controller is used, the domain controller can also be used as a KDC server when Kerberos authentication is used for the NFS service.

LDAP server

A server required for the following purposes:

- User authentication

  Required if user information is managed using an LDAP server.

- User mapping

  For CIFS clients, required to store the user ID or group ID information that has been assigned automatically or manually by the LDAP administrator into a database on the LDAP server.

  If you switch from one LDAP server to the other, you must change the File Services Manager settings.

- System administrator account authentication

  Required if system administrator accounts are authenticated using an LDAP server.

For details about the LDAP server environment setup, see Environment settings for the LDAP server on page 3-17.

Scan server

A server required to perform real-time virus scanning. For details about the environment settings for a scan server, see Environment settings for the scan server on page 3-34.

FTP server

A server that is necessary for batch-downloading dump files.

Proxy server

A server that is necessary to relay HTTP or HTTPS communication between an HDI system and an HCP system.

SMTP server

A server required for receiving email error notifications. For details about SMTP server environment settings, see SMTP server environment settings on page 3-41.

DHCP server

A server required for using DHCP to set node network information when HDI is used and managed in a single-node configuration. For details about environment settings on the DHCP server, see DHCP server environment settings on page 3-41.

Relaying devices used by an HCP system to be linked (such as a load balancer)

A relaying device (such as a load balancer) is required for HTTP or HTTPS communications between an HDI system and an HCP system. If an HCP system to be linked uses relaying devices, the host information that has been made external and that is used to connect to the HCP system should be set for the HDI system.

In addition, if end users will use the HDI GUI, a computer that satisfies the requirements for the management console is required. For details about the

requirements for the management console, see Environment settings for a management console on page 3-9.

External servers and devices required in an HDI system when using the NDMP functionality

This section explains the external server or devices that are required when using the NDMP functionality.

For notes on using backup management software and any other software that is compatible with Backup Restore, see the supplementary Backup Restore documentation that is provided with HDI.

Backup server

A backup server is a server that has backup management software installed. A backup server can also function as a media server.

For a backup server, backup management software is required.

Media server

A media server manages tape devices.

For a media server, backup management software is required.

Tape device

You can back up file system data and restore the data from tape devices.

For details on tape devices that can be connected to a media server, see the documentation for the backup management software.

For details on specifications for tape drives, and vendors and model names of tape devices that can be connected to nodes via a SAN, contact our sales representatives.

The following figure shows an example hardware configuration when using the NDMP functionality provided by Backup Restore in a cluster configuration.

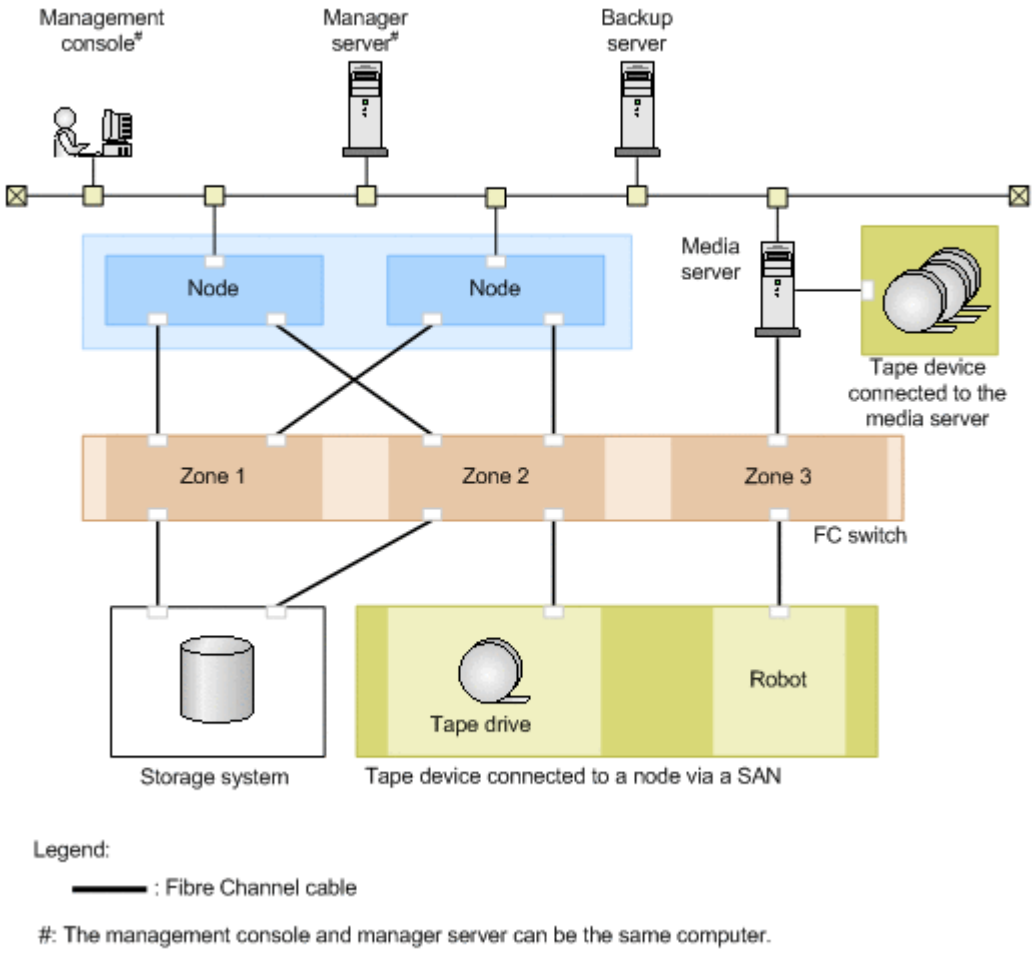


Figure 2-1 An example hardware configuration when using the NDMP functionality in a cluster configuration

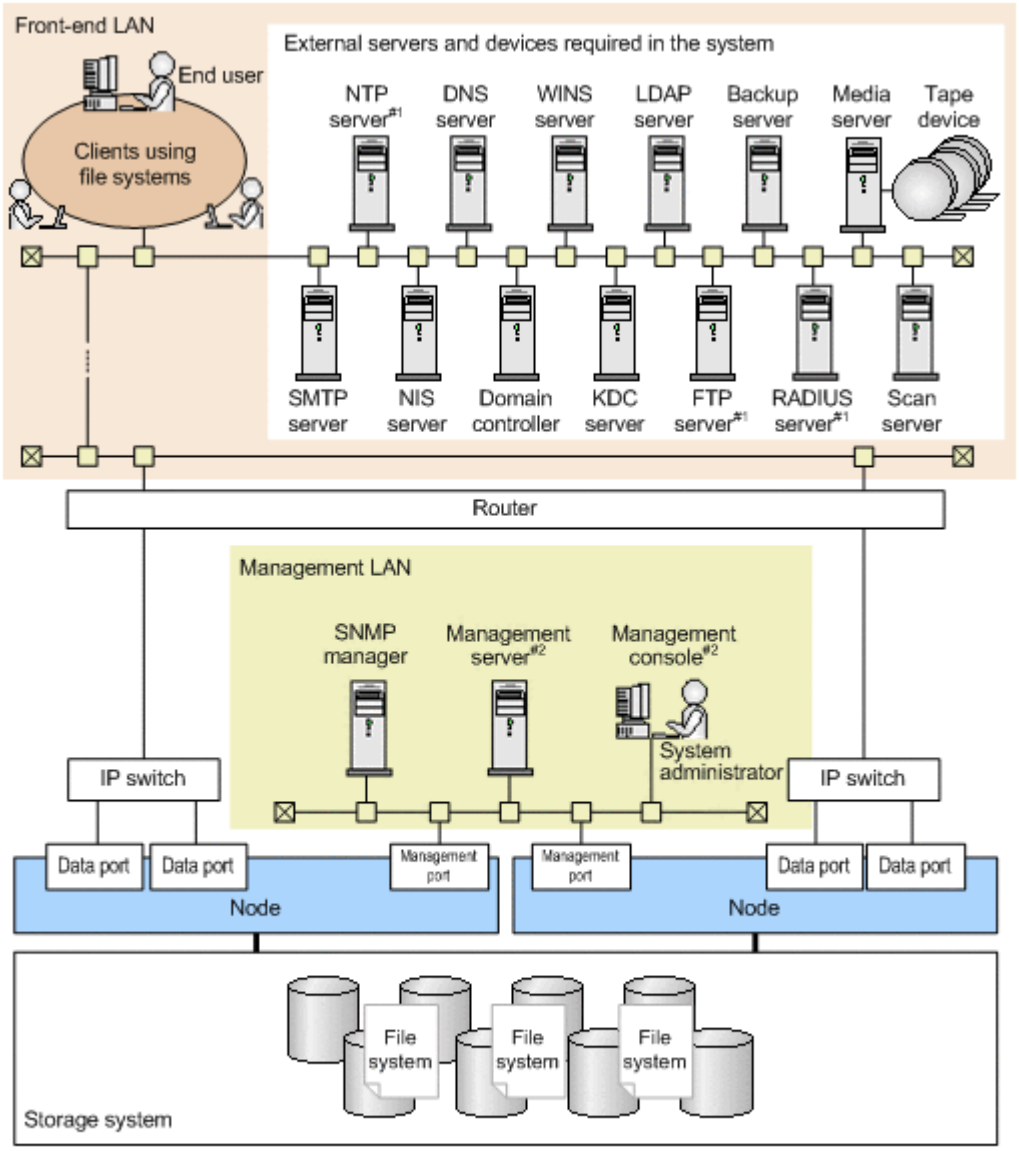
To use a tape device connected to a node via a SAN, make sure the configuration is constructed so that the media server manages the robot, and the NDMP server manages the tape drives.

Network configurations

HDI system networks consist of a management LAN, which is used by the system administrator to operate and manage an HDI system, and a front-end LAN, which is used by clients to access resources stored in a storage system or on an internal hard disk drive.

The following figure shows an example of a network configuration for an HDI system in a cluster configuration. For single-node network configurations, see the *Single Node Getting Started Guide*.

There is also a maintenance LAN, which is used by maintenance personnel for maintenance operations and troubleshooting.



#1: Specify the settings so that the server can communicate with the management server when necessary.
#2: By installing the prerequisite programs for the management console on the management server, you can also configure the system so that all tasks can be performed from one computer.

Figure 2-2 Example of an HDI system network configuration

A node's management port connects to the management LAN and its data port connects to the front-end LAN.

Fixed IP addresses and virtual IP addresses can be set for management ports and data ports for nodes. The following table describes the use of IP addresses set for each port, as well as points to note.

Table 2-1 Use of IP addresses set for each port and points to note

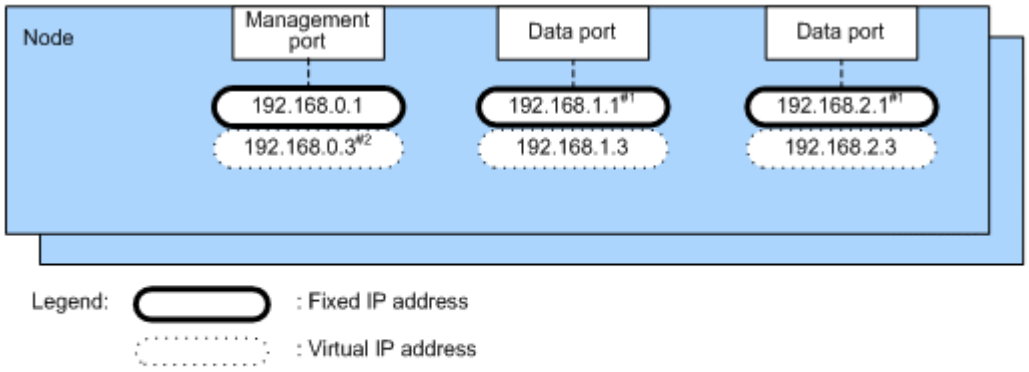
Classification			Use	Points to Note
Node	Management port	Fixed IP address	• Used by a system administrator to manage HDI system operations, by connecting to a node from the management console or management server • Used for connecting a node to an external server in the management LAN	Setting in IPv4 is required.
		Virtual IP address	Used by end users to access file systems on a node from clients in the management LAN	A virtual IP address is optional if a client that accesses file systems does not exist in the management LAN.
	Data port	Fixed IP address	• Used for connecting the HDI system to an external server in the front-end LAN • Used by a system administrator to manage HDI system operations, by connecting to a node from the management console or management server in the front-end LAN	• A fixed IP address is optional if the external server, management console, and management server all exist in the management LAN. • A fixed IP address is required if any of the external server, management console, and management server exists in the front-end LAN.
		Virtual IP address	Used by end users to access file systems on a node from clients in the front-end LAN	-

The table below shows the IP addresses to be set for each port.

Table 2-2 IP addresses to be set for each port

Classification			Specify or not
Node	Management port	Fixed IP address	Specify.
		Virtual IP address	Specify if a client exists in the management LAN.
	Data port	Fixed IP address	Specify if an external server, management console, or management server is configured in the front-end LAN.

Classification			Specify or not
		Virtual IP address	Specify.



#1: Specify if an external server, management console, or management server is configured in the front-end LAN.

#2: Specify if a client exists in the management LAN.

Figure 2-3 Example of setting IP addresses

The types and names of data ports that can be used differ according to the configuration of the optional cards installed in the node's expansion slots. For the relationship between the optional card configuration and usable data ports, see Appendix C, Layout of Node Ports on page C-1.

To access file systems, clients use a virtual IP address set for a data port. Even if a failover occurs due to an error and services continue on the other node in the cluster, clients can continue to access the file systems because the virtual IP address is passed on to an interface that has the same name.

By setting a virtual IP address for the management port, file systems can also be accessed from the management console set for the management LAN. In addition, the management port can be used as a data port.

By planning the network configuration, and the mounting of file systems, a system administrator can distribute file access across both nodes and balance the loads between the nodes.

HDI systems support IPv4 and IPv6. The systems also can be used in environments where IPv4 and IPv6 networks coexist.

In addition to the above notes, other notes on system configuration and requirements for linkage with an HCP system apply. For these notes and requirements, see System configurations when linking with an HCP system on page 2-26.

Before configuring a network

- The SNMP manager must all be connected to the management LAN.
- External servers and devices required by an HDI system (excluding the SNMP manager) can be connected to the management LAN and front-end LAN. However, a fixed IP address must be set for a

management port or data port to be connected to a LAN that connects to these external servers and devices.

- The computers to be used by end users who use the File Services Manager GUI must be placed on the front-end LAN.
- The fixed IP addresses and virtual IP addresses used for the node data ports, the trunked virtual ports, and the virtual network interfaces for VLANs must all be in separate network segments.
- The fixed IP addresses and virtual IP addresses used for ports that correspond to each other between nodes in a cluster must be in the same network segment.
- You must set the routing information from File Services Manager to ensure that nodes can communicate with external servers or client computers.

  Additionally, to update the software of a node from File Services Manager, you must specify the settings so that File Services Manager can communicate via `mng0`.
- You must synchronize the time of the nodes, external servers, and client computers.
- In a cluster configuration, a BMC port on a node can be connected in the ways (configurations) shown below.

  – Connecting a BMC port to the IP switch that connects to the management port

  The network address of the BMC port must be the same as the network address of `mng0`.

  – Connecting a BMC port to the port that connects to the other node (`pm1`)

  The network address of the BMC port must be different from the network address of `mng0`.

  When changing the connection configuration, you must use the `bmcctl` command to change the BMC port settings.

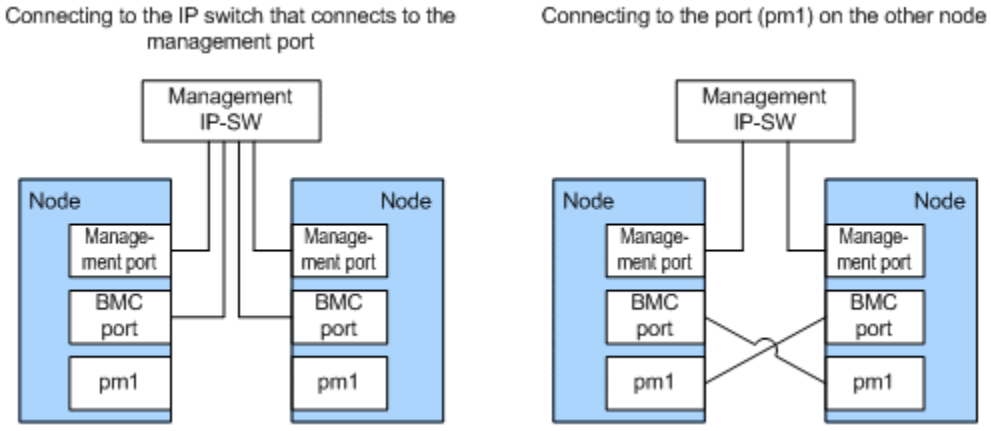


Figure 2-4 Connection configurations of a BMC port

When a BMC port is connected to the IP switch that connects to the management port, the node OS can be started from Hitachi File Services Manager.

- Linkage with Compute Systems Manager is not supported. Do not include the IP address of a BMC port as a search target for Compute Systems Manager.
- One or more virtual IP addresses must be set to activate the resource group. In addition, for nodes clustered in an active-standby configuration, one or more virtual IP addresses must also be set for the standby node to activate the resources on both nodes.
- To use the window of Hitachi File Service Manager shown below, you must specify the virtual IP address for the port of the HDI system that is connected from Hitachi File Services Manager. Specify the virtual IP address for the node to be set in the window below.

  - **Migration Task Wizard**

  - **Migration Tasks** dialog
- You must specify the virtual IP address for the port of the HDI system that is used by the following functions:

  - Automatic failover when a link goes down (Automatically fails over only when a link goes down for a port for which the virtual IP address is specified)

  - Linkage to MMC (Microsoft Management Console)

  - GUI for end users

Before managing the system from the management server and management console on the front-end LAN

You can manage the system from the management server and management console on the front-end LAN. When managing the system from the management server and management console on the front-end LAN, note the following:

- Use fixed IP addresses to connect the management server and nodes. Make sure that a fixed IP address is set for the data port used for management.
- Even in a network configuration in which the system is managed from the management server and management console located on the front-end LAN, some operations must be performed from the management server and management console located on the management LAN, such as when configuring an HDI cluster or recovering the network from an error. Move the computers used as the management server and management console to the pertinent network, or provide both the management LAN and front-end LAN with management server and console computers. Note that when changing the network to which the management server and console are connected, you must modify the IP addresses assigned to the management server and management console.
- Depending on the file system access status, the File Services Manager GUI processing might take some time.
- When using Hitachi Storage Navigator Modular 2 to create an LU, connect the management port of the storage system controller (CTL) to the front-end LAN used for management.

- The network address translation (NAT) functionality cannot be used for communication between the data port used for management and the management console or management server.
- When changing settings for the data port used for management, perform the operation from the management server and management console in the management LAN. If you change a data port setting from a management server and management console in the front-end LAN, the GUI might become unable to respond. If this problem occurs, click the **X** button on the title bar to close the window.
- If you specify an incorrect setting when trunking the data port used for management, you might be unable to use the File Services Manager GUI from the management server and management console in the front-end LAN. The system administrator must retry network setup from the management server and management console in the management LAN.
- For Hitachi AMS2000 series storage or HUS100 series, you cannot create a VLAN interface for the data port that will be used for management.
- When updating the software, perform the operation from the management console located on the management LAN.

  Note that the management server must be included in the management LAN and must be connected to the management port of the node.

Note that if the following setting tasks have yet to be completed at the time of system implementation, you must perform these tasks from the management server and management console located on the management LAN:

- Defining the HDI cluster configuration
- Setting the data ports

Configure the network so that the management server and management console can be used from the management LAN. After completing the necessary settings, change the network configuration so that the management server and management console can be used from the front-end LAN, and then start operation.

In addition, the following error recovery actions must be performed from the management server and management console located on the management LAN:

- Recovering the front-end LAN from a network error
- Recovering a data port from a link error
- Restoring saved system LU information

You also need to perform operations from the management server and management console located on the management LAN when you are instructed to operate the clusters by the maintenance personnel for error recovery. Change the network configuration so that the management server and management console that have been used from the front-end LAN can be used from the management LAN. After the necessary recovery action is completed, restore the network configuration so that

the management server and management console can be used from the front-end LAN, and then resume operation.

Network configuration required to use CIFS shares

If CIFS shares are to be used, both the nodes within a cluster must belong to the same workgroup, NT domain, or Active Directory domain.

CIFS clients specify the virtual IP address of a node or use the name resolution service to access CIFS shares.

CIFS clients can also use a browser to access CIFS shares. Notes for using a browser are as follows:

- When configuring a network, make sure that names are resolvable using a service such as DNS, WINS, or lmhosts.
- The system must be configured in the **CIFS Service Management** page (**Setting Type**: `Security`) so that it accepts access requests from CIFS clients using NetBIOS over the TCP/IP protocol. If not, the following problems occur:
  - The CIFS service of the HDI system does not work as a local master browser.
  - The CIFS service of the HDI system is not displayed in the list of computers on the CIFS client.
  - Names cannot be resolved by using a broadcast from a CIFS client in the same subnet.
- Whenever you start or stop a domain controller placed on the same subnet, the system attempts to select a local master browser (for about 12 minutes). If no domain controller exists on the same subnet and the system attempts to restart a local master browser, the process of selecting a local master browser or acquiring computer information will take a long time. The CIFS client cannot access CIFS shares until the local master browser starts.
- A list of computers displayed on the CIFS client is based on information that is provided by a local master browser, and it does not correspond to the operational status of each computer. Therefore, the CIFS client cannot access a stopped computer, even though the computer exists in the list of computers.

The following describes the network configuration when using the browsing functionality.

When the CIFS client and the node are connected to the same subnet

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

If a domain controller does not exist in the same subnet, the CIFS service of the HDI system might work as a local master browser. In such a case, the CIFS service that works as a local master browser temporarily stops when a

failover occurs. Because of this temporary stop, the CIFS client will take longer to acquire a list of computers. When the CIFS client access CIFS shares, the CIFS service must have worked as a local master browser.

The following figure illustrates a network where the CIFS client and the node belong to a single work group.

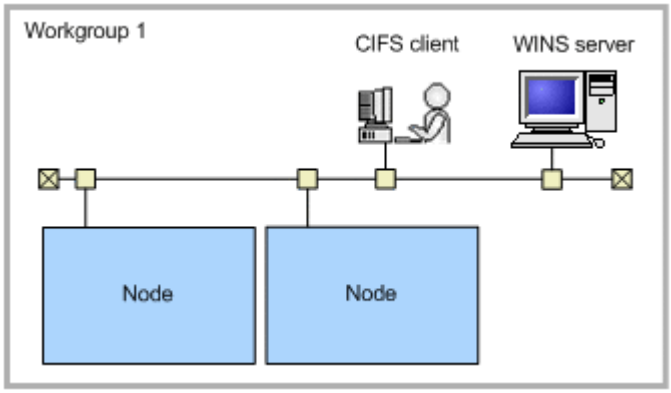


Figure 2-5 Network where the CIFS client and the node belong to a single work group

The following figure illustrates a network where the CIFS client and the node belong to multiple work groups.

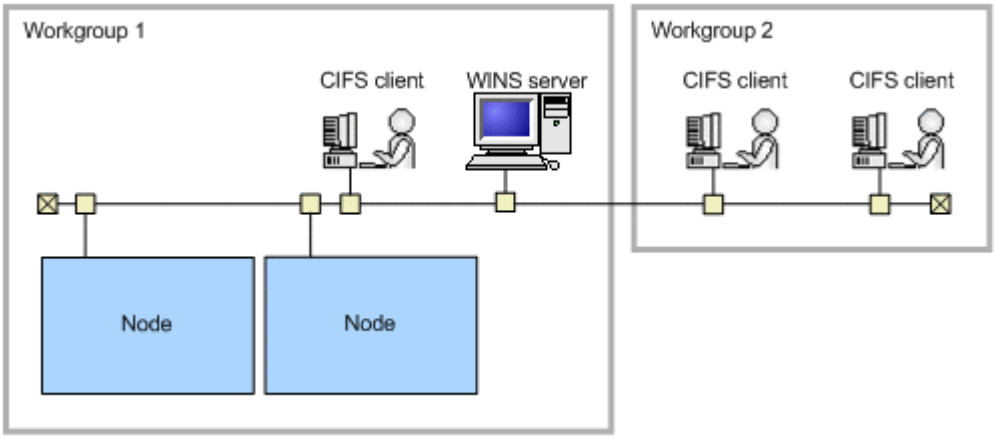


Figure 2-6 Network where the CIFS client and the node belong to multiple work groups

The following figure illustrates a network where the CIFS client and the node belong to a single NT domain.

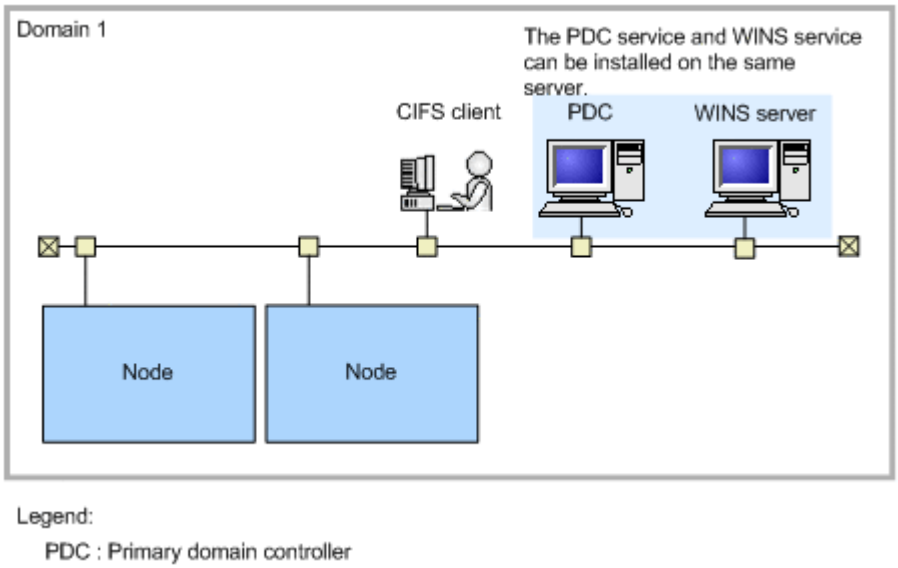


Figure 2-7 Network where the CIFS client and the node belong to a single NT domain

When the CIFS client and the node are connected to different subnets

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

- An NT domain configuration or Active Directory domain configuration is required.
- A domain controller is required for the subnet to which the node is connected.
- If a WINS server is used as a name server to CIFS clients, we recommend that all the CIFS clients in the network be set as WINS clients.
- If a WINS server is not used, the `lmhosts` file must be modified as follows:

  In an NT domain configuration

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

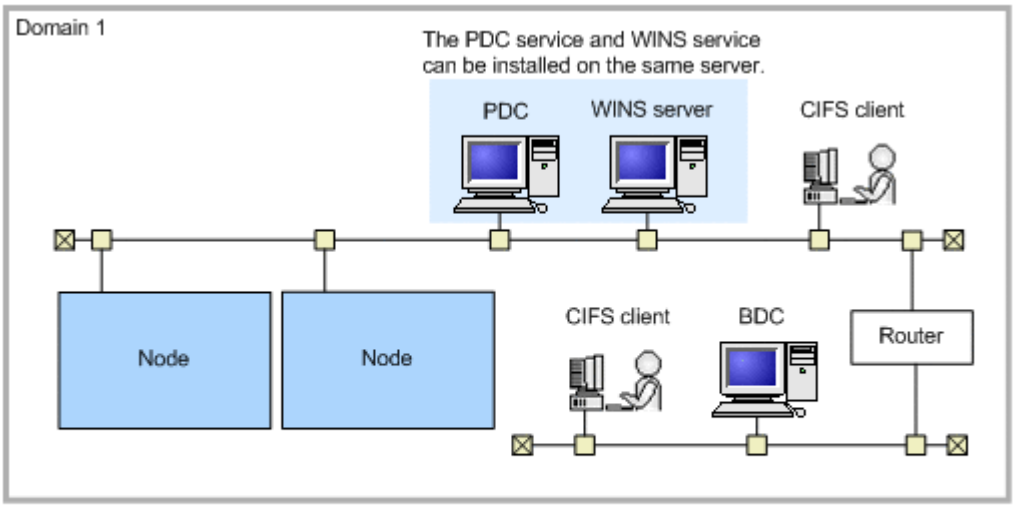
  `IP-address-of-the-primary-domain-controller domain-name``#1B`

  In an Active Directory domain configuration

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

  `IP-address-of-the-domain-controller-that-exists-in-the-same-subnet-as-the-node``#1B`

In an NT domain configuration, the following figure illustrates a network where the node and the primary domain controller exist in the same subnet.



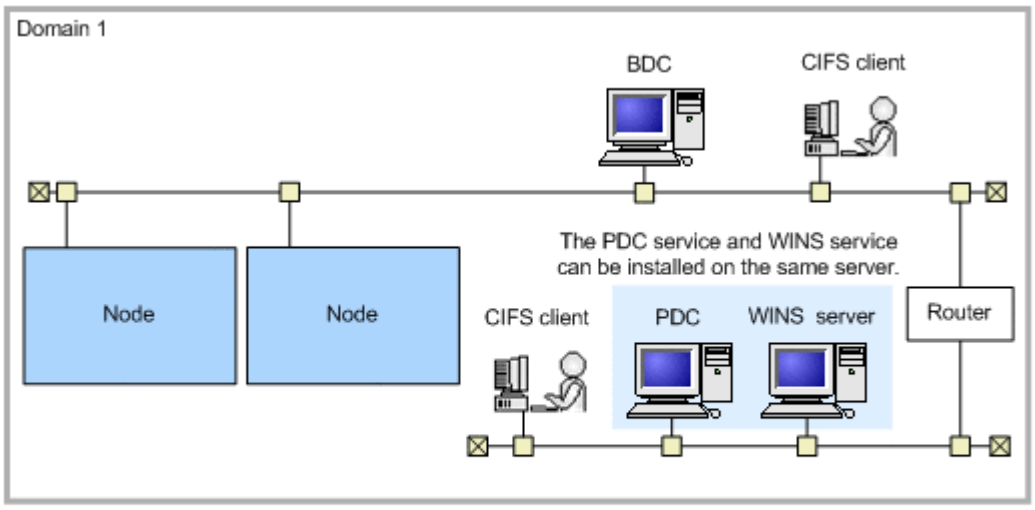
Legend:

PDC : Primary domain controller

BDC : Backup domain controller

Figure 2-8 Network where the node and the primary domain controller exist in the same subnet (NT domain configuration)

The figure below shows an example of a network in an NT domain configuration in which the nodes and the primary domain controller are placed on different subnets.



Legend :

PDC : Primary domain controller

BDC : Backup domain controller

Figure 2-9 Network where the nodes and the primary domain controller are placed on different subnets (NT domain configuration)

In an Active Directory domain configuration, the following figure illustrates a network where the node and the primary domain controller exist in the same subnet.

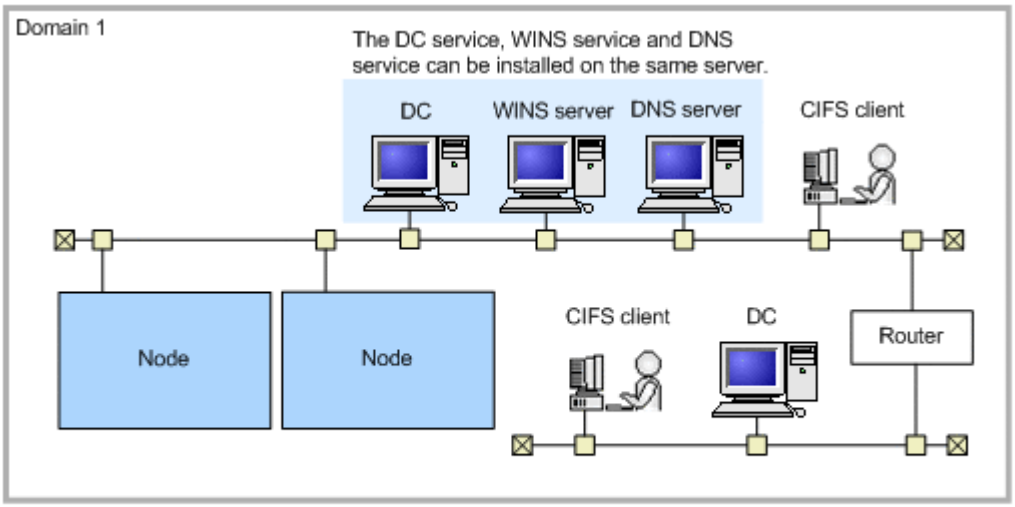


Figure 2-10 Network where the node and the primary domain controller exist in the same subnet (Active Directory domain configuration)

When the CIFS service is used with multiple ports

When the CIFS service is used with multiple ports, a separate WINS server is necessary for each subnet to which each port is connected. All the CIFS clients connected to the network can select an access path to the node for the HDI system according to the used WINS servers.

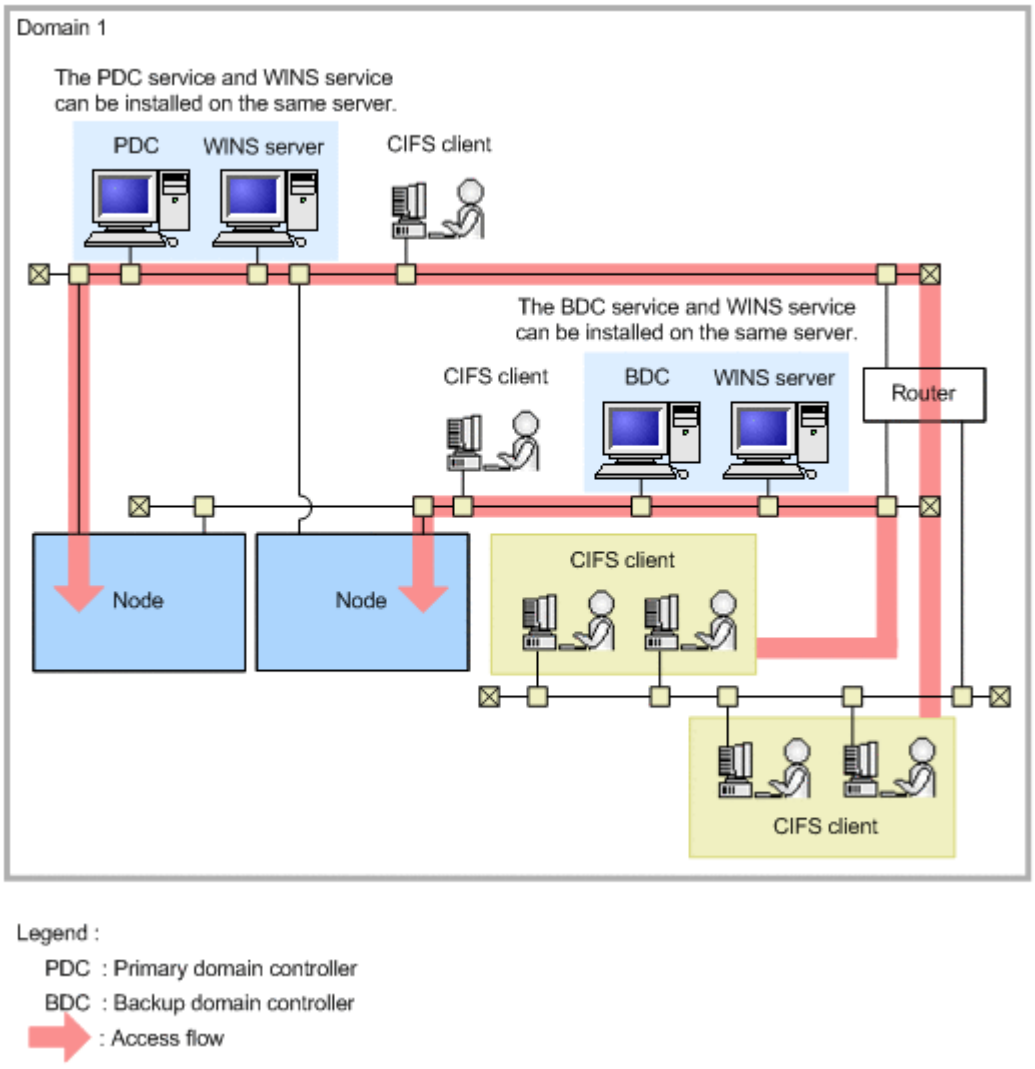


Figure 2-11 Network where multiple ports use the CIFS service

Using trunking in an HDI system

On an HDI system, *link aggregation*, *link alternation*, and *cascaded trunking* can be used to perform trunking. (Cascaded trunking uses both link aggregation and link alternation.)

Link aggregation

In link aggregation, the multiple ports to be aggregated are connected to the same switch, and each port is used simultaneously. Link aggregation can increase the amount of bandwidth usable for communication. Even if a link error occurs on some ports, processing can continue by using the other ports connected to the same switch.

Link alternation

In link alternation, two ports are grouped, and one port is kept in standby in case an error occurs. If a hardware error (such as a switch or NIC

error) does occur, the ports are switched automatically, and processing can continue by using the standby port.

Cascaded trunking

In cascaded trunking, link alternation is set for two ports, including at least one virtual port configured by using link aggregation. Since the combination of link aggregation and link alternation can handle both link errors and hardware errors, we recommend using cascaded trunking to configure networks on an HDI system. When using cascaded trunking, always use it together with a tagged VLAN to stabilize communication between the client and an HDI system.

This subsection describes recommended network configurations for the trunking functionality available on HDI systems.

Features

By using trunking in the HDI system, you can achieve the following:

- If all physical ports connected to the network are trunked, failover can be avoided when some of the ports encounter a link error (note that a failover will occur if all the ports encounter a link error).
- You can simultaneously use multiple physical ports grouped by link aggregation to increase the communication speed of these ports as a single interface.
- Because IP addresses are assigned to trunked virtual ports, the number of IP addresses you need to manage is smaller than when IP addresses are assigned to all physical ports.
- Trunking and a VLAN can be used together. Always use a VLAN together with trunking when using cascaded trunking. To use both a VLAN and trunking, see Using both a VLAN and trunking in an HDI system on page 2-26.

Trunking prerequisites

Before using trunking, verify the following:

- Ports with different media types cannot be trunked. Trunking must only be configured on ports whose media types are identical.
- Ports with different Ethernet standards cannot be trunked. Trunking must only be configured on ports with the same Ethernet standard, such as Gigabit Ethernet or 10 Gigabit Ethernet.
- Before using trunking, you must configure the network environment to which nodes are connected (specify switch settings, for example).
- To use link aggregation, the switches to be used must comply with IEEE802.3ad (Dynamic LACP). Set the LACP mode to Active.
- Depending on the types of switches to which the nodes are connected, the number of ports eligible for link aggregation might be limited. For details on the maximum number of ports that can be link aggregated, see the documentation for the switch being used.

- The switches that are connected to the nodes include a switch that provides a Port Fast/Uplink Fast (or Fast-forwarding) functionality, which is an extension of STP (Spanning Tree Protocol). For continuous operation of the HDI system, we recommend that you enable the Port Fast/Uplink Fast functionality of the switches that are connected to the nodes.
- A failover will occur if a failure occurs on a non-trunked node port. As a result, we recommend that you use trunking for all ports.
- On an HDI system, link alternation cannot be set for three ports or more.
- Before using a trunk port, make sure that the appropriate negotiation mode is set for the port. If the negotiation mode is changed when the port is running, communication via the port might be stopped temporarily.

Recommended trunking configurations

If link aggregation is enabled, in the event of a link error on some ports, processing can continue by using other ports connected to the same switch. If link alternation is enabled, in the event of a hardware error in the switch or NIC hardware, the port will be automatically switched to a standby port to continue processing.

For an HDI system, we recommend that you configure the network using cascaded trunking to ensure that operation can continue even when a link error or hardware error occurs. You should also trunk all ports. This is because if the node contains a port that is not trunked, an error on that untrunked port will cause a failover.

For an HDI system, we recommend that you configure cascaded trunking so that the node that is running will have higher performance than the standby node. Note, however, that a too-large difference in performance between the executing and standby nodes might affect operation because the system performance drastically drops upon changeover to the standby port. Configure the network so that the standby node will maintain the minimum performance required to continue processing.

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

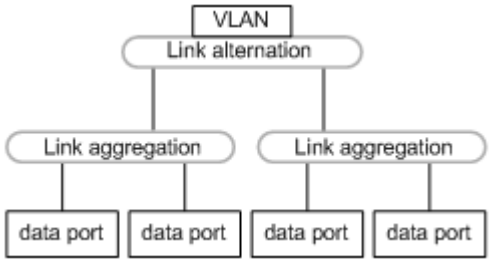


Figure 2-12 Example cascaded trunking configuration recommended for an HDI system

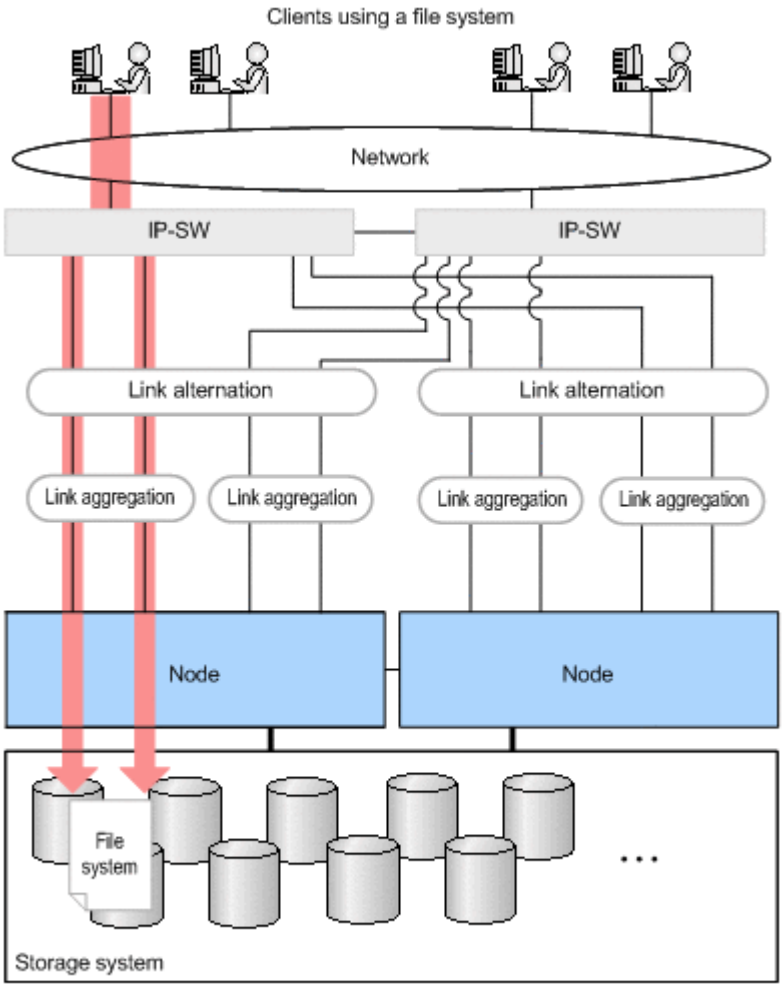
The HDI system does not support the following trunking configurations:

- Link alternation set among three or more ports.

- Trunking set for a link alternation port.
- Link aggregation set for a link aggregation port.

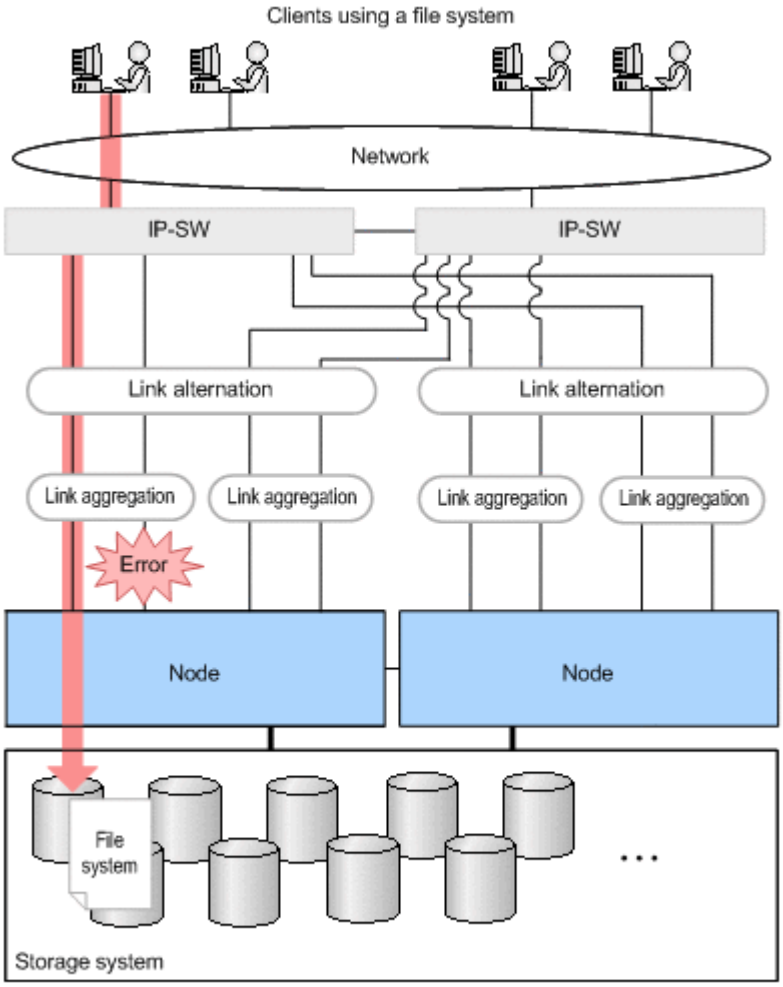
Examples of a network configuration

The following are examples of a network configuration when cascaded trunking is used.



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

Figure 2-13 Example of a network configuration when cascaded trunking is used (when no error has occurred)



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

Figure 2-14 Example of a network configuration when cascaded trunking is used (when a link error has occurred)

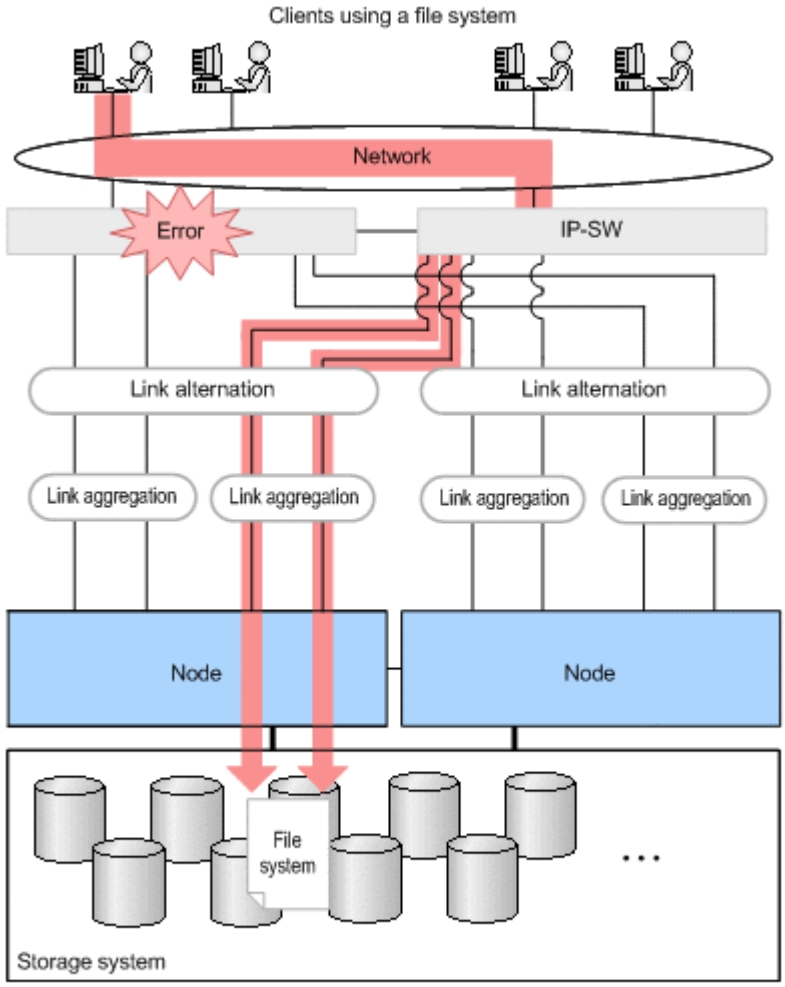


Figure 2-15 Example of a network configuration when cascaded trunking is used (when a hardware error has occurred)

Using a VLAN in an HDI system

HDI systems allow you to use VLANs to configure a network. This subsection outlines VLANs available in an HDI system.

Features

The following describes the features for when a VLAN is used in an HDI system:

- An IEEE802.1Q tagged VLAN can be used.
- Even if a network is configured using a VLAN, in the event of an error in a node, you can perform maintenance work such as error recovery or replacement while the service continues to be provided by a failover.

- You can set an MTU value (the maximum value of data that can be transmitted for each transfer operation in the communication network) for each VLAN.

VLAN prerequisites

To use a VLAN in an HDI system, a switch supporting an IEEE802.1Q tagged VLAN is required.

VLAN interface setting

When a VLAN is used, a virtual interface (a VLAN interface) is created for the data port. An identifier called a *VLAN ID* must be assigned to the VLAN interface.

Also, a virtual IP address can be set for the VLAN interface so that the resource group can be connected using the same IP address during failover. To detect an error such as a link down in both nodes, we recommend that you specify a virtual IP address for both nodes. If you do not specify a virtual IP address, you must check the system message in the **List of RAS Information** page (for `List of messages`) of the **Check for Errors** dialog box.

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

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

Range of VLAN IDs
: You can set VLAN IDs from 1 to 4094. VLAN IDs must not be duplicated within a cluster.

Number of virtual IP addresses
: You can set a maximum of 256 virtual IP addresses per cluster.

Example network configurations

The following shows an example of a network configuration when a VLAN is used.

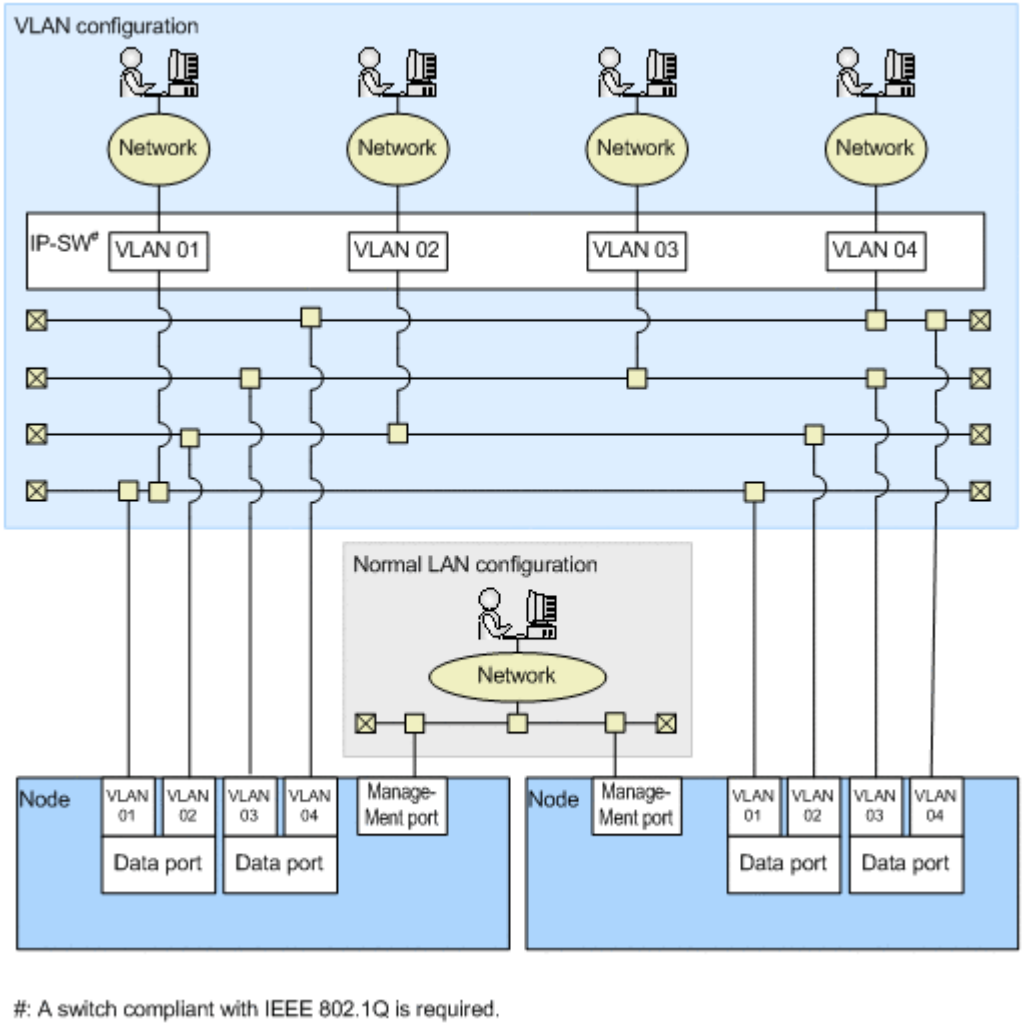


Figure 2-16 Example of a network configuration when a VLAN is used

Using both a VLAN and trunking in an HDI system

In an HDI system, you can use both a VLAN and trunking to configure a network that can provide both VLAN features and trunking features. The VLAN features improve security, and provide an easy and flexible network design. The trunking features provide increased bandwidth for communication, and improve availability.

To configure a network using both a VLAN and trunking, set trunking to combine multiple ports into one logical port, and then set the VLAN interface for this logical port.

System configurations when linking with an HCP system

This section describes system configurations in which HDI systems link with an HCP system.

We recommend that you use the NTP server in order to synchronize the times between the HCP system and the individual devices of the HDI system.

Linking to an HCP system that shares the same storage system

The following figure shows a configuration example of an HDI system that links with an HCP system that shares the same storage system.

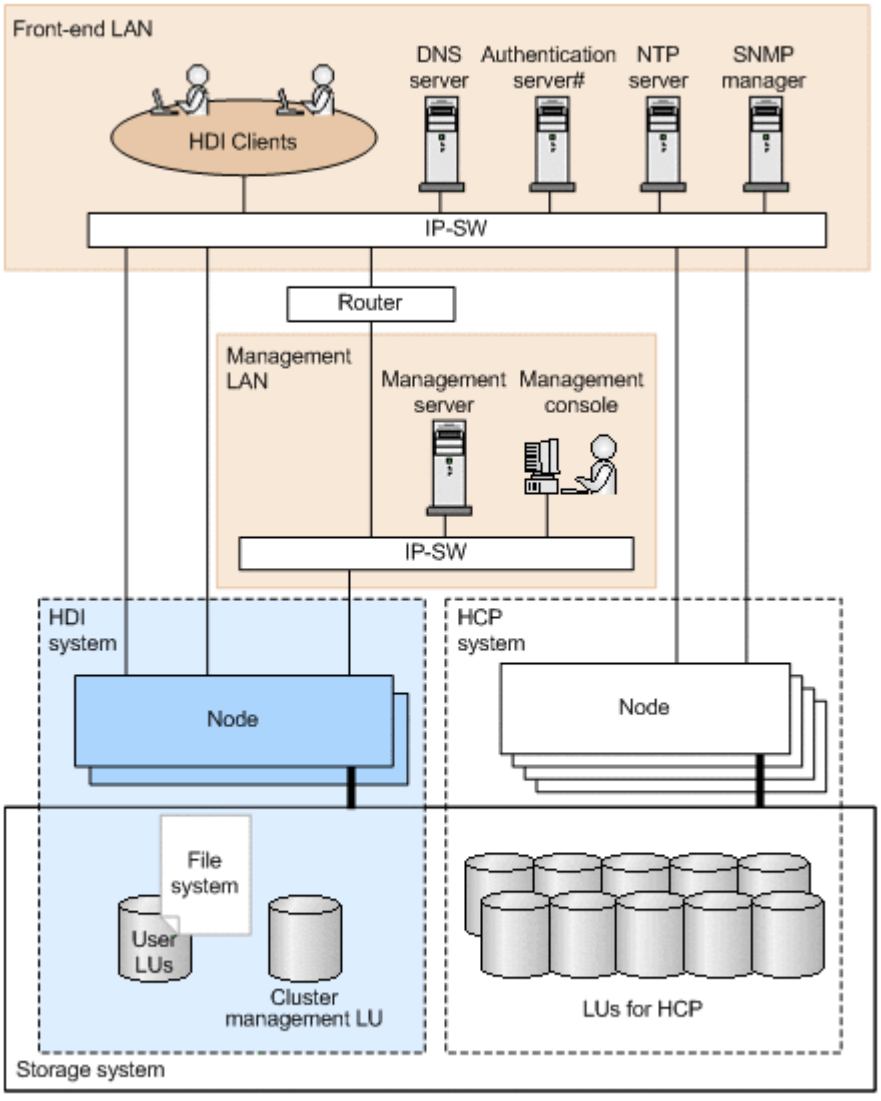


Figure 2-17 Configuration example of an HDI system linking with an HCP system that shares the same storage system

The following conditions must be satisfied to link an HDI system with an HCP system that shares the same storage system:

- Connect the HDI and HCP ports that are used for client data access to the front-end LAN.

- A router is placed between the management LAN and the front-end LAN so that the HCP system on the front-end LAN can communicate with a management server and management console on the management LAN by using `http` or `https`. In addition, if you place an external server on the front-end LAN, specify, as necessary, the settings so that the external server and the management server can communicate.
- The DNS server is placed on the front-end LAN.
- The HCP system that links with the HDI system has a minimum configuration (basic configuration) of 4 nodes and can use up to 16 nodes.
- If you use the HCP GUI on the HDI management console, a DNS server that can resolve the names for the HCP system must be registered in the management console.

When linkage is made via a network

The following figure shows a configuration example of HDI systems that link with an HCP system via a network (WAN) by using Network Address Translation (NAT) functionality or Virtual Private Network (VPN) functionality.

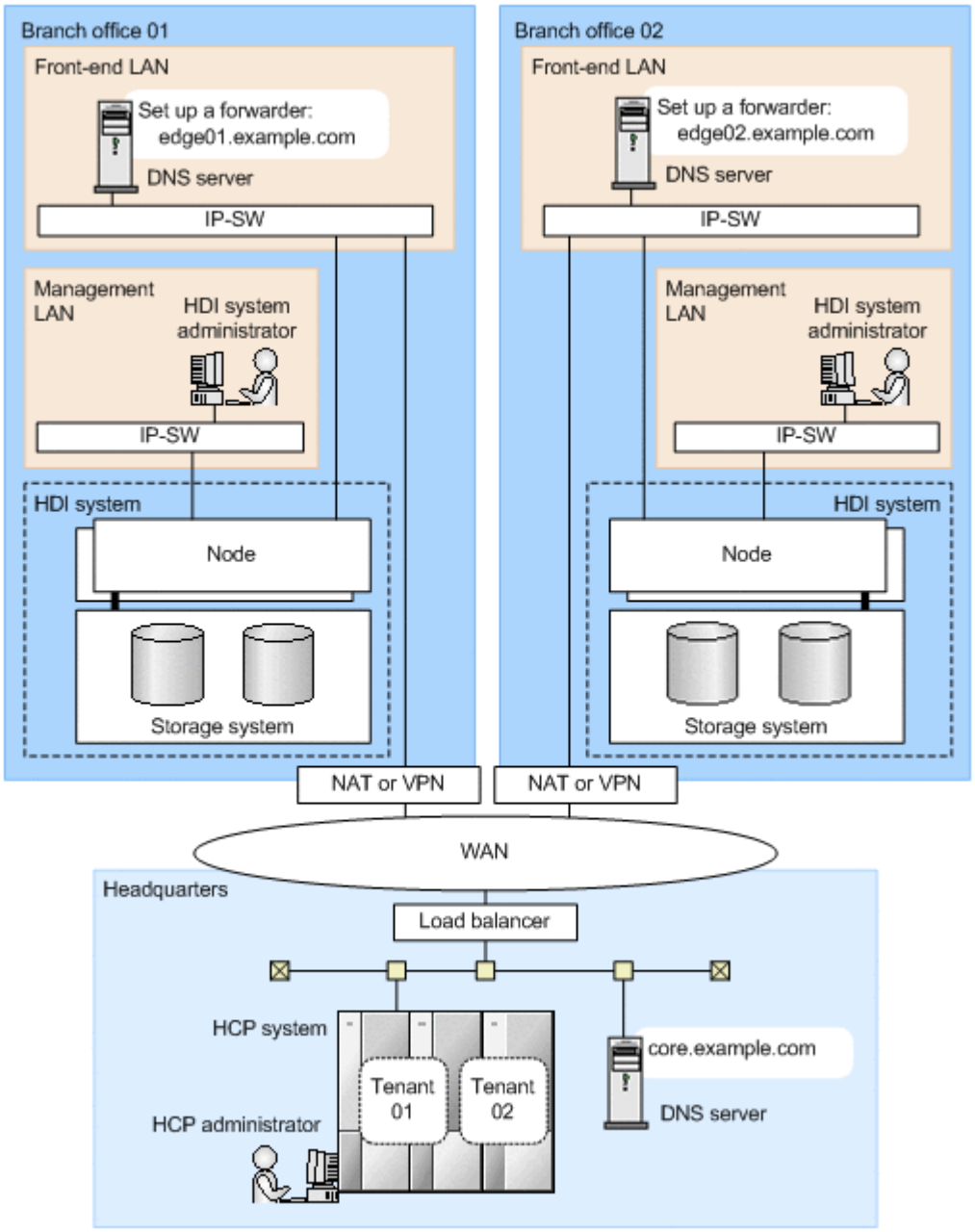


Figure 2-18 Configuration example of HDI systems linking with an HCP system via a network

The following conditions must be satisfied for HDI systems to link with an HCP via a network:

- If the HCP system that links with the HDI system does not use a relaying device such as a load balancer when connecting to the network, for the DNS server used by the HDI system, you need to set a forwarder to the DNS server used by the HCP system so that the names of the HCP nodes can be resolved.

If the HCP system that links with the HDI system uses a relaying device, you need to specify settings so that the HDI system can communicate with the HCP system via the relaying device.

- Ask the HCP administrator to create tenants to be used by the HDI system.
- The HCP system that links with the HDI system has a minimum configuration (basic configuration) of 4 nodes and can use up to 16 nodes.

The settings required for an HCP system that links with the HDI system are as follows:

- If the HCP system that links with the HDI system uses a relaying device when connecting to the network, round-robin DNS cannot be used for load balancing. Use a load balancer or another device for balancing the load as necessary.
- Relaying devices used when an HCP system connects to a network, such as a load balancer, need to be configured to meet the following conditions:
  - The device can communicate with the port used to connect to an HCP system (`80` or `9090` for HTTP, `443` or `9090` for HTTPS).
  - The device can transfer the Host header of an HTTP request without converting it.
  - The device can use chunked transfer encoding.
  - When the file compression function is enabled for communications with an HCP system, gzip can be specified in the Accept-Encoding header.
  - When SSL is enabled, HTTPS communications can be relayed.

3

Environment Settings for External Servers

To run and manage an HDI system, you must provide several external servers on the network.

This chapter describes the environment settings for these external servers.

- DHCP server environment settings
- DNS server environment settings
- Proxy server environment settings

External servers required in an HDI system

The following table summarizes the external servers required in an HDI system.

Table 3-1 External servers required in an HDI system

External server	Description	Settings for linkage with an HDI system
DHCP server	A DHCP server is required in a single-node configuration to set network information such as the IP address or the default gateway of a node using DHCP.	None
DNS server	A DNS server is required for searching for host names via the DNS.	IP address
FTP server	An FTP server is required for downloading dump files, and all log files. A destination directory must be created for the transfer.	• IP address or host name • User name and password • Destination directory
KDC server	A KDC server is required for authenticating users by using Kerberos authentication with the NFS service.	• Server name • Domain name
LDAP server	An LDAP server is required for managing user information on the LDAP server. The LDAP server for user authentication can also be used as a server for NFSv4 domain ID mapping.	• IP address or host name • Port number • Route ID name (in DN format) • Administrator name (in DN format) and password
	An LDAP server is also required for storing information about automatically assigned user IDs and group IDs in the database on the LDAP server.	• IP address or host name • Port number • Route ID name (in DN format) • ID name for adding a user mapping account (in DN format) • Administrator name (in DN format) and password
NIS server	An NIS server is required to search user and host information via the NIS.	• Domain name • IP address or host name (when a specific server is to be used)
NTP server	An NTP server is required for ensuring the correct time on physical nodes.	IP address or host name
SNMP manager	An SNMP server is required for viewing system information and receiving failure reports. Note that an SNMP manager must be connected to the management LAN.	If SNMPv2 will be used: • Community name

External server	Description	Settings for linkage with an HDI system
		• IP address or server name If SNMPv3 will be used: • Verify the user name • Security level • Authentication type, and authentication password • Encryption type, and encryption password
SMTP server	An SMTP server is required to receive error notifications.	• IP address or host name (FQDN) of the SMTP server • Port number • Recipient email addresses • Sender email address • Reply-to email address • Message level for reporting failures
WINS server	A WINS server is required for CIFS clients to resolve names by using WINS. Since an HDI system does not support the WINS client functionality, register the virtual IP address and NetBIOS name of the physical node in the WINS server manually.	None
Scan server	A scan server is required to use the real-time scan functionality.	• IP address or host name • Port number
Domain controller	A domain controller is required for an HDI system to authenticate users by using Active Directory authentication or NT domain authentication.	• Server name • Administrator name and password
	A domain controller is required when Active Directory schema user mapping is used.	Name service switch (SFU or RFC2307 schema)
	A domain controller is also required for mapping IDs on an NFSv4 domain.	• Server name • Administrator name and password • Name service switch (SFU or RFC2307 schema)
Proxy server	A proxy server is required for relaying HTTP or HTTPS communications between an HDI system and an HCP system.	• IP address or host name • Port number • User name and password (when user authentication is to be performed)

External server	Description	Settings for linkage with an HDI system
Management console	A management console is a computer that is needed to use HDI commands or its GUI.	None
Management server	A management server is a computer on which Hitachi File Services Manager has been installed. A management server can also be used as a management console.	None
Relaying devices used by an HCP system to be linked (such as a load balancer)	A relaying device (such as a load balancer) is required for HTTP or HTTPS communications between an HDI system and an HCP system.	IP address or host name

Environment settings for a management server

This section describes the environment settings for a management server.

Requirements for a management server

The following table summarizes the requirements for a management server.

Table 3-2 Requirements for a management server

Item	Requirement
Applicable OSs	• Microsoft(R) Windows Server(R) 2008 R2 Datacenter (with SP1) • Microsoft(R) Windows Server(R) 2008 R2 Enterprise (with SP1) • Microsoft(R) Windows Server(R) 2008 R2 Standard (with SP1) • Microsoft(R) Windows Server(R) 2012 Datacenter#1 • Microsoft(R) Windows Server(R) 2012 Standard#1 • Microsoft(R) Windows Server(R) 2012 R2 Datacenter#1 • Microsoft(R) Windows Server(R) 2012 R2 Standard#1 • Microsoft(R) Windows Server(R) 2016 Datacenter#1 • Microsoft(R) Windows Server(R) 2016 Standard#1
CPU	Minimum configuration: Dual-core processor Recommended configuration: Quad-core or better processor
Memory	Minimum 2 GB

Item	Requirement
	Recommended At least 4 GB[#2]
Disk space	Minimum 7 GB Recommended At least 8 GB You cannot install Hitachi File Services Manager on a disk created by using Windows Thin Provisioning or on a disk whose physical or logical sector size is 4,096 bytes (4K native).
LAN card	10/100 Ethernet LAN card If the computer and the LAN cable are compatible with Gigabit Ethernet, you can use a Gigabit-class card.
DVD-ROM drive	Required

#1:

Both Modern UI and Desktop are available for the user interface. Use Desktop.

#2:

If other software products are used simultaneously, the memory requirements of all of the software products must be taken into account.

If there is not enough virtual memory on the management server, program operations might become unstable, or programs might not be able to start. To stably operate Hitachi File Services Manager, virtual memory that meets the following conditions is required in addition to the virtual memory that is used by the OS and other programs.

Table 3-3 Virtual memory requirement for Hitachi File Services Manager

Program	Virtual memory (MB)
Hitachi Command Suite Common Component (64-bit)	2,501
Hitachi File Services Manager	1,024

If Hitachi Command Suite products are installed on the management server, virtual memory space for those products is also required. The table below lists the recommended amount of virtual memory for each Hitachi Command Suite product as of version 8.5.0 and Hitachi Storage Navigator Modular 2 as of version 28.55. Secure virtual memory that is larger than the total of these sizes.

Table 3-4 Recommended amount of virtual memory for Hitachi Command Suite products (64-bit)

Product	Virtual memory (MB)	
Hitachi Command Suite[#] • Device Manager • Tiered Storage Manager • Replication Manager • Host Data Collector	When the memory heap size in Device Manager is set to Small	7,700
	When the memory heap size in Device Manager is set to Medium	8,200
	When the memory heap size in Device Manager is set to Large	9,200
Tuning Manager		5,000
Global Link Manager		1,000
Compute Systems Manager	When Deployment Manager is used	6,400
	When Deployment Manager is not used	5,000
Hitachi Storage Navigator Modular 2		200

#:

Device Manager, Tiered Storage Manager, Replication Manager, and Host Data Collector are always installed together.

Tip:

- If the Device Manager agent is installed on the management server, secure the virtual memory required for the Device Manager agent. To set a virtual memory size for Device Manager agent, use the `server.agent.maxMemorySize` property. For details about this property, see the *Hitachi Command Suite Installation and Configuration Guide*.
- If Replication Manager Application Agent is installed on the management server, secure the virtual memory required for Replication Manager Application Agent. For the amount of virtual memory to be secured, see the *Hitachi Command Suite Replication Manager Configuration Guide*.
- If the Tuning Manager series agents are installed on the management server, secure the virtual memory required for all agents. For the amount of virtual memory to be secured, see the explanation that describes memory requirements in the applicable agent manual.

Management server cluster configuration

Management servers can be clustered in an active-standby configuration. In a cluster, the server that is being used for operation is called the *executing node* and the server that is standing by so that it can take over operation in the event of an error on the executing node is called the *standby node*.

If an error occurs on the executing node, the cluster software detects this and switches the executing node to the standby node (that is, the standby node

becomes the executing node). This arrangement allows management servers to run continuously without interruption.

Use Microsoft Failover Cluster as a cluster software when the management servers are clustered.

Executing a command with administrative privileges from a command prompt

When you use a Windows operating system that provides the UAC feature and the UAC feature is enabled, some commands can be executed only by users who have administrative privileges. Unless otherwise indicated, when you execute the commands described in the manual from the management server command prompt, you need administrative privileges.

You can use either of the following methods to execute commands that require administrative privileges. We recommend that you use the first method so that you can view the results output to the command prompt.

1. Execute the command from an elevated command prompt. (This is the recommended method.)

   If you are using Windows Server 2008 R2 version, select and right-click the command prompt icon in the **Start** menu and choose **Run as Administrator** to open the elevated command prompt window.

   If you are using Windows Server 2012, move the mouse cursor to the lower-left corner of the desktop and right-click the small Start screen. From the management menu, select **Command Prompt (Admin)** to open the elevated command prompt window.

2. Enter the command from an ordinary command prompt, and then consent to elevating your privileges in the message dialog box that appears.

   When you attempt to execute a command from an ordinary command prompt, a message prompting you to elevate your privileges appears. Consent to this request.

   Note that, with this method, execution results are displayed in a new command prompt window rather than in the command prompt window from which you executed the command. Also, the new window closes automatically when the execution results have been displayed.

   If you choose not to elevate your privileges, the command is not executed, although a return code of 0 (for normal termination) is returned.

Referential note:

Performing one of the following operations from the Windows **Start** menu (or the application list in the Start menu of Windows Server 2012) also requires you to right-click the menu item icon and then choose **Run as Administrator**.

Table 3-5 Operations performed from the Windows Start menu (or the application list in the Start menu of Windows Server 2012) and their menu items

Operation	Menu item
Starting the Hitachi File Services Manager	**Start - HFSM**
Stopping the Hitachi File Services Manager	**Stop - HFSM**
Checking the operating status of the Hitachi File Services Manager	**Status - HFSM**
Acquiring the Hitachi File Services Manager logs	**Get Logs - HFSM**
Uninstalling the Hitachi File Services Manager	**Uninstall - HFSM**

Environment settings for a management console

This section describes the environment settings for a management console.

Requirements for a management console

The following table summarizes the requirements for a management console. Note that if you use the HCP GUI on the management console in an HDI system, the management console must also satisfy the requirements for an HCP console. For details on requirements for an HCP console, see the documentation for the HCP system.

Table 3-6 Requirements for a management console

Item	Requirement
OS	• Microsoft(R) Windows(R) 7 Enterprise (with SP1) • Microsoft(R) Windows(R) 7 Enterprise x64 Edition (with SP1) • Microsoft(R) Windows(R) 7 Professional (with SP1) • Microsoft(R) Windows(R) 7 Professional x64 Edition (with SP1) • Microsoft(R) Windows(R) 7 Ultimate (with SP1) • Microsoft(R) Windows(R) 7 Ultimate x64 Edition (with SP1) • Microsoft(R) Windows(R) 8.1 32-bit[#1] • Microsoft(R) Windows(R) 8.1 64-bit[#1] • Microsoft(R) Windows(R) 8.1 Enterprise 32-bit[#1] • Microsoft(R) Windows(R) 8.1 Enterprise 64-bit[#1] • Microsoft(R) Windows(R) 8.1 Pro 32-bit[#1] • Microsoft(R) Windows(R) 8.1 Pro 64-bit[#1]

Item	Requirement
	• Microsoft(R) Windows(R) 10 Education 32-bit[#2] • Microsoft(R) Windows(R) 10 Education 64-bit[#2] • Microsoft(R) Windows(R) 10 Enterprise 32-bit[#2] • Microsoft(R) Windows(R) 10 Enterprise 64-bit[#2] • Microsoft(R) Windows(R) 10 Home 32-bit[#2] • Microsoft(R) Windows(R) 10 Home 64-bit[#2] • Microsoft(R) Windows(R) 10 Pro 32-bit[#2] • Microsoft(R) Windows(R) 10 Pro 64-bit[#2] • Microsoft(R) Windows Server(R) 2008 Datacenter 32-bit (with SP2) • Microsoft(R) Windows Server(R) 2008 Datacenter 64-bit (with SP2) • Microsoft(R) Windows Server(R) 2008 Enterprise 32-bit (with SP2) • Microsoft(R) Windows Server(R) 2008 Enterprise 64-bit (with SP2) • Microsoft(R) Windows Server(R) 2008 Standard 32-bit (with SP2) • Microsoft(R) Windows Server(R) 2008 Standard 64-bit (with SP2) • Microsoft(R) Windows Server(R) 2008 R2 Datacenter (with SP1) • Microsoft(R) Windows Server(R) 2008 R2 Enterprise (with SP1) • Microsoft(R) Windows Server(R) 2008 R2 Standard (with SP1) • Microsoft(R) Windows Server(R) 2012 Datacenter[#1] • Microsoft(R) Windows Server(R) 2012 Standard[#1] • Microsoft(R) Windows Server(R) 2012 R2 Datacenter[#1] • Microsoft(R) Windows Server(R) 2012 R2 Standard[#1] • Microsoft(R) Windows Server(R) 2016 Datacenter[#1] • Microsoft(R) Windows Server(R) 2016 Standard[#1] • Red Hat Enterprise Linux(R) 6.4[#3]
Memory	At least 512 MB
CPU	Any CPU recommended for the OS installed on the management console
Monitor resolution	At least 1,024 **x** 768 pixels
Monitor display colors	16,777,216 colors (True color, 32-bit) or higher
Web browser[#4]	Any of the following Web browsers: • Internet Explorer 10.0 (32-bit desktop version, when the OS is Windows) • Internet Explorer 11.0[#5] (32-bit desktop version, when the OS is Windows)

Item	Requirement
	• Firefox ESR 38.*x*[#6] (When managing HDI systems in a single node configuration if the architecture is x86 and the OS is Red Hat Enterprise Linux(R)) • Firefox ESR 45.*x*[#6] (When the architecture is x86 and the OS is Windows) • Firefox ESR 52.*x*[#6] (When the architecture is x86 and the OS is Windows) Also, if you are managing an HDI system in a single-node configuration, install Adobe(R) Flash(R) Player 10.1 or later in the web browser.

#1:

Both Modern UI and Desktop are available for the user interface. Use Desktop.

#2:

The only supported browser is Internet Explorer.

#3:

Logging on to the system in a single-node configuration using UPnP (Universal Plug and Play) is unavailable.

#4:

Certain Web browser requirements must be met to view the Hitachi Storage Navigator Modular 2 GUI from Hitachi Files Systems Manager. For details about compatible Web browsers, see the Hitachi Storage Navigator Modular 2 documentation.

#5:

When Internet Explorer 11.0 is used, if you click a button or anchor on the screen to open a new tab or new window, an extra blank window or transitional window might be displayed at the same time. In such a case, please close the unnecessary window.

If such problems occur repeatedly, create a new Windows user account, and then use the new user account to operate the browser.

#6:

x implies any digit. The final number in the version does not affect browser support.

Settings when Internet Explorer is used on the management console

This subsection describes the settings that must be configured when Internet Explorer is used. If you want to change the Web browser settings, close all browsers beforehand. Note that Internet Explorer 10.0 settings are used for this subsection. For details on the settings when the version of Internet Explorer is not 10.0, see Internet Explorer Help.

Notes when using Internet Explorer

Note the following when using Internet Explorer:

- The tabbed browsing function cannot be used.
- A certificate error message or a security warning might be displayed in some dialog boxes. However, this is not a problem because an HDI system uses HTTPS communication between nodes and the management console.

  If you import an SSL certificate to the management server, a certificate error no longer occurs. For details about how to import the required SSL certificate for communication between the management server and nodes, see Importing the required SSL certificate for communication between the node and management server on page 7-99.
- If you change the setting for whether to display the menu bar, Internet Explorer might not operate properly.
- If you enlarge or reduce the font size, the GUI might not be displayed properly, and the scroll bar might not be displayed.
- If you are using Internet Explorer on Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 you might not be able to download files from HTTPS servers, because the Internet Explorer Enhanced Security Configuration setting is enabled by default. In this case, disable the setting Internet Explorer Enhanced Security Configuration.

Internet Explorer settings

The following table shows the settings when using Internet Explorer. For items other than those indicated in the table, use the Internet Explorer default settings.

Table 3-7 Internet Explorer settings

Category	Settings
Text Size	Select **Medium**.
Using the cache[#1]	Select the **Every time I visit the web page** radio button.
Languages	In **Language Preference**, add either "English [en]" or "Japanese [ja]".
Registering URLs as trusted sites zones[#2]	• Clear the **Require server verification (https:) for all sites in this zone** check box. • In the **Add this website to the zone** text box, add the management server URL, the URLs for all managed nodes, and `about:internet`.[#3]
Disabling the pop-up blocker[#4]	In the **Address of website to allow** text box, add the management server URL and the URLs for all managed nodes.[#3]
Disabling download monitoring[#5]	• Enable **File download**.

Category	Settings
	• Clear the **Do not save encrypted pages to disk** check box.
Verifying security settings	• Enable **Run Active X controls and plug-ins**. • Enable **Script Active X controls marked safe for scripting**. • Enable **Active scripting**. • Enable **Launching programs and files in an IFRAME** or specify **Prompt**. • Enable **Submit non-encrypted form data** or specify **Prompt**.
Enabling animations	Select the **Play animations in web pages** check box.
Setting the proxy#6	If a proxy server is used, add the addresses of the management server and all the management-target nodes to the **Exceptions** text box in the **Proxy Settings** dialog box.
Setting tabbed browsing	Select a radio button other than **Always open pop-ups in a new tab**.
Setting the enhanced protected mode	Clear the **Enable Enhanced Protected Mode** check box.
Configuring browser security settings	In the **Advanced** tab of the **Internet Options** dialog box, clear the check boxes **Use SSL 2.0** and **Use SSL 3.0** if they are selected. Select the check boxes **Use TLS 1.0**, **Use TLS 1.1**, and **Use TLS 1.2** if they are cleared.

#1:

If you incorrectly use the cache, an old version of the GUI might be displayed, or the GUI might freeze when File Services Manager or a program that runs on a node is upgraded.

#2:

If the Internet Explorer security enhancement configuration function is enabled, the operations available from the GUI might become limited.

In this case, register the URLs of the management server, all the managed nodes, and `about:internet` into the trusted sites zone of the Internet Explorer security zone.

#3:

Use the following URL format:

- Management server URL:

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

  `http://`*management-server-IP-address-or-host-name* (for non-SSL communication)

  `https://`*management-server-IP-address-or-host-name* (for SSL communication)

- Node URLs:
  Cluster configuration:
  `https://`*fixed-IP-address-of-physical-node-management-port*
  `https://`*virtual-IP-address-of-management-port-of-physical-node*
  Single-node configuration:
  `https://`*IP-address-of-management-port*
- `about:internet`

#4:

If the pop-up blocker is enabled, the login window might not appear or a GUI error might occur. In order to avoid this, you need to disable the pop-up blocker to ensure that pop-ups from the management server will not be blocked.

#5:

If download monitoring is enabled, you cannot download error information or setting files by using the GUI.

The node from which files are downloaded must be registered as a trusted site.

#6:

When a proxy server is used, the correct GUI is not displayed unless the management server and all the management-target nodes are specified as exceptions.

Settings when Firefox is used on the management console

This subsection describes the settings that must be configured when Firefox is used. If you want to change the Web browser settings, close all browsers beforehand.

Notes when using Firefox

If you use Firefox ESR 45.*x* or later, when you set the migration policy, do not use Firefox to save the user name and the password of the account that is used to access the migration-destination namespace.

In the **Migration Task Wizard**, on the **5.Confirmation** page, select the **Apply** button to display the confirmation window, which displays the prompt "Would you like Firefox to remember this login?" From the drop-down menu, select **Never Remember Password for This Site**.

Firefox settings

The following table shows the settings when using Firefox. For items other than those indicated in the table, use the Firefox default settings.

Table 3-8 Firefox settings

Category	Settings
Using the cache[#1]	Follow the procedure below to specify settings: 1. Enter `about:config` in the address bar to display the list of configuration items. 2. In the displayed list, select and double-click **browser.cache.check_doc_frequency**. 3. In the displayed dialog box, enter `1`, which means "Every time I view the page", and then click **OK**.
Languages	From the **Content** tab of the **Options** dialog box, click the **Choose** button in the **Languages** area. In the **Languages** dialog box, add either "English [en]" or "Japanese [ja]" to **Languages in order of preference**.
Setting the pop-up blocker[#2]	From the **Content** tab of the **Options** dialog box, click **Exceptions** for **Block pop-up windows**, and then add the management server URL and the URLs for all managed nodes in the **Address of web site** text box.[#3]
Enabling add-ons[#4]	From the **Security** tab of the **Options** dialog box, click **Exceptions** for **Warn me when sites try to install add-ons**, and then add the management server URL and the URLs for all managed nodes in the **Address of web site** text box.[#3]
Acknowledging security exceptions	If **This Connection is Untrusted** is shown while accessing or downloading data on the management server, managed nodes, you can acknowledge the warning as a security exception by performing the following procedure: 1. Click **I Understand the Risks**. 2. Click **Add Exception**. 3. Make sure that the sites where the management server, managed nodes are located are shown correctly in **Location**, and then click **Confirm Security Exception**.
Configuring windows to close properly[#5]	Follow the procedure below to specify settings: 1. Enter `about:config` in the address bar to display the list of configuration items. 2. In the displayed list, select and double-click **dom.allow_scripts_to_close_windows**. 3. Confirm that the setting has changed from the initial value `false` to `true`.
Setting the proxy[#6]	If a proxy server is used, click the **Settings** button in **Connection** in the **Network** tab of the **Advanced** panel of the **Options** dialog box, and then specify the following addresses in the **No Proxy for** text box. • IP address of the management server • Fixed IP addresses and virtual IP addresses for all of the managed nodes

Category	Settings
Setting the security exceptions in TLS communication (when using Firefox ESR 38.*x* or later)	Follow the procedure below to specify settings: 1. Enter `about:config` in the address bar to display the list of configuration items. 2. In the displayed list, select and double-click **security.tls.insecure_fallback_hosts**. 3. In the displayed dialog box, enter the fixed IP addresses and virtual IP addresses for all of the managed nodes, and then click **OK**. If you want to specify multiple IP addresses, use a comma to separate the IP addresses.

#1:

If you incorrectly use the cache, an old version of the GUI might be displayed, or the GUI might freeze when File Services Manager or a program that runs on a node is upgraded.

#2:

If the pop-up blocker of a Web browser is enabled, the login window might not appear or a GUI error might occur. In order to avoid this, you need to set the pop-up blocker to ensure that pop-ups from the management server will not be blocked.

#3:

Use the following URL format:

- Management server URL:

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

  `http://`*management-server-IP-address-or-host-name* (for non-SSL communication)

  `https://`*management-server-IP-address-or-host-name* (for SSL communication)

- Node URLs:

  Cluster configuration:

  `https://`*fixed-IP-address-of-physical-node-management-port*

  `https://`*virtual-IP-address-of-management-port-of-physical-node*

  Single-node configuration:

  `https://`*IP-address-of-management-port*

#4:

The HDI GUI might not function properly if this setting is disabled.

#5:

Open windows might not close during the operation unless this setting is specified.

#6:

When a proxy server is used, the correct GUI is not displayed unless the management server and all the management-target nodes are specified as exceptions.

Environment settings for the NIS server

A maximum of two NIS servers can be specified.

When two servers of the same type are specified, if a failure occurs on the server that is running, operation continues by automatically switching to the other server.

In an HDI system, you can use the domain controller instead of a UNIX computer for the NIS server.

When managing the HDI user information on the NIS server, keep the following points in mind:

- In a user name or group name, you can use alphanumeric characters for the first character, and alphanumeric characters, hyphens (-), and underscores (_) for the second and subsequent characters.
- The user information must not duplicate any user names, group names, user IDs, or group IDs registered by File Services Manager or registered in an LDAP server for user authentication, otherwise you will not be able to set quotas for that user or group.
- If you perform user mapping for CIFS clients, user IDs and group IDs within the range set in user mapping cannot be used.
- Passwords for the File Services Manager end-user service must be encrypted using either the DES or MD5 algorithm.

If an NFSv4 domain exists in the HDI system, the NIS server can perform ID mapping.

Environment settings for the LDAP server

A maximum of two LDAP servers can be specified.

When two servers of the same type are specified, if a failure occurs on the server that is running, operation continues by automatically switching to the other server.

The following requirements must be satisfied for configuring an LDAP server to be used in an HDI system.

Configuring an LDAP server for user authentication

The following products are required for configuring the server. Use any one of these products to configure the LDAP server.

- OpenLDAP
- Sun Java System Directory Server

The LDAP server configured for user authentication can also be used as an ID-mapping server in an NFSv4 domain.

Configuring an LDAP server for user mapping

The following products are required for configuring the server. Use any one of these products to configure the LDAP server.

- OpenLDAP
- Sun Java System Directory Server
- ADAM

Configuring an LDAP server for system administrator account authentication (when linking with an external authentication server only)

Used software products must comply with LDAP v3.

Configuring an LDAP server for system administrator account authentication (when also linking with an external authorization server)

An external authentication server and external authorization server that satisfy the following requirements must be running on the same computer.

Prerequisite OSs

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Software

Active Directory

Protocol

LDAP v3

Notes on using an LDAP server

Note the following when using an LDAP server:

When using an LDAP server for user authentication

- In a user name or group name, you can use alphanumeric characters for the first character, and alphanumeric characters, hyphens (-), and underscores (_) for the second and subsequent characters.
- The user information must not duplicate any user names, group names, user IDs, or group IDs registered by File Services Manager or registered in an NIS server, otherwise you will not be able to set quotas for that user or group.
- If you perform user mapping for CIFS clients, user IDs and group IDs within the range set in user mapping cannot be used.
- When using the File Services Manager end user service, passwords must be encrypted using one of the following algorithms: DES, MD5, SMD5, SHA or SSHA.

When using an LDAP server for user mapping

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

After restarting the CIFS service, delete the user mapping information cached in the CIFS service environment.

Notes on using OpenLDAP

If you use OpenLDAP to configure an LDAP server, the `sizelimit` directive needs to be set.

When you use an LDAP server configured by using OpenLDAP, you can specify a maximum search number (the number of entries returned by search requests from an LDAP client). The default is 500 entries.

When the number of user information entries and user mapping information entries stored in the LDAP server exceeds the maximum, you will not be able to perform operations, such as:

- Downloading user mapping information in the **List of RAS Information** page (for `Batch-download`) of the **Check for Errors** dialog box, or
- Viewing quotas in the **List of Quota Information** page of the **Edit Quota** dialog box in an HDI system in a cluster configuration.

In addition, **All Users** or **All Groups** will not be correctly displayed in **Special permitted users/groups** in the **Access Control** tab of the **Create and Share File System** dialog box, **Add Share** dialog box, or **Edit Share** dialog box in an HDI system in a cluster configuration. To resolve this problem, add the following sizelimit directive to the LDAP server definitions:

```
sizelimit -1
```

There is no need to create a schema file when using an LDAP server for user authentication.

Notes on using Sun Java System Directory Server

When using Sun Java System Directory Server to configure an LDAP server, client restrictions need to be set.

For an LDAP server configured by using Sun Java System Directory Server, you can specify the maximum search number (the number of entries that can be returned in response to search requests from an LDAP client). The default is 2,000 entries.

When the number of user information entries and user mapping information entries stored in the LDAP server exceeds the maximum, you will not be able to perform operations, such as:

- Downloading user mapping information in the **List of RAS Information** page (for `Batch-download`) in the **Check for Errors** dialog box, or

- Viewing quotas in the **List of Quota Information** page in the **Edit Quota** dialog box in an HDI system in a cluster configuration.

In addition, **All Users** or **All Groups** will not be correctly displayed in **Special permitted users/groups** in the **Access Control** tab of the **Create and Share File System** dialog box, **Add Share** dialog box, or **Edit Share** dialog box in an HDI system in a cluster configuration. To prevent this problem, change the maximum number of search results to **Unlimited** for the LDAP server configured by using Sun Java System Directory Server.

The following describes the procedure for changing the maximum number of search results to **Unlimited**. For details on the terms used in the procedure, see the Sun Microsystems documentation.

To change the maximum number of search results:

1. In the **Configuration** page at the top level in the LDAP server configured by using Sun Java System Directory Server, display the directory tree, and then select **Performance**.
2. In the right panel, choose the **Client Control** tab.
3. For **Size Limit** and **Look-through Limit**, select the check box for **Unlimited**.
4. Click the **Save** button.

   A message appears, indicating that Sun Java System Directory Server must be restarted.
5. Click the **OK** button.
6. Click the **Tasks** tab, and then click the button for restarting Sun Java System Directory Server.

   A dialog box confirming that you want to restart Sun Java System Directory Server appears. Click **Yes**.
7. Click **Close** to close the **Restart Directory Server** dialog box.

There is no need to create a schema file when using an LDAP server for user authentication.

Notes on using ADAM

When using ADAM to configure an LDAP server for user mapping, restrictions on the search numbers need to be set.

When you use an LDAP server configured by using ADAM, you can specify a maximum search number (the number of entries returned in response to search requests from an LDAP client). The default is 1,000 entries.

When the number of user mapping information entries in the LDAP server exceeds the maximum, downloading of user mapping information in the **List of RAS Information** page (for `Batch-download`) of the **Check for Errors** dialog box will fail. To prevent this problem, increase the limit value in `MaxPageSize` so that the maximum number of search results does not exceed the total number of managed users and groups.

The following describes the procedure for increasing the `MaxPageSize` limit. For details on the **ADAM ADSI Edit** tool and the terms used in the procedure, see the Microsoft documentation.

To expand the limit:

1. Use the **ADAM ADSI Edit** tool to connect to the configuration partition.
2. Expand the console tree, click **CN=Services**, **CN=Windows NT**, **CN=Directory Service**, and then click **CN=Query-Policies**.
3. In the Details window, double-click **CN=Default Query Policy**. In the Properties window, double-click the **lDAPAdminLimits** attribute to edit the attribute value.
4. Select **MaxPageSize=1000**, and then click the **Remove** button.
5. Enter **MaxPageSize=***limit*, and then click the **Add** button.
   For *limit*, enter the sum of the maximum number of users and the maximum number of groups, considering the range of user IDs and group IDs to be set when you set user mapping in File Services Manager.
6. Click **OK** twice to complete the setting.

Note that ADAM does not support LDAP server configurations for user authentication and cannot be used for such purposes.

Settings example when using OpenLDAP

This section provides a settings example when using OpenLDAP to configure an LDAP server.

Creating a schema file

To enable user mapping using LDAP, create a schema file that defines attributes and object classes recognized by the LDAP server configured by using OpenLDAP. You must define the attribute and object classes to store the user IDs and group IDs that have been converted by using the user mapping functionality.

The HDI system provides a schema file (`samba.schema`) for user mapping using LDAP. Obtain the schema file from the following directory by using the `scp` command from the remote host:

`/usr/share/doc/cifs/examples/samba.schema`

When you create a schema file for the LDAP server configured by using OpenLDAP, define the following attribute and object classes:

```
attributetype ( 1.3.6.1.4.1.7165.2.1.20 NAME 'sambaSID'
        DESC 'Security ID'
        EQUALITY caseIgnoreIA5Match
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{64} SINGLE-VALUE )
objectclass ( 1.3.6.1.4.1.7165.2.2.7 NAME 'sambaUnixIdPool' SUP top AUXILIARY
        DESC 'Pool for allocating UNIX uids/gids'
        MUST ( uidNumber $ gidNumber ) )
objectclass ( 1.3.6.1.4.1.7165.2.2.8 NAME 'sambaIdmapEntry' SUP top AUXILIARY
        DESC 'Mapping from a SID to an ID'
        MUST ( sambaSID )
        MAY ( uidNumber $ gidNumber ) )
```

```
objectclass ( 1.3.6.1.4.1.7165.2.2.9 NAME 'sambaSidEntry' SUP top STRUCTURAL
        DESC 'Structural Class for a SID'
        MUST ( sambaSID ) )
```

After a schema file is created or obtained, add the include directive to the LDAP server definitions to read the schema file required to use the user mapping functionality.

The following example demonstrates the usage of the include directive when the schema file is stored in the directory `/etc/ldap/schema`:

```
include /etc/ldap/schema/samba.schema
```

Setting the index directive

When you store a large number of user IDs and group IDs in the LDAP server configured by using OpenLDAP, the search performance of the LDAP server might be adversely affected. In such a case, set the index directive. We recommend that you set the index directive in the LDAP server definitions as follows:

LDAP server for user authentication

```
index uidNumber,gidNumber,objectClass,uid,cn,memberUid eq
```

LDAP server for user mapping

```
index uidNumber,gidNumber,objectClass,sambaSID eq
```

If you have changed the index directive, you must re-create an index based on the database currently stored in the LDAP server. Use the `slapindex` command provided by OpenLDAP to re-create an index. When executing the `slapindex` command, stop the LDAP server, execute the `slapindex` command, and then restart the LDAP server.

Settings example when using Sun Java System Directory Server

This section provides a settings example when using Sun Java System Directory Server to configure an LDAP server.

Creating a schema file

To enable user mapping using LDAP, create a schema file that defines attributes and object classes recognized by the LDAP server configured by using Sun Java System Directory Server. You must define the attribute and object classes to store the user IDs and group IDs that have been converted by using the user mapping functionality.

The HDI system provides a schema file (`samba.ldif`) for user mapping using LDAP. Obtain the schema file from the following directory by using the `scp` command from the remote host:

```
/usr/share/doc/cifs/examples/samba.ldif
```

When you create a schema file for the LDAP server configured by using Sun Java System Directory Server, define the following attribute and object classes:

```
dn: cn=schema
changetype:modify
add: attributeTypes
attributeTypes: ( 1.3.6.1.4.1.7165.2.1.20 NAME 'sambaSID' DESC 'Security ID'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE X-ORIGIN 'user defined' )
-
add:objectClasses
objectClasses: ( 1.3.6.1.4.1.7165.1.2.2.7 NAME 'sambaUnixIdPool' SUP top
  AUXILIARY MUST ( uidNumber $ gidNumber ) X-ORIGIN 'user defined' )
-
add:objectClasses
objectClasses: ( 1.3.6.1.4.1.7165.1.2.2.8 NAME 'sambaIdmapEntry' SUP top
  AUXILIARY MUST sambaSID MAY ( uidNumber $ gidNumber ) X-ORIGIN  'user
defined' )
-
add:objectClasses
objectClasses: ( 1.3.6.1.4.1.7165.1.2.2.9 NAME 'sambaSidEntry' SUP top
  STRUCTURAL MUST sambaSID X-ORIGIN 'user defined' )
-
```

After a schema file is created or obtained, enter the following command to expand the schema so that you can read the schema file for using the user mapping functionality. If you are prompted for a password, enter the password that was set for `cn=Directory Manager` during installation.

```
#ldapmodify -h host-name -p port-number -D "cn=Directory Manager" -w
- -f samba.ldif
```

Use the `ldapmodify` command provided by Sun Java System Directory Server (do not use the command of the same name provided by OpenLDAP). In *host-name*, specify the host name of the LDAP server configured by using Sun Java System Directory Server. In *port-number*, specify the LDAP port number that you set when installing Sun Java System Directory Server.

Setting an index

When you store a large number of user IDs and group IDs in the LDAP server configured by using Sun Java System Directory Server, the search performance of the LDAP server might be adversely affected. In such a case, set indexes.

We recommend that you set an equivalent index in the Sun Java System Directory Server definitions, as follows:

LDAP server for user authentication

Set an equivalent index (`eq`) for `uidNumber`, `gidNumber`, `memberUid`, `uid`#, and `cn`#.

#: An equivalent index is set by default.

LDAP server for user mapping

Set an equivalent index (`eq`) for `uidNumber`, `gidNumber`, and `sambaSID`.

The procedure for setting an equivalent index (`eq`) is described below. For details on the terms used in the procedure, see the Sun Microsystems documentation.

To set an equivalent index:

1. In the **Configuration** page at the top level in the LDAP server configured by using Sun Java System Directory Server, expand the **Data** node, and then select the suffix for which you want to create an index.
2. In the right panel, choose the **Indexes** tab.
   You cannot change the system index table.
3. Add an index with the attribute shown in the **Additional Indexes** table.
4. To add an index whose attribute is not generated, click the **Add Attributes** button.
   In the dialog box that appears, select the attributes for generating the index, and then click **OK**.

   LDAP server for user authentication

   Select `uidNumber`, `gidNumber`, `memberUid`, `uid`#, and `cn`#.

   #: An equivalent index is set by default.

   LDAP server for user mapping

   Select `uidNumber`, `gidNumber`, and `sambaSID`.
5. To change the index of an attribute, in the **Additional Indexes** table, select the check box for the index type that you want to maintain with the attribute.

   LDAP server for user authentication

   Make sure that the check boxes for the **Equivalent** index are selected for `uidNumber`, `gidNumber`, `memberUid`, and `uid`. Clear the check boxes for the **Presence** index. Do not select any other check boxes. Make sure that the check boxes for the **Equivalent**, **Presence**, and **Partial String** indexes are selected for `cn`. Do not select any other check boxes.

   LDAP server for user mapping

   Make sure that the check boxes for the **Equivalent** index are selected for `uidNumber`, `gidNumber`, and `sambaSID`. Clear the check boxes for the **Presence** index. Do not select any other check boxes.
6. Click **Save** to save the new index setting.
   A warning dialog box appears, indicating that the database file must be updated before you can use the new index.
   You can either re-create the index for the suffix or re-initialize the suffix. Since mapping information is not yet registered, select **Do nothing**.

Settings example when using ADAM

This section provides a settings example when using ADAM to configure an LDAP server for user mapping.

Creating a schema file

To enable user mapping using LDAP, create a schema file that defines attributes and object classes recognized by the LDAP server configured by

using ADAM. You must define the attribute and object classes to store the user IDs and group IDs that have been converted by using the user mapping functionality.

The HDI system provides a schema file (`samba.ldf`) for user mapping using LDAP. Obtain the schema file from the following directory by using the SCP functionality from the remote host:

`/usr/share/doc/cifs/examples/samba.ldf`

When you create a schema file for the LDAP server configured by using ADAM, define the following attribute and object classes:

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

dn: CN=gidNumber,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: attributeSchema
cn: gidNumber
instanceType: 4
attributeID: 1.3.6.1.1.1.1.1
attributeSyntax: 2.5.5.9
isSingleValued: TRUE
showInAdvancedViewOnly: FALSE
adminDisplayName: gidNumber
adminDescription: An integer uniquely identifying a group in an
administrative domain
oMSyntax: 2
searchFlags: 1
lDAPDisplayName: gidNumber
systemOnly: FALSE
systemFlags: 16

dn: CN=sambaSID,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: attributeSchema
cn: sambaSID
instanceType: 4
attributeID: 1.3.6.1.4.1.7165.2.1.20
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: FALSE
adminDisplayName: sambaSID
adminDescription: Security ID
oMSyntax: 64
searchFlags: 1
lDAPDisplayName: sambaSID
systemOnly: FALSE
```

```
systemFlags: 16

dn: CN=sambaUnixIdPool,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: classSchema
cn: sambaUnixIdPool
instanceType: 4
possSuperiors: container
subClassOf: top
governsID: 1.3.6.1.4.1.7165.1.2.2.7
rDNAttID: cn
showInAdvancedViewOnly: FALSE
adminDisplayName: sambaUnixIdPool
adminDescription: Pool for allocating UNIX uids/gids
objectClassCategory: 3
lDAPDisplayName: sambaUnixIdPool
systemOnly: FALSE
systemPossSuperiors: organizationalUnit
systemPossSuperiors: domainDNS
mustContain: uidNumber
mustContain: gidNumber
defaultSecurityDescriptor:
 D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDS DDTSW;;;SY)
(A;;RPLCLORC;;;AU)
systemFlags: 16
defaultHidingValue: FALSE

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

dn: CN=sambaSidEntry,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: classSchema
cn: sambaSidEntry
instanceType: 4
possSuperiors: container
subClassOf: top
governsID: 1.3.6.1.4.1.7165.1.2.2.9
rDNAttID: sambaSID
showInAdvancedViewOnly: FALSE
adminDisplayName: sambaSidEntry
adminDescription: Structural Class for a SID
objectClassCategory: 1
```

```
lDAPDisplayName: sambaSidEntry
systemOnly: FALSE
systemPossSuperiors: organizationalUnit
systemPossSuperiors: domainDNS
mustContain: sambaSID
defaultSecurityDescriptor:
 D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDS DDTSW;;;SY)
(A;;RPLCLORC;;;AU)
systemFlags: 16
defaultHidingValue: FALSE
```

After a schema file is created or obtained, enter the following command at the command prompt, on one line, to read the schema file for using the user mapping functionality.

```
ldifde -i -f C:\samba.ldf -s localhost:port-number -j . -k -c
"CN=Schema,CN=Configuration,DC=X" #schemaNamingContext
```

In this example, the schema file is saved as `C:\samba.ldf`. For *port-number*, specify the LDAP port number that was specified when ADAM was installed. The `ldifde` command exists in the system when ADAM or Active Directory is installed. To use the `ldifde` command for ADAM, choose **Start**, **All programs**, **ADAM**, and then **ADAM Tool command Prompt**.

Setting an index

When you store a large number of user IDs and group IDs in the LDAP server configured by using ADAM, the search performance of the LDAP server might be adversely affected. In such a case, set an index.

When you use ADAM to expand a schema, an index is set for the expanded attributes `uidNumber`, `gidNumber`, and `sambaSID`. The following describes the procedure for setting an index for `objectClass` that is the system's existing attribute. For details on the **ADAM ADSI Edit** tool and the terms used in the procedure, see the Microsoft documentation.

To set an index:

1. Use the **ADAM ADSI Edit** tool to connect to the schema partition.
2. Expand the console tree. In the Details window, double-click **cn=Object-Class**.
3. In the Properties window, double-click the **searchFlags** attribute to edit the attribute value.

   The current setting is `8`. Change it to `9`.

   If the setting has already been changed, modify the value as follows:

   Odd number:

   Use the setting without modification.

   Even number:

   Increase the setting value by one.
4. Click **OK** twice to close the dialog box.

Environment settings for the domain controller

If you use the domain controller for Active Directory schema user mapping or as an NFSv4 domain for ID mapping, configure Active Directory on the domain controller. If you are using GUI on Windows Server 2008, also install the ID management tool for UNIX.

If the backup domain controller meets the above conditions, make sure to use the same name service switch (either SFU or the RFC2307 schema) as the primary domain controller.

In addition, if you use Active Directory schema user mapping, make sure that **Domain controller: LDAP server signing requirements** of the domain controller policy is not **Require signing**.

To check the domain controller policy, choose **Administrative Tools**, **Group Policy Management Editor**, **Computer Configuration**, **Policies**, **Windows Settings**, and then **Security Settings**. In the window that appears, choose **Local Policies** and then **Security Options**, and then check whether **Domain controller: LDAP server signing requirements** is specified.

When choosing a computer name for a domain controller that authenticates CIFS clients, we recommend a name that is 15 bytes or less. In order for the HDI system to be able to perform name resolution, if you choose a computer name that is greater than 15 bytes, register only the first 15 bytes of the computer name using a service such as DNS or `lmhosts`. If a computer name is not registered, the CIFS service might not properly start up and user authentication might not properly function. Note that each domain controller name must be unique within a system.

If the domain controller, which is used to authenticate the CIFS service, uses NTLMv2 authentication, do not set the network security setting to `Send NTLMv2 response only\refuse LM & NTLM` or else the CIFS service will fail to start up. As such, do not use the setting listed above for the network security setting.

To set a network security setting for the domain controller, Choose **Administrative Tools**, **Group Policy Management Editor**, **Computer Configuration**, **Policies**, **Windows Settings**, and then **Security Settings**. In the window that appears, choose **Local Policies**, **Security Options**, and then **Network security: LAN Manager authentication level**.

If Kerberos authentication is used to authenticate users for the NFS service, the Active Directory domain controller can be used for the KDC server. For details on how to set up an environment for the KDC server, see Environment settings for the KDC server on page 3-28.

Environment settings for the KDC server

The following requirements must be satisfied for configuring a KDC server to be used.

Configuring a KDC server for user authentication

You can use a UNIX computer or the Active Directory domain controller for the KDC server.

However, if you use Active Directory authentication for the CIFS service and Kerberos authentication for the NFS service at the same time, you will need to share the Active Directory domain controller. If you plan to use Active Directory authentication for the CIFS service, we recommend that you use the Active Directory domain controller for the KDC server.

If you newly start using Active Directory authentication for the CIFS service when a UNIX computer is used for the KDC server, delete the current KDC server definition. After that, define the Active Directory domain controller used for Active Directory authentication as the KDC server, and then restart the NFS service.

Configuring a KDC server for system administrator account authentication

A computer used as a KDC server must satisfy the requirements below. If you use both an external authentication server and external authorization server, they must be running on the same computer.

Prerequisite OSs

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Software

Active Directory

Protocol

External authentication server: Kerberos v5

External authorization server: LDAP v3

Environment settings for the RADIUS server

When RADIUS authentication is used to authenticate system administrator user accounts, a computer used as a RADIUS server must satisfy the following requirements:

When linking with an external authentication server only

The server must support an RFC2865-compliant PAP or CHAP as the PPP authentication protocol.

When also linking with an external authorization server

An external authentication server and external authorization server that satisfy the following requirements are required. Note that they can be the same computer or different computers.

External authentication server

The server must support an RFC2865-compliant PAP or CHAP as the PPP authentication protocol.

External authorization server

The server must satisfy the following requirements:
Prerequisite OSs:
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Software: Active Directory
Protocol: LDAP v3

Environment settings for the SNMP manager

This section describes the environment settings for the SNMP manager.

Configuring the machine to be used for the SNMP manager

On the machine to be used for the SNMP manager, set the character encoding to Unicode (UTF-8). Note that if the trap messages received by the SNMP manager include non-ASCII characters, the messages are not displayed correctly.

Setting specific-traps

If specific-traps for the HDI system are set in the SNMP manager, you can specify whether the SNMP manager receives SNMP traps issued by the HDI system. By setting necessary specific-traps in accordance with the operational procedure, you can make the SNMP manager receive the specific traps issued by the HDI system.

The following shows the enterprise-OID of specific-traps for the HDI system.
`.1.3.6.1.4.1.116.3.11.5.0`

The following table lists specific-traps for the HDI system.

Table 3-9 Specific-traps for the HDI system

ID	Specific-trap	Description
0	stdTrapNotice	This trap is disabled.
1	stdEventTrapFatalError	A message of the Fatal Error level was received.
2	stdEventTrapError	A message of the Error level was received.
3	stdEventTrapWarning	A message of the Warning level was received.
4	stdEventTrapInformation	A message of the Information level was received.

ID	Specific-trap	Description
5	stdQuotaTrapFSSoftLimit	The SNMP agent detected a user or group that exceeded a quota soft limit specified in the HDI system.
6	stdQuotaTrapFSLimitExceeded	The SNMP agent detected a user or group that exceeded a quota grace period specified in the HDI system.
7	stdCoreTrap	The `core` file was detected.
8	stdQuotaTrapFSSummary	The following user or group was detected: • A user or group that exceeded a quota soft limit specified in the HDI system. • A user or group that exceeded a quota grace period specified in the HDI system.
9	stdQuotaTrapFSDetailSuppress	The individual notification of quotas for each file system in the HDI system was suppressed.
10	stdQuotaTrapFSSubtreeSoftLimit	The SNMP agent detected that a subtree quota soft limit, specified in the HDI system, has been exceeded.
11	stdQuotaTrapFSSubtreeLimitExceeded	The SNMP agent detected that a subtree quota grace period, specified in the HDI system, has been exceeded.
12	stdQuotaTrapFSSubtreeSummary	The following user, group, or directory was detected: • A user, group, or directory that exceeded a subtree quota soft limit specified in the HDI system. • A user, group, or directory that exceeded a subtree quota grace period specified in the HDI system.
13	stdQuotaTrapFSSubtreeDetailSuppress	The individual notification of subtree quotas for each directory in the HDI system was suppressed.

Obtaining a definition file for Hitachi MIB objects

When you import a MIB definition file for Hitachi MIB objects into the SNMP manager, load the file from the media provided with the HDI system.

Note:

Load the latest MIB definition file into the SNMP manager.

If an older MIB definition file is loaded, the SNMP manager might not correctly recognize the MIB objects that are obtained.

`\etc\snmp\STD-EX-MIB.txt`

For details on how to load the MIB definition file, see the documentation for the SNMP program you are using.

If an HDI system and Hitachi Essential NAS Platform are managed by one SNMP manager and the MIB group name and object name of Hitachi Essential NAS Platform are to be used for the operation, use the following MIB definition file stored in the media of Hitachi Essential NAS Platform.

`\etc\snmp\E-NAS-EX-MIB.txt`

SNMP agent version

HDI systems use net-snmp 5.4.1 as the SNMP agent on a node. Depending on the SNMP program used, MIB definition files need to be downloaded from the net-snmp web site, and loaded into the SNMP manager. For details on how to check the version of the SNMP program and load MIB definition files, see the documentation for the SNMP program used.

Trap notification when the SNMP agent starts or stops

Before the SNMP agent on a node starts or stops, the following trap text notification is sent to the SNMP manager:

Trap text sent when SNMP agent on a node starts

MIB Object name: `coldStart`

OID: `.1.3.6.1.6.3.1.1.5.1`

Trap text sent when SNMP agent on a node stops

MIB Object name: `nsNotifyShutdown`

OID: `.1.3.6.1.4.1.8072.4.0.2`

Although this notification is usually sent as a result of the SNMP agent being started or stopped because the OS has started or stopped, this notification is also sent when the SNMP agent is restarted in the following situations:

- When the `/etc/snmp/snmpd.conf` file is updated in File Services Manager
- 00:00 every day (when the SNMP agent is automatically restarted)

You can prevent the notification from being sent as a result of the SNMP agent being started or stopped by changing the SNMP manager settings.

Setting the HDI engine ID

If you need to set the HDI engine ID in the SNMP manager when SNMPv3 is used, obtain the MIB object below from HDI, and then specify the engine ID. For details about the engine ID specification format, see the documentation for the SNMP manager.

Object name: `snmpEngineID`

OID: `.1.3.6.1.6.3.10.2.1.1`

The HDI engine ID is changed when you install an OS on an HDI node as a new installation or when you restore the system LU that was damaged due to

a failure on the OS disk. After you perform such a task, re-obtain the above MIB object, and then set the engine ID again in the SNMP manager.

Environment settings for the NTP server

Use a unique combination for the host name and IP address when you set an NTP server. For example, in an environment where the DNS round-robin function changes the combination of host name and IP address for each response, time cannot be synchronized with an NTP server whose IP address is different from the initial IP address.

For a Windows server that is a domain controller or member server of the Active Directory domain, if you want to use the server as an NTP server, you will need to configure the server so that its system time can be synchronized with that of other NTP servers in the network. To do this, from the **Local Group Policy Editor** (`gpedit.msc`), click **Computer Configuration**, **Administrative Templates**, **System**, and then **Windows Time Service**, specify the settings as follows, and then restart the Windows Time service.

Time Providers

Enable **Configure Windows NTP Client**.

Enable **Enable Windows NTP Client**.

Enable **Enable Windows NTP Server**.

Configure Windows NTP Client Properties

NtpServer: Specify the IP address of the NTP server to be synchronized.

Type: Specify `NTP`.

SpecialPollInterval: Specify a value of 3,600 or lower.

For a Windows server that does not belong to the Active Directory domain is to be used as an NTP server, if you want to synchronize the system time of the server with that of other NTP servers in the network, you will need to configure the above settings, set the following properties, and then restart Windows Time Service.

Global Configuration Settings Properties

AnnounceFlags: Specify `5`.

LocalClockDispersion: Specify `0`.

Note that, if you need to use Windows Server as an NTP server in an environment where Windows Server cannot synchronize its time with other NTP servers, specify the settings as follows, and then restart the Windows Time service.

Time Providers

Enable **Configure Windows NTP Client**.

Disable **Enable Windows NTP Client**.

Enable **Enable Windows NTP Server**.

Global Configuration Settings Properties

AnnounceFlags: Specify `5`.

LocalClockDispersion: Specify `0`.

Environment settings for the scan server

This section describes the environment settings for the scan server.

Connect a scan server to the network, and then install scan software on the scan server. Note that if scan software is used within a cluster, the scan software product must be the same and have the same version. Be particularly careful when using multiple scan servers.

All scan servers must have the same settings in a cluster. Also note that all virus definition files on the scan servers must be updated to the latest version at the same time to prevent infection by recent viruses.

The settings necessary to link the scan server, on which scan software has been installed, with the HDI system are as follows. For details on the setup procedure and notes, see the documentation for the scan software you are using.

When using Symantec Corporation virus scan software

- Setting the scan software connection protocol

  Set up the connection protocol so that the ICAP interface can be used as the connection protocol to the HDI system.
- Setting the bind address

  When limiting the number of clients that can connect, set up a bind address to enable the node to access as a client of the scan server.
- Setting the port number

  Set the same number as the port number specified for the scan server in the HDI system. If the port number entered on the scan server differs from the port number set for the HDI system, the HDI system cannot be connected to the scan server.
- Setting methods of repairing infected files

  Set the way in which the system will respond to infected files when they are detected.
- Setting the data trickle function

  Disable the data trickle function. Note that if you enable the data trickle function, the trickled data might contain a virus.

By changing the settings for the items in the following table, the performance of real-time virus scans can be improved. Consider the effect these settings will have on the scan server before changing them.

Table 3-10 Settings that can be used to improve the performance of real-time virus scans (when using Symantec Corporation software)

Item	Description	Result
Number of available threads for scanning	Specifies the number of threads used for virus scanning.	It might be possible to scan more files at the same time.
Threshold number of queued requests	Specifies the size of the waiting queues for virus scanning requests.	
Maximum RAM used for in-memory file system	Specifies the maximum size of memory used for virus scanning.	The time required for virus scanning might decrease.
Maximum file size stored within the in-memory file system	Specifies maximum size of files to be scanned when virus scanning is performed on memory.	

For details about the items in the table above and the recommended values, see the anti-virus software documentation.

When using Trend Micro ServerProtect

- Configuring the environment for the scan server

  If the scan server runs Windows Server 2008 R2, a memory leak might occur on the server. Download the fix KB2647452 from the Microsoft website and apply the fix. For details, refer to the following web page of the Microsoft website:

  http://support.microsoft.com/kb/2647452

- Configuring the virus scan software

  The virus scan software lets you configure real-time virus scanning or specify files that should not be scanned.

  Configure the settings for real-time virus scanning as follows:

  - The **Enable Real-time Scan** check box is selected.
  - The **Incoming & outgoing** radio button is selected.
  - The **Scan mapped network drive** check box is selected.

  To limit the files to be scanned, use the scan software to specify the files that you do not want to be scanned.

  For information about the other settings, see the appropriate scan software document from Trend Micro.

- Installing and setting up Hitachi Server Protect Agent

  The Hitachi Server Protect Agent is required for linking HDI systems and scan software together to perform real-time scanning.

  Hitachi Server Protect Agent supports the following OSs:

  - Microsoft(R) Windows Server(R) 2012 64-bit (without any SP)
  - Microsoft(R) Windows Server(R) 2012 R2 64-bit (without any SP)

- Microsoft(R) Windows Server(R) 2008 32-bit (with SP2)
- Microsoft(R) Windows Server(R) 2008 64-bit (with SP2)
- Microsoft(R) Windows Server(R) 2008 R2 64-bit (with SP1)

Note: Server Core environments are not supported.

Insert the installation media into the scan server, and then execute the `HspaInstaller.msi` file stored in the `HSPA` folder to begin installation of Hitachi Server Protect Agent.

If installation fails, perform the action described in the following table.

Table 3-11 Action to be performed if installation of Hitachi Server Protect Agent fails

Problem	Cause and action
The following message is displayed: "KAQV40001-E This OS is not supported."	Hitachi Server Protect Agent cannot be installed, because the OS of the scan server is not supported for the version of Hitachi Server Protect Agent to be installed. Check the version of Hitachi Server Protect to be installed and the OSs that are supported.
The Hitachi Server Protect Agent setup wizard displays the following message: "Select whether you want to repair or remove Hitachi Server Protect Agent."	The version of Hitachi Server Protect Agent you attempted to install is already installed. No action is required.
The Hitachi Server Protect Agent setup wizard displays the following message: "Unable to install because a newer version of this product is already installed."	A newer version of Hitachi Server Protect Agent is already installed. In the Windows Control Panel, go to **Programs and Features**, select **Hitachi Server Protect Agent**, and then check which version of Hitachi Server Protect Agent is installed.

After the installation finishes, start Hitachi Server Protect Agent Manager, and then set the following information. After setting the information, be sure to click **OK** to complete the setting.

Table 3-12 Information required for Hitachi Server Protect Agent setup

Information category	Item
Information for the nodes to be connected to a scan server (set this information in the **Basic** tab)[#1] (Up to 32 nodes)	Host name[#2]:
	IP address[#3]:
	CIFS administrator's user name[#4#5]:
	CIFS administrator's password:

Information category	Item
Settings used for linking to Anti-Virus Enabler (set this information in the **Advanced** tab) (optional)	Port number:
	Timeout value (0 to 900 seconds):
	Queue size (1 to 500):
	The number of queues (1 to 4):
	Log file size (1 to 10 MB):
	The number of log files (1 to 10):
	Trace log file size (1 to 10 MB):
	The number of trace logs (1 to 10):

#1:

If the node information is changed, also change the Hitachi Server Protect Agent Manager settings.

#2:

The host name is case sensitive, so make sure that the case is consistent with that in the host name of the node to be registered.

#3:

Use the specified IP address to access the HDI system. If multiple network interfaces are connected to the scan server, use the same network interface for both accepting real-time virus scan requests and accessing the HDI system.

#4:

If Active Directory authentication is used to authenticate CIFS users, add the NetBIOS name of the Active Directory domain to the user name, as shown below:

*NetBIOS-name-of-Active-Directory-domain**user-name*

You do not need to add the scan server to the Active Directory domain.

#5:

The specified CIFS administrator's user information is used for accessing CIFS shares and performing real-time scanning.

- Using DHCP with HDI

  If the IP address of an HDI network interface that is connected to the scan server is changed by DHCP, in Hitachi Server Protect Agent, you must specify FQDN as the IP address for nodes used to connect to the scan server. In this case, node names are resolved every time you perform real-time scanning, which lowers response performance. We recommend that you connect scan servers to HDI network interfaces that do not use DHCP.

  If the node IP address used to connect to the scan server is changed by DHCP, it might take a long time for the new IP address to take effect because the old IP address is cached on the scan server. We recommend that you assign static IP addresses to the nodes and the

scan server ports when you configure the DHCP server, and then specify the IP addresses from Hitachi Server Protect Agent.

- To change the **SMB protocol** settings by using the HDI GUI

  If real-time scanning by using Trend Micro ServerProtect is enabled, when you change the **SMB protocol** setting on the **CIFS Service Management** page (Setting Type: Basic), you need to restart the OS on the scanning server.

When using Trend Micro InterScan Web Security Virtual Appliance

- Deployment mode settings in the Deployment Wizard

  Select **ICAP mode**.

- ICAP settings in the Deployment Wizard

  Select the following check boxes:

  –**Enable X-Infection-Found ICAP header**

  –**Enable X-Virus-ID ICAP header**

- HTTP Scan Policy: Settings on the **Virus/Malware Scan Rule** tab of **Edit Global Policy**

  Clear the following check boxes under **Large File Handling**:

  –**Do not scan files larger than**

  –**Enable special handling**

- HTTP Scan Policy: Settings on the **Action** tab of **Edit Global Policy**

  Select the **Delete** action for **Infected files** under **File Type**.

- Setting for automatic URL blocking

  Disable the setting.

- If an access to a file is blocked due to the scan server setting

  The action same as that selected for **Method of dealing with infected file** in the **Scan Conditions** page on the **Virus Scan Server Configuration** dialog is taken. The operation result varies per client who accesses the blocked file depending on the selected action. For the operation result of file creation, referring, or update, see *Administrator's Guide*.

When using McAfee virus scan software

Install the add-ons for linking to the storage system. Then, change the settings according to the following:

- Setting a bind address

  Set the IP address specified for the scan server in the HDI system in order to connect to the HDI system.

- Setting a port number

  Set the same port number as the port number specified for the scan server in the HDI system.

- Scan item options

  Enable the internal scan of compressed files.

- What to do when a threat is detected

Set **Remove** as the first thing to do.

- What to do when a suspicious program is detected
  Set **Remove** as the first thing to do.

By changing the settings for the items in the following table, the performance of real-time virus scans can be improved. Consider the effect these settings will have on the scan server before changing them.

Table 3-13 Settings that can be used to improve the performance of real-time virus scans (when using McAfee anti-virus software)

Item	Description	Result
Maximum scan time(seconds)	Specifies a timeout value for virus scans.	Files are less likely to cause a timeout while they are being scanned.
Number of scan threads	Specifies the number of threads to be used for virus scans.	It might be possible to scan more files at the same time.

For details about the items in the table above and the recommended values, see the anti-virus software documentation.

Environment settings for a tape device connected to a node via a SAN

This subsection describes how to set up a tape device that is connected to a node via a SAN. A tape device connected to a node via a SAN can be used in cluster configurations.

Registering tape drive information

A tape device that is only physically connected to a node via a SAN is not usable. When a new tape device is installed, after the maintenance personnel and SAN administrator are done installing the tape device (for example, connecting it, and setting up the FC switch zones), the system administrator needs to register the tape drive information with the NDMP server.

If multiple nodes share tape drives, register the information for the shared tape drives on each NDMP server. If the nodes use separate tape drives, register the information for each tape drive on each NDMP server.

For details on how to register tape drive information on the NDMP server, see the *CLI Administrator's Guide*.

To check whether tape drive information is already registered, execute the `tapelist` command without any options specified.

Enabling the registration information of tape drives

If the registration information of tape drives is disabled after you have registered the tape drives, you cannot use the tape drives to execute backup and restore operations until you have re-enabled the registration information.

Tape drive information can be disabled if the system administrator manually disables it by specifying the `-i` option and running the `tapedel` command.

When the registration information of tape drives is disabled, re-enable the registration information before starting a backup or restore operation that uses the tape drives.

Unregistering tape drive information

When a tape device connected to a node via a SAN is no longer needed, remove the tape drive information registered in the backup management software, and then unregister the tape drive information from the NDMP server. For details on how to unregister tape drive information, see the *CLI Administrator's Guide*.

Notes on setting up a tape device connected to a node via a SAN

Note the following points when setting up a tape device that is connected to a node via a SAN:

- When you are using a tape device whose block size can be changed by the backup management software, if you change the block size after performing a backup operation, you might not be able to restore backup data stored on the tape device.
- Make sure that you use a tape drive registered on a node on which a backup or restore operation is to be performed. If you use a tape drive registered on another node, the data to be backed up or restored might travel over the LAN.
- When the system is operating in degenerate mode, an error might occur during a backup or restore operation, or you might have to change the settings to perform a backup or restore operation. For notes on operating the system in degenerate mode, see the *Troubleshooting Guide*.

Replacing of tape devices

This subsection explains how you can replace a tape device in cooperation with maintenance personnel or the SAN administrator. For details on the commands used in the procedure, see the *CLI Administrator's Guide*.

To replace a tape device:

1. Use the backup management software to unregister the tape device you want to replace.
2. Execute the `tapedel` command to delete the information about the tape drives registered on the NDMP servers on all nodes.

3. Working with the SAN administrator, remove the FC cable connected to the tape device that you want to stop using.
4. Working with maintenance personnel or the SAN administrator, replace the tape device.
5. Working with the SAN administrator, connect the FC cable to the new tape device.
6. Execute the `tapeadd` command to register the tape drive on the NDMP servers.
7. Use the backup management software to register the new tape device.

Stopping use of a tape device

This subsection explains how you can stop using a tape device in cooperation with maintenance personnel or the SAN administrator. For details on the commands used in the procedure, see the *CLI Administrator's Guide*.

To stop using a tape device:

1. Use the backup management software to unregister the tape device that you want to stop using.
2. Execute the `tapedel` command to delete the information about the tape drives registered on the NDMP servers on all nodes.
3. Working with the SAN administrator, remove the FC cable connected to the tape device that you want to stop using.
4. Remove the tape device.

SMTP server environment settings

To receive email notifications containing error information when errors occur in an HDI system or when users perform an invalid operation, an SMTP server is required for sending emails to preset addresses. This section describes the SMTP server environment settings.

If an SMTP server is already set up in a LAN containing HDI nodes, you can use that SMTP server. If no such SMTP server exists, you need to install an SMTP server in the LAN or connect the LAN to a network in which an SMTP server exists.

Client machines must support Unicode (UTF-8) to receive emails.

DHCP server environment settings

A DHCP server is required in a single-node configuration when DHCP is used to set the interface of a node. This section describes the DHCP server environment settings.

To automatically register node host names to the DNS server, enable the DDNS functionality on the DHCP server and DNS server. For details about the

environment settings on the DNS server, see DNS server environment settings on page 3-42.

The DHCP server manages the following settings that HDI uses:

- IP addresses and subnet masks
- Default gateway
- MTU (Specify 1,500 for this value.)
- DNS server
- The domain where the node belongs and the domain you want to be the search target for name resolution
- Routing information (static route)

We recommend that you manage the routing information from the DHCP server instead of setting the routing information in HDI.

When you manage the DNS server information from the DHCP server, the settings from the DHCP server will be used after you restart the OS on nodes even if you set the DNS server in HDI.

DNS server environment settings

A maximum of two DNS servers can be specified.

When two servers of the same type are specified, if a failure occurs on the server that is running, operation continues by automatically switching to the other server.

When using DHCP in a single-node configuration, you must configure the environment settings of the DNS server to automatically register node host names to the DNS server. Configure the settings as follows:

- Enable the DDNS functionality. Also change the security settings to permit dynamic updating of DNS records from the DHCP server.
- Enable scavenging of stale resource records so that unused records can be deleted.

Proxy server environment settings

You can use a proxy server that performs user authentication to relay communication between an HDI system and an HCP system. Note the following when using a proxy server:

- Basic authentication must be set for user authentication.
- We recommend that you use HTTPS for communication with an HCP system.

  If you use the `arcsslctl` command to set HTTP instead of HTTPS, the HDI system uses the `CONNECT` method to request tunneling to the proxy server. In this case, it might be necessary to change the settings of the proxy server if it fails to relay the communication.

The following is an example of changing the `squid.conf` settings on a `squid` proxy server (version 3.1.10):

- Add "`acl SSL_ports port 80`" as follows to allow the `CONNECT` method with the HTTP protocol.

```
acl SSL_ports port 443
acl SSL_ports port 80
# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
```

- Add the following line to allow an HTTP request that does not include `Content-Length`.

```
request_header_access Content-Length allow all
```

- Add the following line to ignore an HTTP request that includes `100-Continue`.

```
ignore_expect_100 on
```

4

About HDI

This chapter describes various points that system administrators must understand and take into consideration before using an HDI system.

For details about backup operations in an HDI system, see Chapter 5, Backup Operations in an HDI System on page 5-1.

If the HDI system operation links with HCP, see Chapter 6, Linking HDI and HCP on page 6-1 before starting this chapter.

Note:

Make sure you refer to Notes on managing an HDI system (required reading) on page 4-3.

- ☐ Notes on managing an HDI system (required reading)
- ☐ About cluster configurations
- ☐ Before starting communication between HDI system and external devices
- ☐ About client user information
- ☐ About HDI with user mapping
- ☐ About file systems
- ☐ About setting quotas
- ☐ About file sharing
- ☐ About real-time virus scanning
- ☐ About system settings

- About errors
- About monitoring systems with SNMP
- About importing data from other file servers
- About clients using file systems

Notes on managing an HDI system (required reading)

The system administrator needs to keep the following in mind when managing an HDI system:

- If you change the configuration of an HDI system, you need to download the system settings file saved on the system LUs, and then save it on storage media outside the system.
- Do not run commands while operations are being performed on the HDI system by way of the GUI.
- Multiple system administrators cannot simultaneously specify or update system settings within a cluster. For this reason, if multiple system administrators are registered, ensure that only one system administrator has the ability to register or modify information.
- If you specify a host name for the management IP address of the node or the IP address of the management port of the storage system controller, in advance, you need to specify settings for the management server so that names can be resolved.
- When changing any DNS server settings after starting an HDI system, you must restart the OS on both nodes in the cluster after the changes are made.
- If NFS shares are being used, do not make any changes to an environment in which host names can be resolved after the HDI system has been started. An environment in which host names can be resolved is an environment in which the IP address and host name of an NFS client are registered in the `/etc/hosts` file of the OS on the node, NIS server, or DNS server so that the host name can be converted into an IP address. If any changes are made to an environment in which host names can be resolved after an NFS share is created, attempting to access a file system from an NFS client might cause an error to occur.
- If you stop the NFS service, contact the administrators of the NFS client hosts and ask them not to access the NFS share until the NFS service starts.
- If you register a client host name on a DNS server and then use an HDI system, check the NFS client host's name resolution beforehand. Confirm that the name resolution (both forward lookup and reverse lookup) responds normally within a short time. For details on how to check the result of DNS name resolution, see the *Troubleshooting Guide*. If the DNS server does not respond normally and within a short amount of time, check the DNS server settings.

  If you start an HDI system without registering an NFS client host on the DNS server confirm beforehand that the NFS client host's name resolution sends a error response within a short time. If the DNS server does not respond with an error within a short amount of time, ensure that the processing of queries to the DNS server does not take a long time. You can do this by configuring the system so that the DNS server does not request another DNS server's name for name resolution. One configuration option is defining a reverse lookup zone on the DNS server.

If the DNS server does not send an error response within a short period of time, make sure the processing of queries sent to the DNS server will not take a long time, for example, by defining a reverse lookup zone on the DNS server so that the DNS server does not send a name resolution request to another DNS server.

When the processing of queries sent to the DNS server is taking a long time, if you use an HDI system, the following processes might fail: the creation and deletion of an NFS share, changing the attribute of an NFS share, failover, and failback.

- If you want to register a client host name on the DNS server and then use an HDI system, first make sure the name resolution processing (both forward lookup and reverse lookup) of the management console host responds normally within a short period of time.

  For details on how to check the result of DNS name resolution, see the *Troubleshooting Guide*. If the DNS server does not respond normally and within a short amount of time, check the DNS server settings. If you want to use an HDI system without registering a client host on the DNS server, first make sure the name resolution processing (both forward lookup and reverse lookup) of the management console host sends an error response within a short period of time.

  If the DNS server does not send an error response within a short period of time, make sure the processing of queries sent to the DNS server will not take a long time, for example, by defining a reverse lookup zone on the DNS server so that the DNS server does not send a name resolution request to another DNS server. Alternatively, make sure the name resolution request is not sent to the DNS server by adding the host name and IP address of the management console to the `/etc/hosts` file of the HDI system.
- Be sure to check the following if you are using the CIFS service and performing DNS name resolution for a domain controller or LDAP server for user mapping:
  - Whether the DNS server can perform name resolution for the domain controller or LDAP server (forward lookup)
  - Whether the DNS server quickly responds when performing name resolution for the domain controller or LDAP server (both forward lookup and reverse lookup)

  For details on how to check the result of DNS name resolution, see the *Troubleshooting Guide*. If the DNS server does not send a normal response, check and if necessary, revise the settings for the DNS server such as the record settings, zone settings, and recursion settings.
- In an environment where host names can be resolved, note the following to register or delete a host name:
  - When creating an NFS share for a given host, make sure that a host name for the host is registered.
  - When specifying a netgroup for creating an NFS share, always use the same type of name resolution (conversion from an IP address to a host name, and vice versa) for the host name of the NFS client from which a target file system is mounted.

    - When deleting a host name used in an NFS share for a given host, delete the corresponding NFS share, and then delete the host name.
    - When using an NFS share for file locking, if an NFS client that has a file lock terminates abnormally and cannot be restarted, you must delete the file lock information. For details on how to delete file lock information, see the *CLI Administrator's Guide*.
- The password specified by a system administrator when user information is registered should be used only temporarily. For any users added from the **Add User** page or the **Batch Operation** page of the **Local Users** dialog box, the system administrator must inform the users that they need to change their own passwords.
- If you are using Active Directory, users that have Active Directory authentication can access the CIFS shares. Users that are locally authorized in the HDI system cannot access the CIFS shares.
- If the system goes down, or an error causes the OSs of both nodes within a cluster to stop, and you restart only one node to resume operation, check whether the KAQG72011-E message was output on the **List of RAS Information** page (for `List of messages`) of the **Check for Errors** dialog box. If the relevant settings are enabled, the information can be also sent by using an SNMP trap or email. If the KAQG72011-E message was output, wait until the OS on the node (for which the message was output) is stopped, and then start the OS on the other node.
- If a failover occurs, services associated with the resource group, for which the failover occurred, cannot be started, stopped, or restarted.
- On the **Browse Cluster Status** page (for `Resource group status`) of the **Cluster Management** dialog box, if `Online / No error` is displayed for **Resource group status**, the file systems, NFS services, CIFS services, and virtual IP addresses can be managed from File Services Manager. Because the resource groups start up only after the cluster is running normally, the statuses of the resource groups are displayed as `Online Pending` immediately after the status of the cluster is displayed as `ACTIVE` for **Cluster status** on the **Browse Cluster Status** page (for `Cluster / Node status`). In this situation, file systems, NFS services, CIFS services, or virtual IP addresses cannot be used. Before using a file system, an NFS service, a CIFS service, or a virtual IP address, confirm that the resource group status is `Online / No error`.
- When a resource group is started, the HDI system will block any resources in which an error is detected. The HDI system will use other resources to configure the resource group. When a resource group is *partially blocked*, some services in the node will be stopped but the remaining services will still be provided. If this happens, the **Browse Cluster Status** page (for `Resource group status`) of the **Cluster Management** dialog box displays `Online / No error`, and you will not be able to check the error information about the resource group.

  A partial blockage of a resource group might occur at the following times:

    - When operation of the HDI system starts
    - When a failover or failback occurs

- When a resource group is restarted

  If any of the operations previously listed are performed, or `Online / No error` is displayed on the **Browse Cluster Status** page (for `Resource group status`) (even though you cannot access the file system), from the **List of RAS Information** page (for `List of messages`) of the **Check for Errors** dialog box, you will need to check the system messages to see whether a partial blockage occurred in one of the resource groups.

  The system administrator checks whether the KAQG72006-E or KAQM35018-E error message has been output as a system message.

  Note that, depending on the resource type, resources that use a blocked resource might also become blocked. For example, if a logical volume is blocked, the file system created in that logical volume is also blocked. The system administrator checks whether the KAQG72006-E or KAQM35018-E error message has been output for each blocked resource.

- 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.

About cluster configurations

Information about NFS share settings, CIFS share settings, the virtual IP address, and the file system mounted on a node is managed together as a *resource group* on the nodes that make up a cluster. In normal operation, a single resource group runs on a single node. The following figure illustrates a cluster configuration in an HDI system.

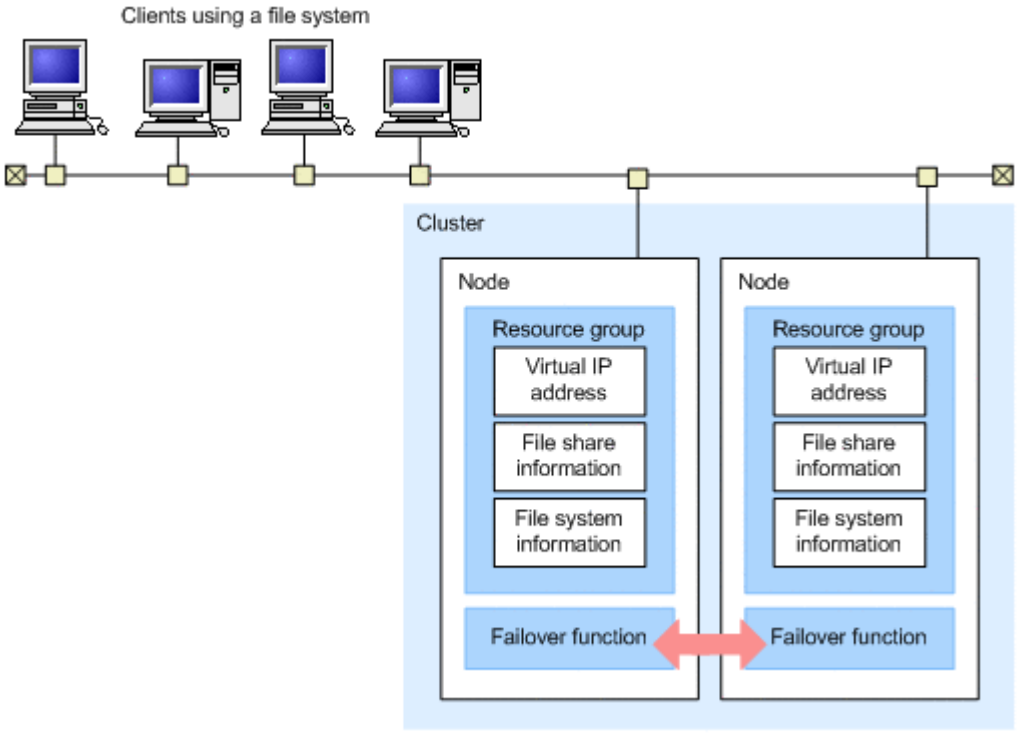


Figure 4-1 Cluster configuration in an HDI system

If an error requiring failover occurs, the error information is reported to the failover functionality, and failover starts automatically. A system administrator can use File Services Manager to verify that a failover has occurred.

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

The following figure shows the general process for client services after failover.

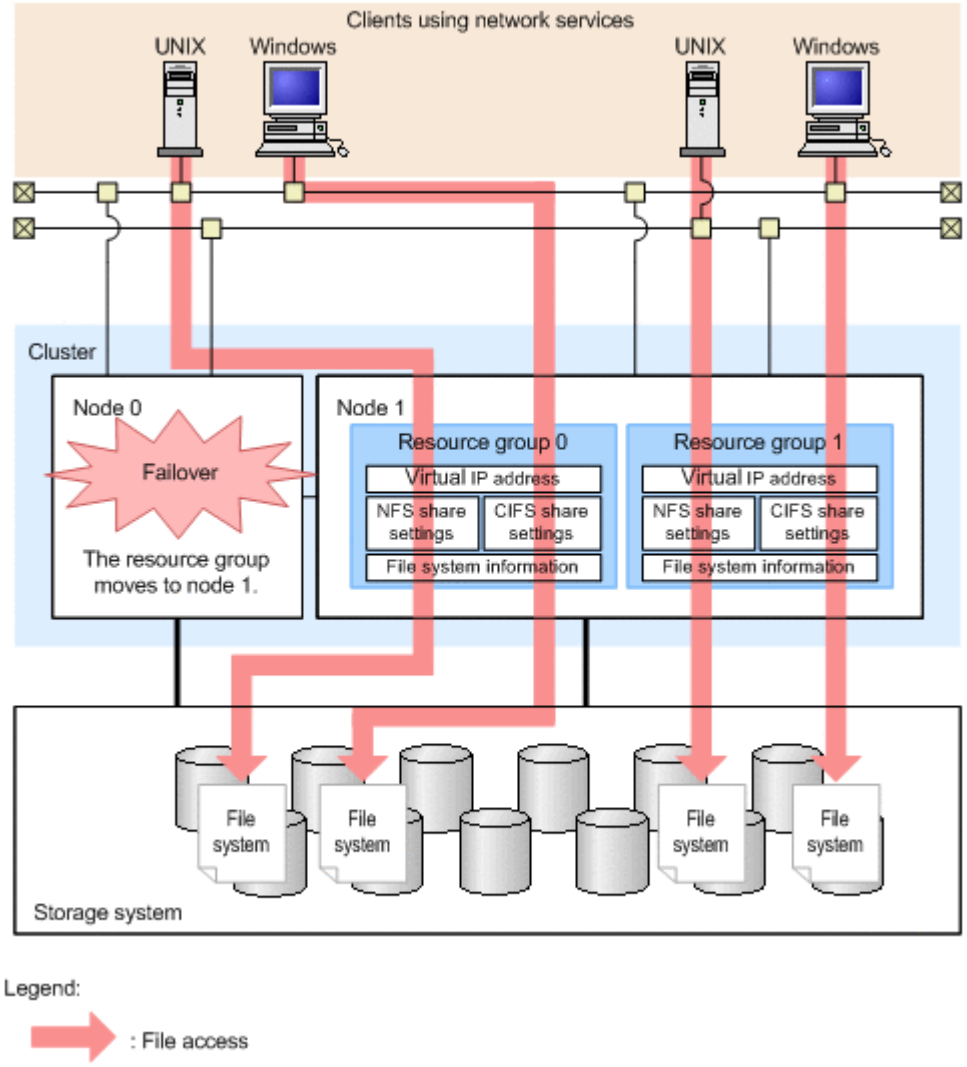


Figure 4-2 Example of the general process for client services (during a failover)

An IP address that clients use to connect to a resource group service is called a *virtual IP address*. When the node on which a resource group is running changes to the other node, the virtual IP address is passed to the other node. Because clients use the virtual IP address to connect to the service, clients can access files even after a failover occurs. Virtual IP addresses are associated with interfaces on a node. When a resource group is moved to another node in the same cluster, the virtual IP address is associated with the same interface on the destination node. For example, the virtual IP address previously associated with the fixed IP address of `eth1` in the original node will be associated with the fixed IP address of the interface `eth1` in the destination node.

In an HDI system, services are provided by mounting a different file system for each resource group. By planning the network configuration, and the mounting of file systems, a system administrator can distribute file access across both nodes and balance the loads between the nodes.

Normal operation restarts when a failed-over resource group is failed back to the original node after an error recovery operation. A system administrator fails back a resource group by changing the node on which the resource group is running. As a system administrator, if you need to carry out failback, you should follow the instructions of the maintenance personnel.

Before starting communication between HDI system and external devices

HDI system can communicate with external devices by using the TLS protocol.

You can check or change the TLS settings to be used for communication between HDI system and external devices by using the tlsctl command. By default, TLS 1.0, TLS 1.1, and TLS 1.2 are all enabled. For details about the tlsctl command, see the *CLI Administrator's Guide*.

Before starting communication between HDI system and external devices, check the following:

- 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.
- If you change the settings by using the `tlsctl` 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.

About client user information

In an HDI system, clients are identified by user IDs and group IDs. The system administrator can use the following methods to manage client user information. The maximum number of user information items that can be managed by each method is the number of user information items per cluster (or node in a single-node configuration).

Using an HDI system to manage user information:

Using this method, a maximum of 2,000 items of user information registered in an HDI system can be managed.

Using an NIS server or an LDAP server (or both) to manage user information:

Using this method, a maximum of 50,000 items of user information registered in an HDI system, an NIS server, or an LDAP server can be managed. Server information must be set in advance in an HDI system to enable management by using an NIS server or LDAP server. Note that the NIS server can be used for managing user information only when IPv4 is used.

Using Active Directory or the NT domain to manage user information:

To assign user IDs and group IDs to user information used for user authentication, user mapping is required, or else user information (user

IDs and group IDs) must be managed by an HDI system, an NIS server, or an LDAP server.

The maximum number of user information items that can be managed by the domain depends on the OS of the domain controller. In all domains to be used (including domains in trust relationships), the maximum number of users and groups for which user mapping can be used is 300,000. Assign user IDs and group IDs from the appropriate range based on the user mapping method. For information on the range of user IDs and group IDs that can be assigned by using each user mapping method, see the *Administrator's Guide*.

Note that the NT domain can be used for managing user information only when IPv4 is used.

About HDI with user mapping

The types of IDs that an HDI system or Windows uses to identify users differ. HDI systems use user IDs and group IDs, while Windows uses unique IDs called security identifiers (*SIDs*).

For an HDI system, if CIFS clients accessing file systems will be authenticated by way of Active Directory authentication or NT domain authentication, you can use *user mapping* to assign user IDs or group IDs.

User mapping also allows you to manage users who belong to 32 or more groups.

This section explains how user mapping is managed in an HDI system and describes the settings necessary to use user mapping.

Domains that allow access to an HDI system

When user mapping is used, users who belong to a domain that is in a trust relationship with the domain that the nodes belong to can also access the CIFS shares in an HDI system.

To access an HDI system, users must belong to a domain that is in a mutually trusting relationship with the domain that the nodes belong to.

In order to establish a trusting relationship between forests, their root domains must have a mutually trusting relationship.

Users cannot access CIFS shares if the users belong to a domain for which the forest is in a unilaterally trusting relationship with the forest containing the domain that the nodes belong to.

The figures below show the scopes of the domains from which users can use HDI CIFS shares.

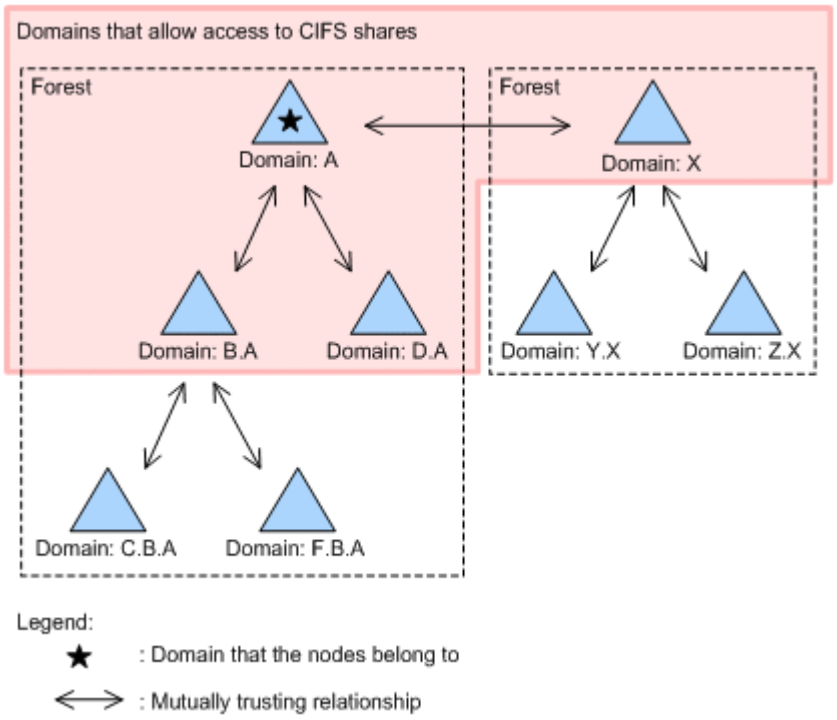


Figure 4-3 Node belonging to the root domain

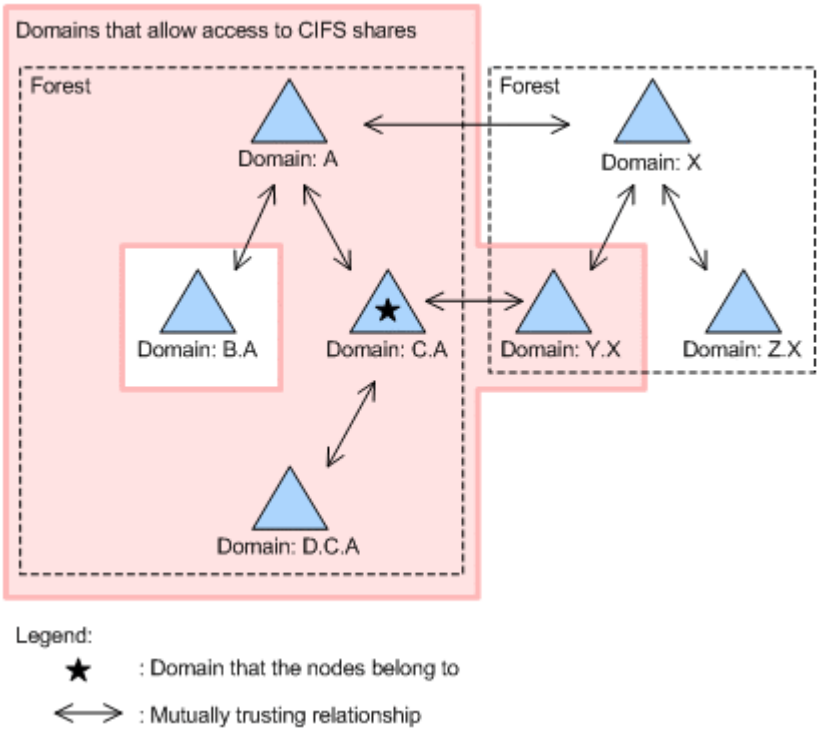


Figure 4-4 Node belonging to a child domain, when there is a mutually trusting relationship between the forests

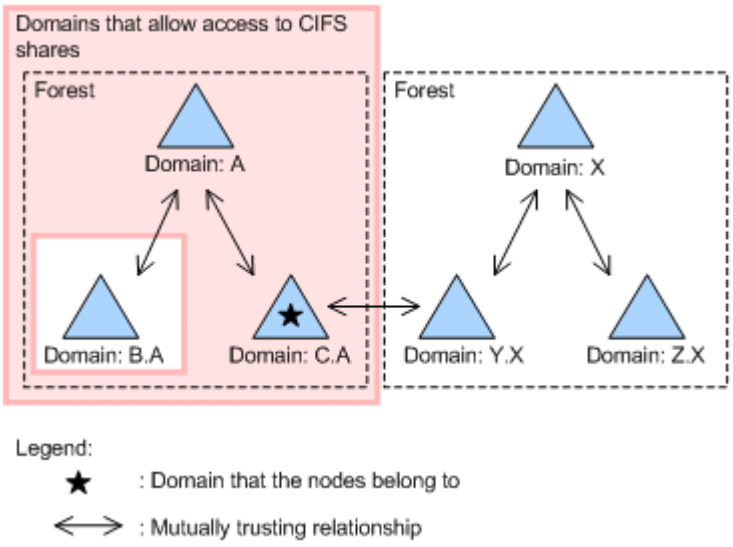


Figure 4-5 Node belonging to a child domain, when there is no mutually trusting relationship between the forests

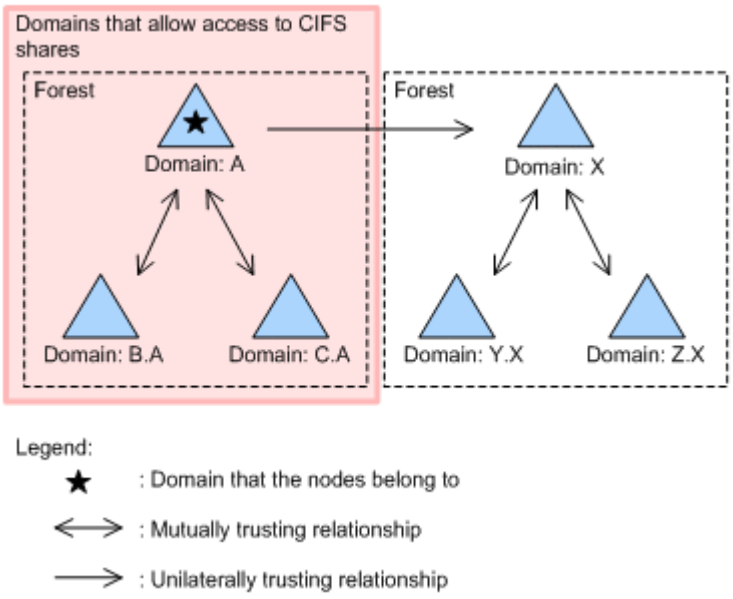


Figure 4-6 Only a unilaterally trusting relationship between the forests

To access an HDI system when the nodes belong to an Active Directory domain, users who belong to a domain that is not in a parent-child relationship with the domain that the nodes belong to must explicitly set up a trust relationship with that domain.

User mapping methods

The following describes the user mapping methods provided by HDI systems:

- User mapping using RIDs (automatic assignment)
- User mapping using LDAP (automatic or manual assignment)

- User mapping using Active Directory schema (manual assignment)

We recommend that you use RIDs, because they are less susceptible to communication errors in the HDI system.

User mapping using RIDs

User mapping using RIDs authenticates CIFS clients via Active Directory authentication or NT domain authentication.

When a CIFS client accesses an HDI file system, the system converts the set of relative identifiers (*RIDs*) contained in the SID and automatically assigns a user ID or group ID to the client.

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

You can manage a maximum of 256 domains when user mapping using RIDs is used. If you have 257 or more domains, choose user mapping using LDAP or an Active Directory schema.

User mapping using LDAP

User mapping using LDAP authenticates the CIFS client via Active Directory authentication or NT domain authentication.

You can choose to automatically or manually assign user IDs and group IDs.

If you choose automatic assignment, user IDs or group IDs within the range specified in File Services Manager will be assigned automatically when the CIFS client accesses an HDI file system. Information about the assigned user ID or group ID is registered in the database of the LDAP server set up as an external server. When the CIFS client next accesses the file system, the user ID or group ID that was already assigned is used.

If you choose to manually assign user IDs and group IDs, they will be assigned according to the user information that was registered beforehand in the LDAP server database.

User mapping using the Active Directory schema

User mapping using the Active Directory schema authenticates the CIFS client via Active Directory authentication.

User mapping using the Active Directory schema allows you to combine the different IDs a user has from NFS and CIFS clients and treat them as the same user by using the Active Directory user attributes. Furthermore, you do not need to prepare an external server for user mapping, because user IDs and group IDs will be assigned according to the user information that was registered in the domain controller beforehand.

Changing the user mapping method

Each user mapping method has its own unique way of assigning user IDs and group IDs. The IDs assigned to CIFS clients differ depending on the user mapping method that is used.

If you change the user mapping method after starting the operation of the HDI system, the user IDs and group IDs assigned to CIFS clients will be changed. This might allow unauthorized users to access files and folders that were created before you changed the user mapping method. In order to change the user IDs and group IDs associated with files and folders to the IDs used by the new user mapping method, the CIFS administrator has to migrate the file system by using the Windows backup function. For other OSs, see the documentation provided with the OSs.

The following procedure is for migrating file systems when the user mapping method is changed from the LDAP method (that automatically assigns user IDs and group IDs) to the RID method:

1. Contact the end users.

   Ask the end users to not access the CIFS shares while this procedure is being performed.
2. Limit access from the CIFS client hosts.

   From **Host access restrictions** on the **CIFS Service Management** page (**Setting Type**: `Security`) of the **Access Protocol Configuration** dialog box, limit access to only the CIFS client host on which the administrator will migrate the file systems.
3. Set up a CIFS administrator.

   From **CIFS administrator name(s)** on the **CIFS Service Management** page (**Setting Type**: `Administration`) of the **Access Protocol Configuration** dialog box, specify the CIFS administrator that you want to have migrate the file systems.
4. Restart the CIFS service.

   From the **List of Services** page of the **Access Protocol Configuration** dialog box, restart the CIFS service.
5. Ask the CIFS administrator to back up the data in the source CIFS shares.

   We recommend that the CIFS administrator use the Windows backup function. If the data is backed up using another method, the ACLs and file attributes might not be restored correctly. Note that data created by NFS clients cannot be migrated by using the Windows backup function.
6. Change the user mapping method.

   From the **CIFS Service Management** page (**Setting Type**: `User mapping`) of the **Access Protocol Configuration** dialog box, specify the required information in **User mapping setup**.
7. Restart the CIFS service.

   From the **List of Services** page of the **Access Protocol Configuration** dialog box, restart the CIFS service.
8. Create and mount a file system.

From the **Create File System** dialog box, create and mount a file system. Create the file system so that the capacity is the same size as the source file system capacity or larger. All other settings should be identical to those on the source file system.

9. Specify quotas for the target file system.

   If a default, user, or group quota was specified on the source file system, use the same quota value for the target file system.

   To specify a default, user, or group quota, use the `quotaset` command. If you do not want to set a limit on the block and inode usage for a particular user or group, specify `0` for the soft and hard limits.

10. Create CIFS shares on the target file system.

    From the **Add Share** dialog box, create CIFS shares on the target file system, and then specify names for the CIFS shares that differ from the source CIFS share names. For the target CIFS shares, use the same settings as those for the source CIFS shares.

11. Specify a subtree quota.

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

    Use the `stquotaset` command to specify a subtree quota. If you do not want to set a limit on the block and inode usage for a particular user or group, specify `0` for the soft and hard limits.

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

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

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

    Compare the data in the source CIFS shares with the data in the target CIFS shares, and make sure that the data was successfully migrated. When comparing the source CIFS shares with the target CIFS shares, we recommend that you check the following:

    - The structures of the folders are the same.
    - The contents of the files are the same.
    - The information about the owners, ACLs, and file attributes are the same.

14. Release the source CIFS shares, if necessary.

    If you want to change the target CIFS share names to the source CIFS share names, click the **Release Share** button in the following window or on one of the following tabs to release the source CIFS shares:

    Cluster configuration:

    - **Shares** subwindow
    - **Shares** tab in the *physical-node* subwindow
    - **Shares** tab in the *file-system* subwindow

    Single-node configuration:

    - **Shares** window
    - **Shares** tab in the *file-system-name* window

15. Delete the source file system, if necessary.

    You can delete the source file system, if it is no longer needed. Click the **Delete File System** button in the following window or tab to delete the source file system:

    Cluster configuration:

    - **File Systems** subwindow
    - **File Systems** tab in the *physical-node* subwindow

    Single-node configuration: **File Systems** tab in the **File Systems** window

16. Change the target CIFS share names, if necessary.

    If the source CIFS shares were released in step 14, from the **Edit Share** dialog box, you can rename the target CIFS share names to the deleted source CIFS share names.

17. Delete the CIFS administrator that was created, if necessary.

    If the CIFS administrator created in step 3 is not necessary, delete the CIFS administrator from **CIFS administrator name(s)** on the **CIFS Service Management** page (**Setting Type**: `Administration`) of the **Access Protocol Configuration** dialog box.

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

    From **Host access restrictions** on the **CIFS Service Management** page (**Setting Type**: `Security`) of the **Access Protocol Configuration** dialog box, remove the access limit to the CIFS client hosts that was set up in step 2.

19. Restart the CIFS service.

    From the **List of Services** page of the **Access Protocol Configuration** dialog box, restart the CIFS service.

Note:

After changing the user mapping method, delete the source CIFS shares. Because some of the user mapping information will still exist in the cache memory, an error could occur if you try to view a Properties window for any of the files and folders that were on the source file system. Use the **CIFS Service Maintenance** page of the **Access Protocol Configuration** dialog box to delete the user mapping information cached in the CIFS service environment.

Examples of assigning user IDs and group IDs with user mapping using RIDs

An RID is assigned to each user, group, and computer account, regardless of the type of object it is. As a result, there will be some IDs that are assigned by using RIDs but not actually used for file access. When thinking about what range to use for the user IDs and group IDs that will be assigned, remember that the range should also include IDs that will not be used for the purposes of file access.

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

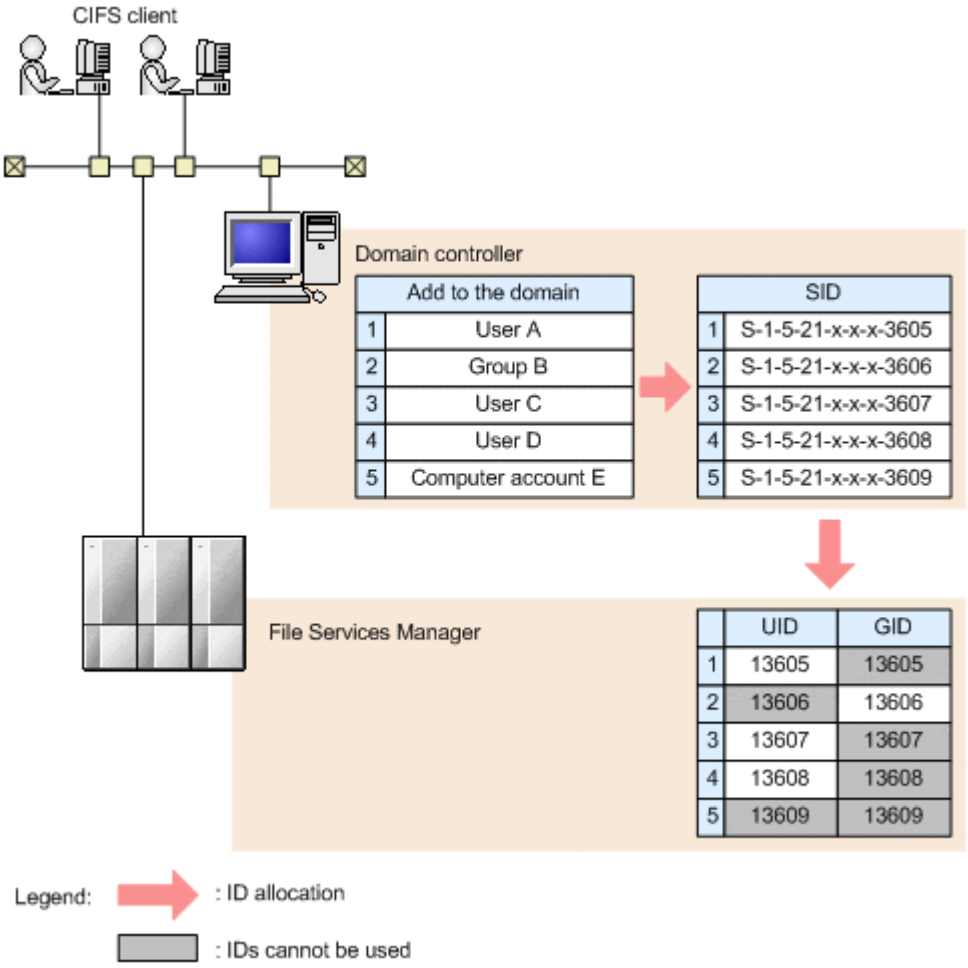


Figure 4-7 Example of assigning user IDs and group IDs by using RIDs

After a range of user IDs and group IDs has been set, you cannot change the minimum value of the range set for the user IDs and group IDs that are available for user mapping. When thinking about what range you want to set for the user IDs and group IDs, be sure to overestimate the necessary range, taking into account all future operational plans and the range of user IDs and group IDs that will be needed for other domains or external servers. When changing the range, if the amount of space necessary for allocating the IDs you want to add is insufficient, you will need to recreate the file system.

When setting the range of IDs available for user mapping, you must also take into consideration future increases in the number of SIDs. At the very least, the range of IDs you decide upon must contain the range of RIDs that are already in use. To ensure that you set an appropriate range of IDs available for user mapping, determine what that range is from the largest RID in use.

A system administrator can use various applications for such a task, such as one provided by Microsoft, to acquire the SID of the object that was last added to the domain controller. This SID will indicate to the system administrator what the largest RID currently in use is. If there are multiple domain controllers in the same domain, the system administrator can check the largest RID by acquiring the SID of the last added object for each domain

controller. For details on how to acquire an SID, see the documentation for the application you are using to acquire the SIDs.

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

- There are two domains (`Domain1` and `Domain2`).
- The domains have a direct trust relationship with each other.
- The largest RID that is currently in use is 8000.
- 1,000 users will be added to each domain annually. (However, from the second year on, 1,000 users will be deleted annually.)
- 1,000 computer accounts will be added to each domain annually. (However, from the second year on, 1,000 computer accounts will be deleted annually.)
- Groups and other objects will not be added or deleted.
- The domains will be in use for 100 years.
- A 50% margin will be added to the range of user IDs and group IDs to be used in order to account for the uncertainty of the rate in which objects will increase.

Number of SIDs per domain that are being used when you estimate a range:

```
Number-of-SIDs = (largest-RID-currently-in-use)
=8,000
```

Annual increase in SIDs per domain after the first year:

```
Number-of-SIDs = (number-of-users-added) + (number-of-computer-
accounts-added)
1,000 + 1,000 = 2,000
```

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

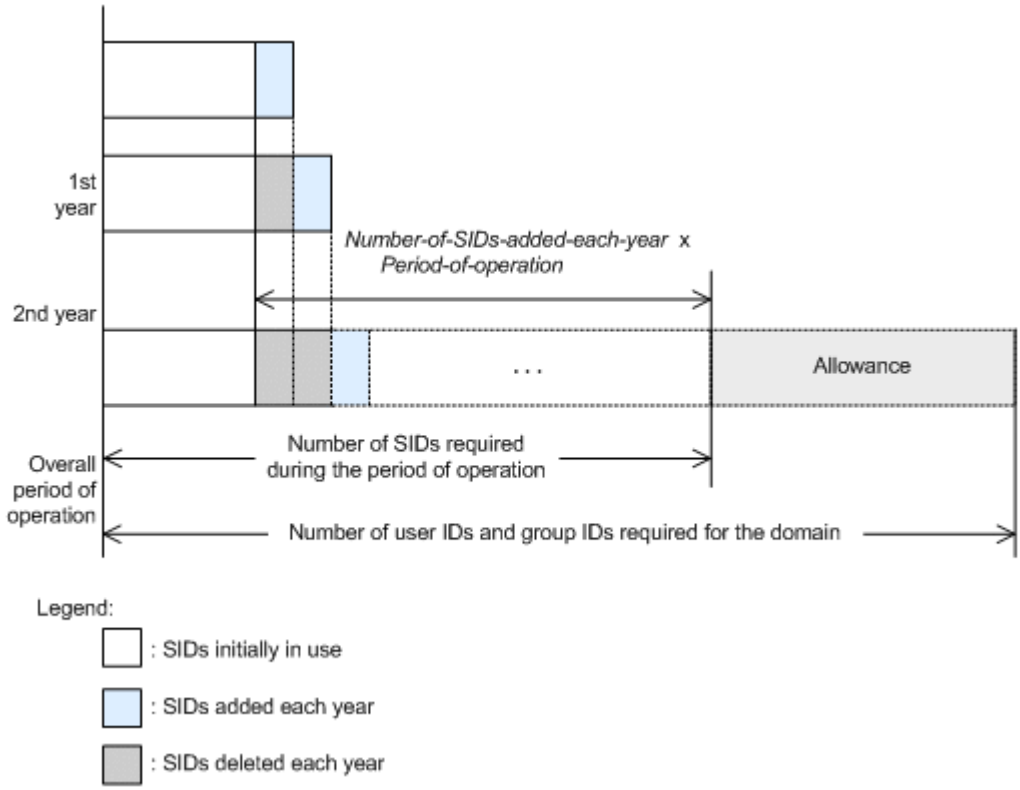


Figure 4-8 Example of how to estimate the total number of user IDs and group IDs required

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

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

```
Number-of-IDs-required-per-domain = (number-of-SIDs-currently-in-
use + (increase-in-the-number-of-SIDs-per-year x number-of-years-
operations-will-continue)) x (100 (%) + margin (%))
(8,000 + (2,000 x 100)) x 1.5 = 312,000
```

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

```
Number-of-IDs-required-for-entire-domains = number-of-IDs-
required-for-domain-1 + number-of-IDs-required-for-domain-2 + ...
312,000 + 312,000 = 624,000
```

For the above example, specify a range of user IDs and group IDs from 70000 to 2147483147. The following examples show what range of user IDs and group IDs to use for the above estimate when the minimum value of user IDs and group IDs is 1000000.

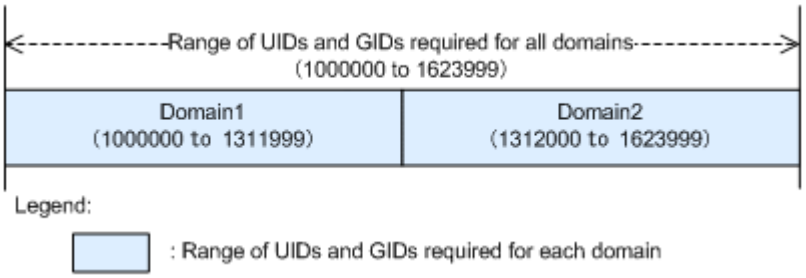


Figure 4-9 Example of what range to use for user IDs and group IDs

Range of user IDs and group IDs required for all of the domains:
1000000 to 1623999

Range of user IDs and group IDs required for `Domain1`:
1000000 to 1311999

Range of user IDs and group IDs required for `Domain2`:
1312000 to 1623999

About file systems

In an HDI system, the size of a file system is a maximum of 1 PB. Using the volume manager functionality (LVM) of File Services Manager, a file system can be put together from a single LU or multiple LUs. An LU (logical unit) is a logic partition on a disk. If File Services Manager is linked with Dynamic Provisioning, you can also allocate a virtual LU. In an environment in which multiple storage systems are connected to one node, a file system cannot be created from LUs in different storage systems.

In a cluster configuration, you can allocate an LU as a user LU (or device file) to be used in a file system.

In a single-node configuration, you can use volume groups. A volume group is the unit used to manage LUs in an internal hard disk drive or storage system. You can allocate multiple LUs to a volume group. You can use a volume group in multiple file systems.

Note the following when creating a file system:

- If you continue to use a file system while its usage is close to 100%, the problems below might occur. Therefore, we recommend that you use a file system so that its usage does not exceed 95%.
  - The file system access performance might degrade or an attempt to create a file might fail.
  - An error might occur when data is recalled from the HCP system or when data is imported from other file servers.
  - Migration tasks will not execute properly.

  You can use the `fsfullmsg` command to enable warning notifications to be sent when the usage of the file system exceeds a certain threshold.

- For the total number of directories and files that can be created in a directory, we recommend specifying a number that does not exceed 10,000.
- A maximum of approximately four billion files can be created in one file system.

  Note that the actual maximum number of files to be created in a file system differs depending on conditions such as the lengths of file paths and the number of files to be created in a directory. If you want to create more files than the maximum number described above, use an additional file system. To prevent the number of files from exceeding the maximum, you can use the `fsfullmsg` command to monitor the amount of inodes used. In addition, an SNMP trap or email (KAQG90003-W) can be sent when the warning threshold is exceeded. In addition, you can use the `fslist` command to periodically check the number of used inodes (`I-node used`) and number of remaining inodes (`I-node free`).
- A management area of at least 4 KB is required for each file. The required management area size differs depending on the settings for ACL, linking with an HCP system, etc. Take this into account when estimating the file system size or when setting quotas.
- Because 64-bit inodes are not supported by default, inode information is stored in an area that occupies the first 1 TB of the file system. File data is also stored in this inode area. Note that file expansion attributes are also stored in the inode area if the file system was configured by using an HDI version earlier than 4.2.3-03.
- On file systems that do not support 64-bit inodes and where the capacity of the inode area exceeds 1 TB, files or directories might not be created due to a lack of space in the inode area even if there is enough capacity for the file data. This issue can be addressed as follows:

  - When the number of files exceeds 100 million

  Use the `fsinodectl` command to enable support for 64-bit inodes. After you modify the settings, this change cannot be reversed. For notes about operating a file system that supports 64-bit inodes, see Notes when supporting 64-bit inodes on page 4-26.

  - When the number of files does not exceed 100 million

  Use the `fslist` command to periodically check the amount of inode usage, or use the `fsfullmsg` command to configure a warning to be displayed when the amount of inode usage exceeds 50%. After inode usage exceeding 50% is detected, use the `fslist` command to check whether there is any other data besides inode information stored in the inode area. Note that when `Block free` (the remaining capacity of the block) is less than 1 TB, or, when `Block free` (the remaining capacity of the block) is 1 TB or more and `I-node free` (the number of inodes remaining) is less than 100 million, other data besides inode information is stored in the inode area.

  If you expect the number of files to increase in the future, be sure to take action before the capacity of the inode area becomes inadequate to prevent a situation whereby files or directories cannot be created in a file system that does not support 64-bit inodes. For actions to be taken when

files or directories cannot be created in a file system that does not support 64-bit inodes, see the *Troubleshooting Guide*.

- In an HDI system, one block (whose size is 4 KB) is assigned for each file.
- In a file system set up on an HDI system, you can also save the file creation time, as well as the last access time (`atime`), the last change time (`ctime`), and the last modification time (`mtime`), to improve compatibility with the CIFS client environment. However, you cannot view the file creation time from an NFS client.
- For a file system set to link with an HCP system, 5% of the total capacity of the file system (maximum 40 GB) is assigned as an area (reserved space) for the system to execute certain processes, such as migration and stub processing. Take this into account when considering the file system capacity.

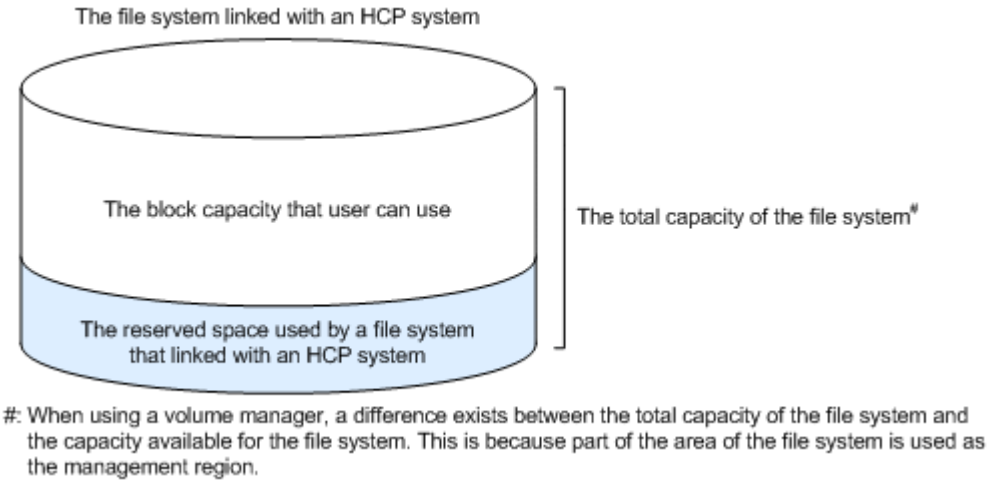


Figure 4-10 Capacity of a file system linked with an HCP system

Note that the reserved space setting can be changed by using the `arcresvset` command.

Note: If the total number of directories and files exceeds 10 million, estimate the required reserved space based on the formula below and use the `arcresvset` command to change the reserved space (unit: GB).

Formula used as a rough guide for the reserved space (unit: GB)

Total-number-of-directories-and-files-to-be-created-in-the-file-system `x 4 / ( 1,024 x 1,024 )`

In addition, the following explains what you need to know in order to manage file systems.

Creating an LU (device file) or volume group

There are two types of LUs that are used in the HDI system: a user LU used for the file system, and a cluster management LU where settings such as those related to a cluster configuration and file system are stored.

The system administrator creates LUs by using Device Manager or Hitachi Storage Navigator Modular 2 when configuring a file system in a storage

system. By using Device Manager or Hitachi Storage Navigator Modular 2, LUs can be created while considering factors, such as disk drive configuration, parity groups, and I/O performance. For details about creating LUs, see the manual for Device Manager or Hitachi Storage Navigator Modular 2. If you are not the storage system administrator, ask the person who is the storage system administrator to create the LUs for you.

If the system is a cluster configuration, make sure to create the LUs for the cluster management LU in the storage system as well. The cluster management LU requires 70 GB of capacity. If LUs in the external storage system are used as cluster management LUs, errors due to operation mistakes are more likely to occur on HDI compared to when LUs are used in the local storage system. For example, the OS on a node might be started while the external storage system has not yet started, or the cable connecting the local storage system and the external storage system might become disconnected.

Including the LUs that are automatically created during file system creation or expansion, a maximum of 1,024 LUs having a hexadecimal LUN in the range from 0000 to 03FF can be created in a cluster configuration. In a single-node configuration, a maximum of 256 LUs having a hexadecimal LUN in the range from 00 to FF can be created.

Specify the LUN (host LU number) for a storage system as a number from 0 to 1,026.

Note: In an HDI system that is version 6.3.1-00 or later, you can specify a value of 512 or more for a LUN (host LU number) that is set by the storage system. If you incorrectly specify a value greater than 512 for a LUN of an HDI system that is a version earlier than 6.3.1-00, an unexpected LU might become available for use when you perform an update installation of software for a node. Check the storage system settings before performing an update installation.

In a single-node configuration in which the internal hard disk of the node is used for a file system, the HDI system automatically allocates LUs to the internal hard disk when the node OS is started. The system administrator does not need to create LUs.

After the LUs are created, perform the following tasks as necessary.

For a cluster configuration

By default, an LU in a storage system connected to a node via an FC path is automatically allocated as a user LU (device file). When settings are changed to prevent user LUs from being automatically allocated, such as during maintenance, the system administrator must manually allocate user LUs. For details about manually allocating user LUs that are connected to a node via an FC path, see the *CLI Administrator's Guide*.

For a single-node configuration

By default, an LU that is connected to an internal hard disk drive or a node via an FC path is automatically allocated to a newly created volume group. When LUs are automatically allocated to volume groups, a separate volume group is created and used to manage LUs that are of the

same drive type (or pool for virtual LUs) and that are in the same chassis (internal hard disk drive or storage system).

When you create LUs after adding an internal hard disk drive or storage system, you can use a Web browser to log on to the HDI system and automatically allocate the LUs to volume groups. For details about how to add a drive, see the *Administrator's Guide*.

Notes on allocating LUs

Note the following points when you allocate LUs to file systems in a cluster configuration or when you allocate LUs to volume groups in a single-node configuration:

- The I/O characteristics and processing speed differ depending on the LU drive type. When considering which LUs to use, the system administrator must carefully consider the intended use of the file system and the characteristics of the disk drives.
- Do not use LUs that are part of different redundant configurations for a file system or volume group. When the file system or volume group consists of LUs from different redundant configurations, the file system or volume group depends on the fault tolerance of the LU that has the minimum level of redundancy. For Hitachi AMS2000 series or HUS100 series storage systems, use Hitachi Storage Navigator Modular 2 to check the LUs before creating the file system or volume group. For VSP G1000, VSP Fx00 model, VSP Gx00 model, Virtual Storage Platform, Universal Storage Platform V/VM, and HUS VM storage systems, or if you are not the storage system administrator, contact the person who is the storage system administrator.
- If you change the LU capacity created in a storage system, perform a refresh operation for the processing node in a cluster configuration. Execute the `fpstatus` command in a single-node configuration.
- To link an HDI system to Dynamic Provisioning to allocate a virtual LU to a file system or volume group, make sure that there is enough space on the pool to which the virtual LU belongs. If there is not enough space in the pool, an application on a client using the file system might terminate abnormally or an HDI error might occur. If a file system uses a virtual LU created from more than one pool and there is not enough space in at least one of the pools, an error might occur even if the usage of the file system does not reach the limit.
- If you are deleting a large amount of files from the file system, execute the `dpreclaim` command to release the unused area of a virtual LU used by the file system. By executing the command after deleting 1 GB or more data, you can prevent the space on the pool to which the virtual LU belongs from being insufficient. If the capacity of the file system that uses the virtual LU is less than 256 MB, the `dpreclaim` command cannot be used to release the unused area of that virtual LU.

  Take note of the following before executing the `dpreclaim` command:

  - 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.

- To release the space on the virtual LU allocated to the deleted file system or volume group, delete the virtual LU.
- Enable the mapping guard for the LUs of the storage systems that are used in the HDI system. For the LUs that are used in the HDI system, if you change the mappings of the LUNs (host LU numbers) and LDEV numbers to be set for the storage system, the HDI system will not function correctly. Do not change these mappings. You can set the mapping guard by using Storage Navigator, or version 6.5 or later of Hitachi Storage Navigator Modular 2.

Notes on using the local data encryption functionality

Keep the following in mind before using the encryption function for user LUs (local data encryption functionality):

- The local data encryption functionality can encrypt user LUs only. User data such as files and directories are decrypted when the file system is accessed. The following figure illustrates the encryption target, using an example of HDI in a cluster configuration:

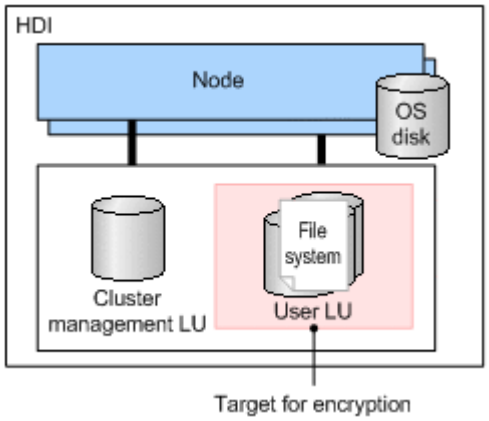


Figure 4-11 HDI encryption target

- The encryption function setting cannot be changed after starting system operation if the encryption function was set at the time the system was newly set up. To change the encryption function setting, you need to set up the system again.
- The common key used for encryption is saved on either the system LU of the HDI system or the HCP system. The key is saved on the HCP system whenever the system settings file is periodically saved on the HCP system. Therefore, if the system settings file is periodically saved on the HCP system, before starting the OS on the node, make sure that the HCP

system is running normally and can properly communicate with the HDI system.

- If the system configuration information is not periodically saved on the HCP system, when a key saved on the system LU becomes corrupted, user data will no longer be available. To recover the key, the system configuration information must be restored. After setting information required for resuming HDI operation (for example, cluster configuration definition and the file system configuration), you must use the **Backup Configuration** dialog box to download the system settings file, and then save the file on storage media outside the system. Even after starting operation, any time you change the system configuration, we recommend manually saving the system settings file on storage media outside the system.
- If you periodically save the system configuration information on the HCP system, when a key saved on the HCP system cannot be obtained, user data will no longer be available. To prepare for failures, after enabling the encryption functionality, we recommend that you use the `encdisplaykey` command to display the key to save on storage media outside the system, and then save the key. After saving the key on storage media outside the system, use the `encverifykey` command to cross-check the key that is saved on the HCP system and the key saved on storage media outside the system.
- HDI file systems using the encryption function are not portable because different keys are used for different HDIs. Therefore, you cannot change nodes connected by a command such as `fsexport` and `fsimport`.
- Data stored in an HCP system will not be encrypted. For details on encrypting data to be stored in an HCP system, see Encrypting data to be stored in an HCP system on page 6-19.

Notes when supporting 64-bit inodes

Please note the following regarding file systems that support 64-bit inodes:

- Changing the settings to support 64-bit inodes is irreversible. If you no longer want the file system to support 64-bit inodes, you must reconfigure the file system and restore the settings from backup data obtained before the system was changed.
- Some applications that run in NFS environments might not support 64-bit inodes. Be sure to configure support for 64-bit inodes only when applications that support 64-bit inodes are used.
- The NFSv2 protocol is not available for files systems that handle 64-bit inodes. Before setting a file system to handle 64-bit inodes, make sure that no clients are using the NFSv2 protocol for the file system.
- When backup data obtained by using NDMP functionality within a file system that supports 64-bit inodes is restored to a file system configured with a version earlier than 4.2.3-03, some files might not be restored.
- When data migrated to an HCP system from a file system that supports 64-bit inodes is restored to a file system that was configured with a version earlier than 4.2.3-03, some files might not be restored.

Issuing warnings about file system usage

When SNMP notifications or email error notifications are enabled, File Services Manager issues warnings about file system usage if file system usage exceeds a predefined value (the *warning threshold*) or reaches a maximum value.

When the system is first installed, warnings related to file system usage are issued if the usage exceeds the warning threshold. A system administrator can use File Services Manager to enable or disable warning notifications. The system administrator can also view the warning notification settings and change the warning threshold.

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

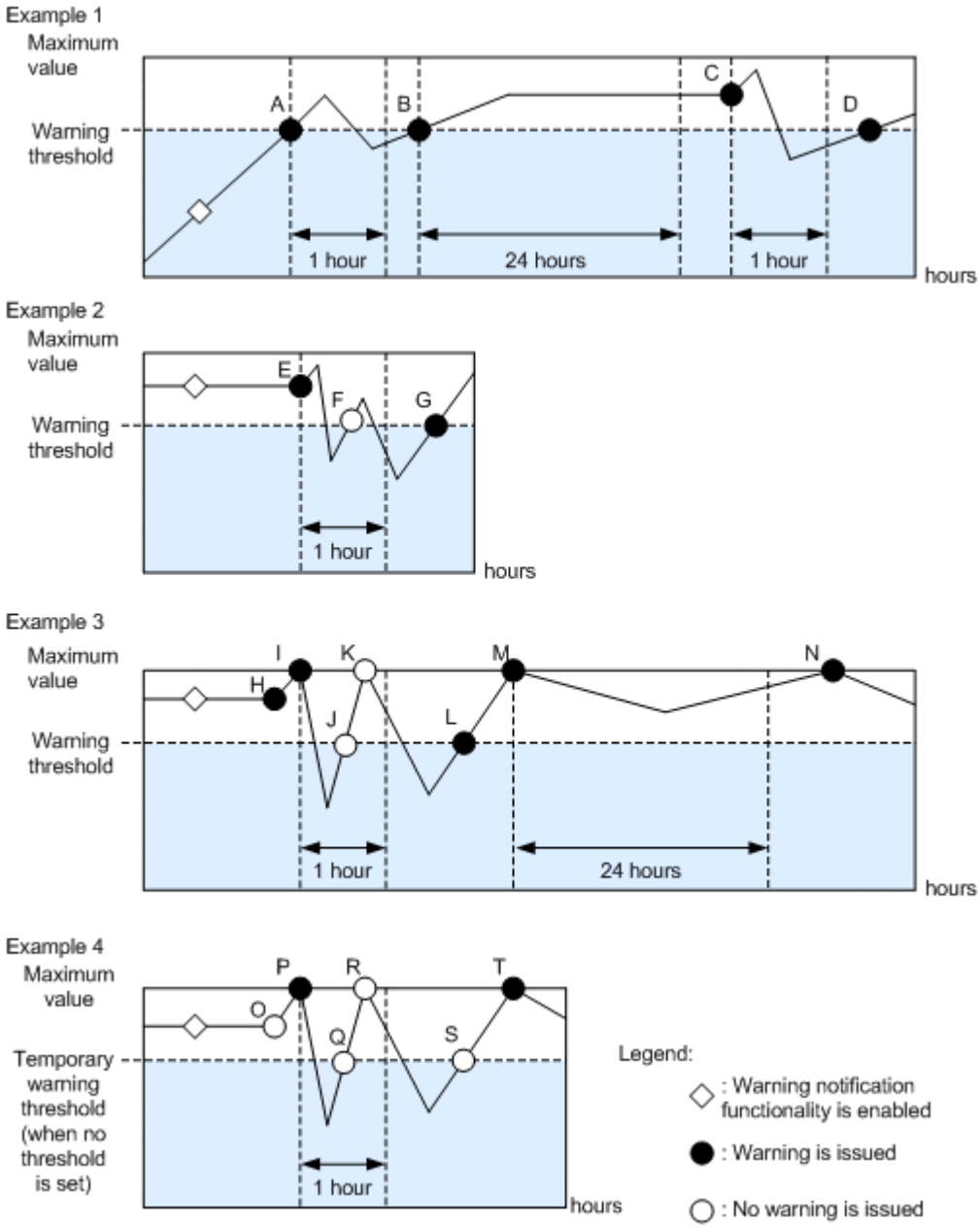


Figure 4-12 Times at which warnings related to file system usage are issued (when monitoring block usage)

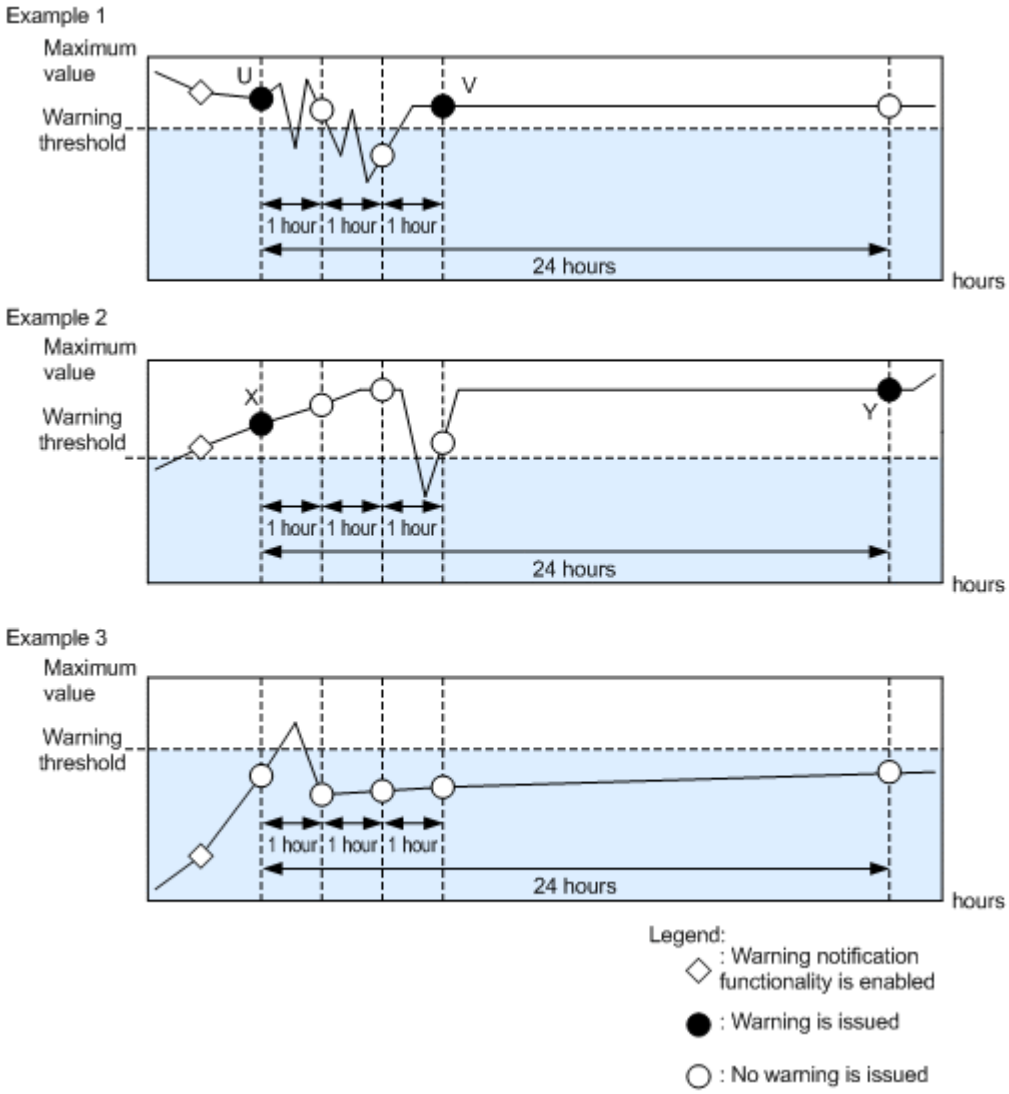


Figure 4-13 Times at which warnings related to file system usage are issued (when monitoring inode usage)

The inode usage is monitored at one hour intervals and a warning is issued when the warning threshold is exceeded.

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

Table 4-1 Times at which the warnings related to file system usage are issued

State	Times at which the warnings related to file system usage are issued	Symbols in the figure
Block usage exceeds the warning threshold	After warning notification is enabled, a warning is issued when block usage exceeds the warning threshold for the first time.	A

State	Times at which the warnings related to file system usage are issued	Symbols in the figure
	If block usage exceeds the warning threshold while warning notification is enabled, a warning is issued when the file system is used.	E, H
	A warning is issued when both of the following conditions are satisfied: • At least one hour has passed since a previous warning was issued because the warning threshold was exceeded. #1 • Block usage exceeds the warning threshold.	B, D, G, L
	A warning is issued when both of the following conditions are satisfied: • After a previous warning was issued because the warning threshold was exceeded, the warning threshold continued to be exceeded for at least 24 hours. • The file system was used.	C
Block usage reaches the maximum value	After warning notification is enabled, a warning is issued when block usage reaches the maximum value for the first time.	I, P
	A warning is issued when both of the following conditions are satisfied: • At least one hour has passed since a previous warning was issued because block usage reached the maximum value. #1 • Block usage went below the warning threshold and then reached the maximum value again. #2	M, T
	A warning is issued when both of the following conditions are satisfied: • After a previous warning was issued because block usage reached the maximum value, block usage continued to exceed the threshold value for at least 24 hours. • Block usage reached the maximum value again.	N
Inode usage exceeds the warning threshold	After warning notification is enabled, a warning is issued when inode usage is monitored and exceeds the warning threshold for the first time.	U, X
	The inode usage did not exceed the warning threshold, but one hour later, inode usage is monitored and exceeds the warning threshold.	V
	A warning is issued when both of the following conditions are satisfied: • After a previous warning was issued because the warning threshold was exceeded, when inode usage is monitored, the warning	Y

State	Times at which the warnings related to file system usage are issued	Symbols in the figure
	threshold continued to be exceeded for at least 24 hours. • When inode usage is monitored, the warning threshold is exceeded.	

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

- Warning notification is disabled and then enabled again.
- The warning threshold is changed.
- The file system is unmounted and then mounted again.
- After the warning threshold is specified with a percentage (%), the file system is expanded. (The warning threshold is re-calculated.)

#1:

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

#2:

If the warning threshold is 0, a dummy warning threshold is set to judge whether block usage went below the warning threshold after reaching the maximum value. A warning is not issued even when block usage exceeds the dummy warning threshold (O, Q, and S in the figure).

When the striping function is used

An HDI system enables you to create file systems by using a volume manager's striping function.

Overview of the striping function

Striping is one of the functions a volume manager (LVM) provides. This function enables you to divide contiguous data blocks of a file system into blocks of a desired size, and then evenly spread out the blocks across multiple device files. Because the number of divided data blocks is equal to the number of stripes and I/O processing is performed on the device files in parallel, access speed to a disk drive might be improved.

The following figure shows how the data blocks are assigned when the striping function is used. The number of stripes is equal to the number of device files that were specified when the file system was created. Also, data blocks are assigned by the order of specified device files. In the following example, device files are specified in the order of `lu00`, `lu01`, `lu02`, and then `lu03`.

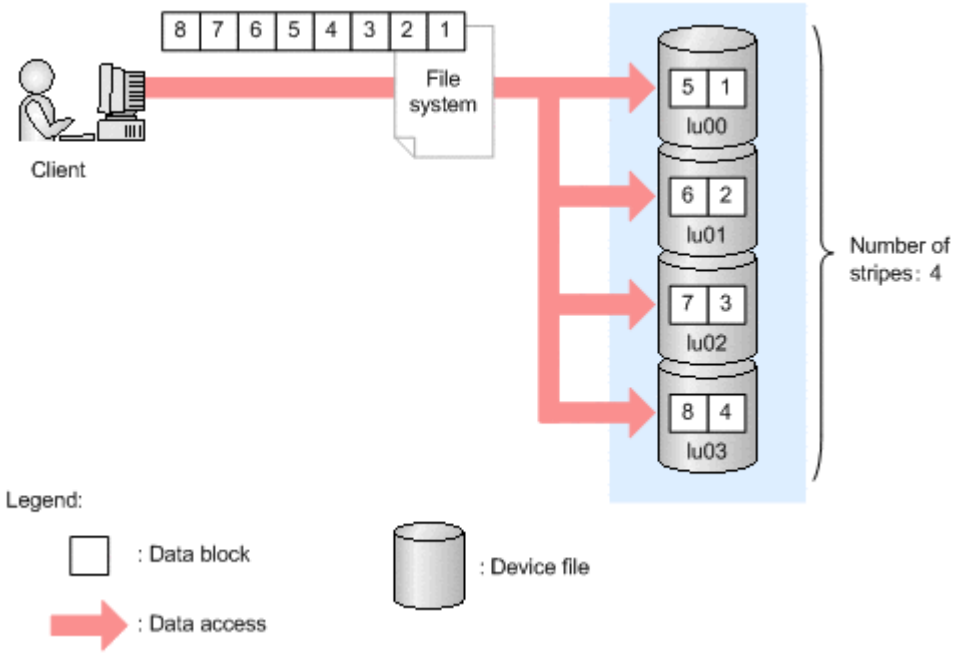


Figure 4-14 Example of the striping function

The following figure illustrates how data blocks are assigned when the capacity of a striped file system has expanded. The number of stripes remains the same, even when you expand the capacity of a file system.

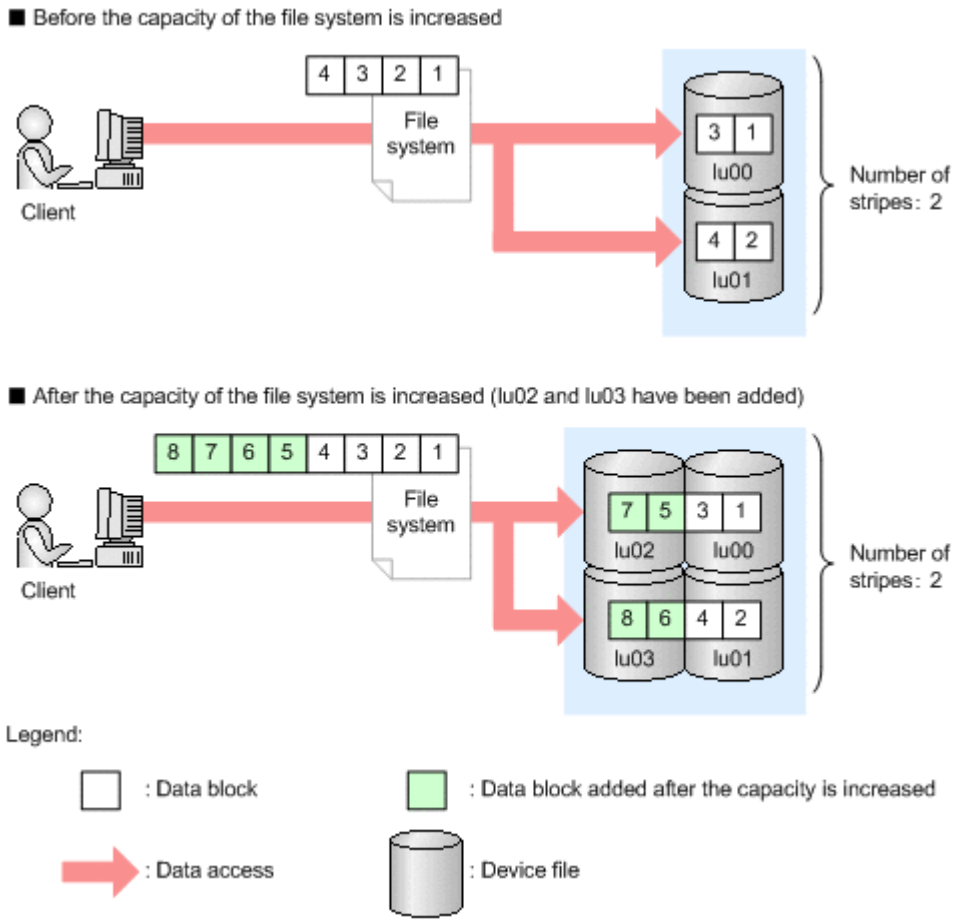


Figure 4-15 Example of the striping function when expanding a file system

If you specify `lu00` and `lu01` for the creation of a file system, and then specify `lu02` and `lu03` in order to expand the file system, `lu00` and `lu02` will become one stripe, and `lu01` and `lu03` will become another stripe.

Notes on the striping function

Note the following when using a volume manager striping function:

- When creating or expanding a file system, specify device files of the same size.
- When expanding a file system, the number of device files and the number of stripes must be the same.
- Make sure that the device files with which you create a file system belong to different parity groups. If you create a file system with device files from the same parity group, access performance might not improve when striping is used.

Selecting which ACL type to use for a file system

The HDI system allows you to specify access control lists (ACLs) for files and directories. The HDI system provides two ACL types for file systems: the

Advanced ACL type, in which ACLs conforming to NTFS ACLs can be specified, and the Classic ACL type, in which ACLs conforming to POSIX ACLs can be specified.

When creating a file system, the system administrator must select the ACL type to be used for the file system. When you want to use only the NFS protocol for a file share in the file system, we recommend you create a file system that uses the Classic ACL type. When you want to use both the CIFS protocol and the NFS protocol or use only the CIFS protocol, we recommend you create a file system that uses the Advanced ACL type.

Note the following when accessing a file system of either ACL type from an NFS client:

- In a file system that uses either ACL type, when a client copies a file by using the NFSv2 or NFSv3 protocol, the file will be copied without the ACL information. If a client copies a file by using the NFSv4 protocol, whether the ACL information is copied with the file depends on the environment settings of the client.
- File systems of the Advanced ACL type cannot be accessed via the NFSv2 protocol.
- Which users can execute the `chgrp` command on an NFS client depends on the ACL type used by the file system:

  Advanced ACL type
  : The root user and users with the owner permission can execute the command.

  Classic ACL type
  : Only the root user can execute the command.

- When you create a symbolic link by executing the `ln` command from an NFS client, the permission mode that is assigned to the symbolic link file depends on the ACL type used by the file system:

  Advanced ACL type
  : The access control entry (ACE) of the parent directory determines the assigned permission mode.

  Classic ACL type
  : The fixed value `777` is always assigned.

  Also, the access permission of a symbolic link file is based on the permission mode of the target file, not the permission mode of the symbolic link file itself.
- From a Solaris 10 or HP-UX 11i v3 NFS client using the NFSv4 protocol, if the command used to view Advanced ACLs is executed on a file whose Advanced ACL was set by a user or group not managed by the HDI system, an error might occur. For example, if you execute the `ls` command without any options on an Advanced ACL type file system, the command results will be properly displayed. However, if you execute the `ls` command with the `-l` option, the command will end with an error.
- By using the NFSv4 protocol, ACLs can be viewed or set up from an NFS client. However, the number of specifiable ACEs on a Linux NFS client

might be less than the normal limit for HDI system ACEs. As a result, you might not be able to specify ACEs from a Linux NFS client. For details on the maximum number of specifiable ACEs, see Table 4-2 Differences between file systems that use the Advanced ACL type and the Classic ACL type on page 4-35.

The following table lists the differences between file systems that use the Advanced ACL type and the Classic ACL type.

Table 4-2 Differences between file systems that use the Advanced ACL type and the Classic ACL type

Item	Advanced ACL type	Classic ACL type
Specification to which the ACL type conforms	NTFS ACL[#1]	POSIX ACL
Owner of files or directories	User or group	User
Maximum number of ACEs[#2]	700	128 (The maximum number of ACEs in the access ACL and default ACL is 64 each.)
ACE type	**Allow** or **Deny**	**Allow**
Access permissions to be set[#3]	• Full Control • Traverse Folder/Execute File • List Folder/Read Data • Read Attributes • Read Extended Attribute • Create Files/Write Data • Create Folders/Append Data • Write Attributes • Write Extended Attributes • Delete Subfolders and Files • Delete • Read Permissions • Change Permissions • Take Ownership	• Read • Write • Execute
ACL to be set when a new file or directory is created	ACL that was inherited from the parent directory Initial permission specified when a CIFS share is created, if the ACL that was inherited from the parent directory is not set.	Initial permissions that were specified when a CIFS share was created
File attributes that can be set (DOS attributes)	• Read only • Archive • Directory	• Read only • Directory

Item	Advanced ACL type	Classic ACL type
	• Hidden file • System file	

#1:

The HDI system only supports discretionary access control lists (DACLs). Accordingly, the standard Windows audit functionality cannot be used. Use the CIFS access log files provided by the HDI system.

#2:

Although more than 700 ACEs can be set in a Windows NTFS ACL, the maximum number of ACEs that can be set in a file system provided by an HDI system is 700 or 128 (the maximum number of ACEs in the access ACL and default ACL is 64 each).

#3:

When you set an NFSv4 ACL from NFS clients, the appropriate access permissions are mapped from the NFSv4 ACL according to what type of ACL is used in the file system.

Migrating to a file system that uses the Advanced ACL type

The HDI system allows you to migrate a file system that uses the Classic ACL type to a file system that uses the Advanced ACL type.

The method for evaluating **Allow** access permissions differs between file systems that use the Classic ACL type and the Advanced ACL type as follows:

When a file system uses the Advanced ACL type:

A user's access permissions are based on the permissions granted to others (`Everyone`) or the group to which the user belongs, regardless of whether those permissions are granted to the individual user. For example, when write permission is granted to others (`Everyone`) or a group to which the user belongs, the user will now also have write permission, even if they were not specifically targeted.

When a file system uses the Classic ACL type:

A user's access permissions are only based on the permissions granted to the user. For example, when only read-only permission is granted to the user, even if write permission is granted to others (`Everyone`) or the group to which the user belongs, the user will not have the write permission.

Because the evaluation methods of the user permissions differ as described above, in order to prevent the access permissions of users and groups that have less permission than the others (`Everyone`) before a migration from being increased to the same permission as the others (`Everyone`) after the migration, **Deny** ACEs are added. This occurs in the following situations:

- When the access permissions (selected in **Permissions** displayed in the Windows Properties window) of a user and the group to which the user belongs are less than those for others (`Everyone`)
- When the access permissions (selected in **Permissions** displayed in the Windows Properties window) of the user are less than those for the group to which the user belongs

In addition, the information displayed in **Permissions** of the Windows Properties window might differ before and after a file system migration. For example, even if **Full Control** is displayed before migration, **Special** might be displayed after migration.

ACLs might differ before and after migration because ACLs are converted based on the ACL inheritance relationship and access permissions that were specified for file systems that use the Classic ACL type. If the converted ACLs are different from the ones intended for the CIFS client that is using the files and directories, the ACLs must be reconfigured for the file system after the migration. Before deciding whether to migrate a file system, the system administrator needs to check the notes on migrating a file system.

After a file system has been migrated, the ACLs for the file system are created with precedence given to making sure that the access permissions for files or directories do not change, rather than making sure that the access permissions can be visually confirmed from the client. Depending on the type of client ACL operation, operations on a file system might become difficult because of the difference in the visual display of the access permissions after migration.

For detailed notes on migrating a file system that uses the Classic ACL type to a file system that uses the Advanced ACL type, see Notes on migrating a file system on page 4-38.

Reference:

In the rest of this subsection, access permissions are represented in the following format:

octal-notation-of-access-permission(*abbreviation-of-access-permission*)

The following table shows how access permissions are represented.

Table 4-3 How access permissions are represented

Octal notation of access permissions	Abbreviation of access permissions	Description
7	rwx	Access permissions allowing reading, writing, and execution
6	rw-	Access permissions allowing reading and writing
5	r-x	Access permissions allowing reading and execution
4	r--	Access permissions allowing reading only

Octal notation of access permissions	Abbreviation of access permissions	Description
3	-wx	Access permissions allowing writing and execution
2	-w-	Access permissions allowing writing only
1	--x	Access permissions allowing execution only
0	---	No access permissions

Notes on migrating a file system

The HDI system creates an ACL so that the inheritance relationship and access permissions can be inherited after migrating a file system from the Classic ACL type to the Advanced ACL type.

Only **Allow** access permissions can be specified for a file system that uses the Classic ACL type. To maintain the inheritance relationship and access permissions, **Deny** ACEs might be added to the ACLs created after the migration. For details on the correspondence between the access permissions specified for a file system that uses the Classic ACL type before a migration and the access permissions created after the migration, see Appendix A, ACLs Created After the File System Is Migrated to That of the Advanced ACL Type on page A-1.

You must keep the following in mind when migrating a file system from the Classic ACL type to the Advanced ACL type:

- **Execute File** displayed as the access permission for CIFS clients corresponds to `4(r--)` for a file system that uses the Classic ACL type, and corresponds to `1(--x)` for a file system of the Advanced ACL type. If the file system that will be migrated contains an executable file whose access permissions are `4(r--)`, you must add `1(--x)` to the access permissions in order to allow the file to be executed after the migration as well. Either change the access permissions before the migration or use the `fsctl` command to add `1(--x)` during the migration. Note that, when `1(--x)` is not included in the access permissions of the parent directory, if you use the `fsctl` command to add `1(--x)` to the access permissions of the files under the parent directory, the inheritance relationship between the parent directory and the files will be lost because their access permissions will differ.
- The access permissions have not been changed, but the visual display of the access permissions might differ after migration. The following figure shows an example where the user's access permissions become a smaller value after a migration (No.1).

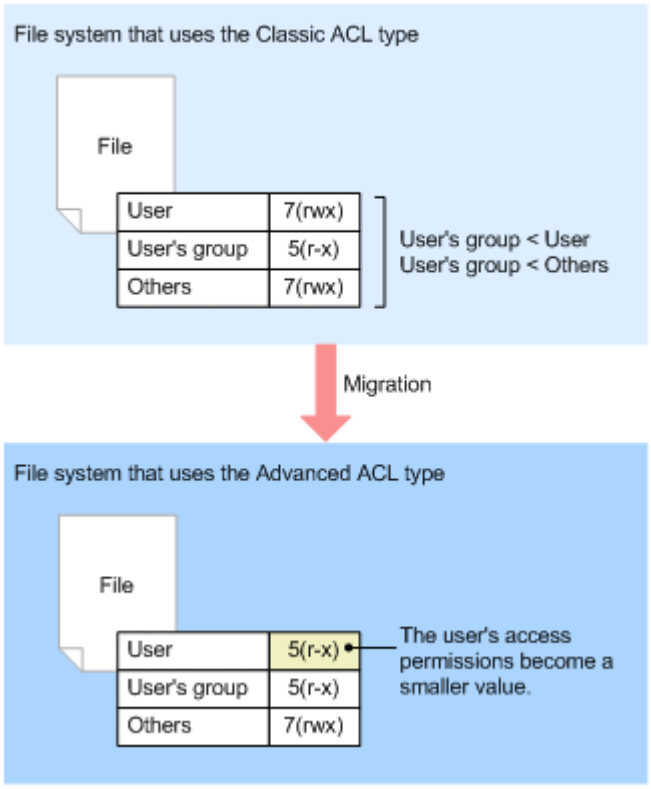


Figure 4-16 Example where the user's access permissions decrease after a migration (No.1)

If a user belongs to a group whose access permissions are lower than that for others (`Everyone`), and the user's access permissions are higher than that of the group, **Deny** ACEs will be added to the group after migration. In a file system that uses the Advanced ACL type, because **Deny** ACEs are evaluated before **Allow** ACEs, the user's access permissions will decrease after a migration.

- If the migration affects the access permissions of a file system, ACLs will be created in such a way that the access permissions become more limited. The following figure shows an example where the user's access permissions will decrease after a migration (No.2).

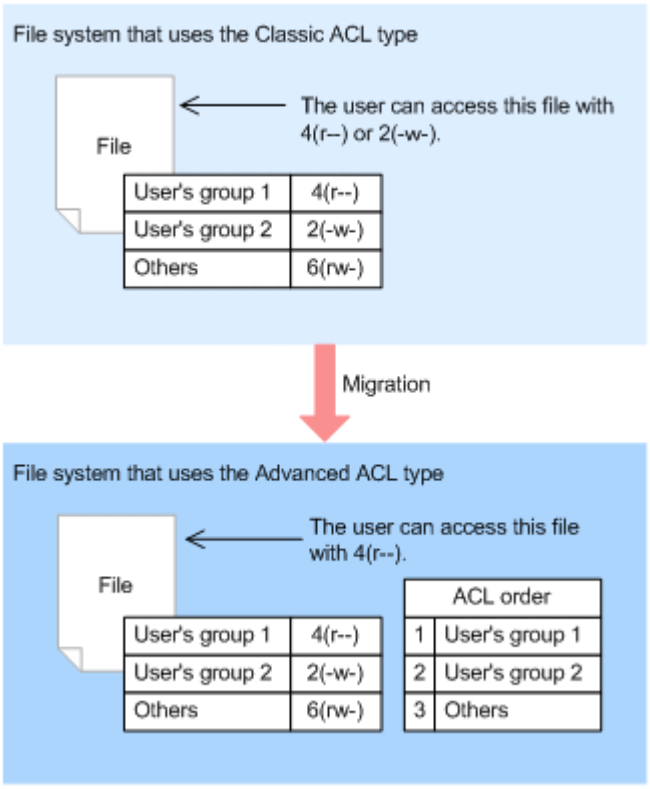


Figure 4-17 Example where the user's access permissions decrease after a migration (No.2)

If a user belongs to multiple groups whose access permissions are lower than that for others (`Everyone`), and each group has different permissions for files not owned by the user, the user's access permissions will decrease after a migration.

- If you migrate a file system, information displayed in **Permissions** of the Windows Properties window might differ before and after migration. For example, if the access permissions are set to `7(rwx)` for a file system that uses the Classic ACL type, the information is displayed so that **Full Control** permission is granted, however, after migration, the displayed information changes so that only **Delete** is not allowed.
- The NFSv2 protocol is not available for file systems that use the Advanced ACL type. Make sure that no clients are using the NFSv2 protocol for the file system after a migration.
- The HDI system allows quota information to be inherited after the migration of a file system from the Classic ACL type to the Advanced ACL type.

Estimating the file system size after a migration

Migrating a file system of the Advanced ACL type increases the amount of information in the ACEs, thus increasing the file system size. Normally, in a file system of the Advanced ACL type, an ACE uses a 4 KB for a file or a directory. The system administrator must allocate sufficient free area before migrating the file system.

An ACE might use up to 64 KB for a file or directory. If too many ACEs have been specified for a file system of the Classic ACL type, take the ACEs into consideration when estimating the file system size.

How to migrate a file system

If a file system that will be migrated contains an executable file whose access permissions are `4(r--)` (a file that can be executed from a CIFS client), you will no longer be able to execute the file after the migration. The system administrator needs to request the file owner to change the access permissions before migration, or use the `fsctl` command to change the access permissions of the file.

Executing the `fsctl` command automatically changes the access permissions of a file of a specified extension. If the system administrator cannot identify the file extension, or if there are settings only allow the file owner to change the access permissions of the file, request the file owner to change the access permissions.

The following describes the procedure for migrating a file system that uses the Classic ACL type to a file system that uses the Advanced ACL type.

To migrate a file system:

1. Contact the end users.

   Ask the end users to not access the file system during this task.

   Also, ask beforehand if the file owner needs to change the access permissions of any executable files whose access permissions are `4(r--)`.
2. Back up the file system you want to migrate.
3. Add `1(--x)` to the access permissions of executable files.

   Use the `fsctl` command to add `1(--x)` to the access permissions of executable files whose access permissions are `4(r--)` in order to enable the files to be executed after migration.

   ```
   $ sudo fsctl -c -x -o add_exeauth filesystem03/unit15
   filesystem03/unit15: Wait ..... Success
   ```
4. Save the file share settings.

   Use the `cifslist` or `nfslist` command to check, and then save the file share settings for the file system that will be migrated.

   ```
   $ sudo cifslist -v -O all
   List of File Shares:
   The number of CIFS share(1)
     Name of file share            : unit15
     Shared directory              : /mnt/filesystem03/unit15
     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        : sys04
     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
  Read-only cache for conflicts : default
  Access Based Enumeration      : default

$ sudo nfslist -O all
List of File Shares:
The number of NFS share(1)
    Shared directory                          : /mnt/filesystem03/unit14
        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)                    : --
        Host/network name resolution          : OK
        Security flavor                       : sys,krb5i
```

5. Release all the file shares.

   Use the `cifsdelete` or `nfsdelete` command to release all the file shares in the file system.

```
$ sudo cifsdelete -x unit15
$ sudo nfsdelete -d /mnt/filesystem03/unit14 -a
```

6. Unmount the file system.

   Use the `fsumount` command to unmount the file system.

```
$ sudo fsumount filesystem03
```

7. Change the ACL type of the file system to the Advanced ACL type, and then mount the file system.

   Use the `fsmount` command to change the ACL type of the file system from the Classic ACL type to the Advanced ACL type, and then mount the file system.

```
$ sudo fsmount -w -c filesystem03
```

8. Convert the ACL type of the files to the Advanced ACL type.

   Use the `fsctl` command to convert the ACL type of the directories and files from the Classic ACL type to the Advanced ACL type.

```
$ sudo fsctl -c -x -o advanced_acl filesystem03
filesystem03: Wait ............. Success
```

Note:

After you have changed the ACL type of the file system in step 7, if the files and directories in the file system are accessed, the ACL type used for the files and directories will automatically change. However, the ACL type might not be changed if there is not enough space in the file system after the migration. The system administrator needs to make sure that there is enough space in the file system after the migration, and then use the `fsctl` command to change the ACL type of the files and directories.

9. Re-create the file shares.

   Use the `cifscreate` or `nfscreate` command to re-create the file shares.

```
$ sudo cifscreate -x unit15 -d /mnt/filesystem03/unit15 -D add:sys04
$ sudo nfscreate -d /mnt/filesystem03/unit14 -H host01
```

Using WORM file systems

On file systems for which the WORM functionality is enabled (*WORM file systems*), any file can be prevented from being changed or deleted for a set period of time. Files that can no longer be changed or deleted are called *WORM files*, and the period for which a WORM file cannot be deleted is called the *retention period*. Note that WORM files for which the retention period has expired can be deleted by canceling the read-only attribute, but they cannot be modified.

Files in a WORM file system can be changed to WORM files by using the autocommit functionality or manually from clients.

Using the autocommit functionality to change files to WORM files

You can set whether to use the autocommit functionality for WORM file systems. When you use the autocommit functionality, a file not changed in the specified period (autocommit period) is changed to a WORM file. The value specified as the default retention period (10 days as the initial value) is set as the retention period for a WORM file created by using the autocommit functionality. You can also change the default retention period even after autocommit operation starts.

Use the autocommit functionality in auto mode or manual mode. In auto mode, all ordinary files, except for the system files and files in the system directories, are subject to the autocommit functionality. Additionally, the autocommit functionality changes a file to a read-only file the first time the WORM file is accessed. In manual mode, files that are specified as read-only files by clients are subject to the autocommit functionality.

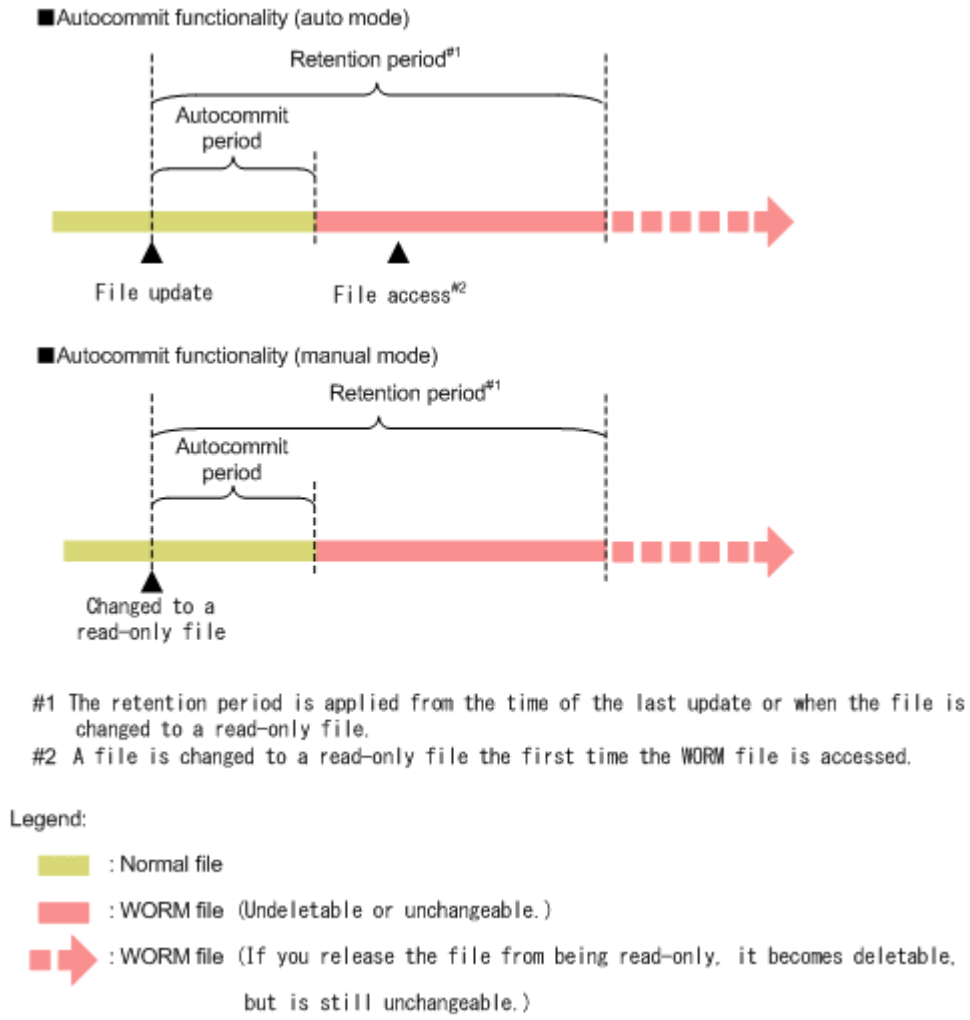


Figure 4-18 Transition of a file when the autocommit functionality is used

Consider the following when you use the autocommit functionality to change files to WORM files:

- After setting a WORM file system to use the autocommit functionality, you cannot set it not to use the autocommit functionality.
- To change the autocommit functionality from manual mode to auto mode, a client must manually change read-only files to WORM files and then change the mode settings.
- Even if you change the autocommit functionality from auto mode to manual mode, files that were created when auto mode was enabled are changed to WORM files by auto mode operation. Therefore, those files are changed to WORM files rather than read-only files.
- When you change the settings to use the autocommit functionality in auto mode, the autocommit management information about a WORM file system is rebuilt. Consequently, access performance is temporarily affected. After the processing is complete, the KAQM37139-I message is output to the system message.
- After the autocommit period is set, it cannot be changed.

- For linkage with the HCP system, if the execution interval of migration is longer than the autocommit period, migration processing might take a long time. Specify settings so that the autocommit period is less than the execution interval of migration.
- The default retention period that is effective when a file is accessed after the autocommit period has elapsed is applied as the retention period. If you change the default retention period, the new default retention period is applied to files whose retention period is undefined. Before changing the default retention period, confirm that no problems exist concerning WORM file system operation.

Manually changing a file to a WORM file from a client

You can change a file to a WORM file by changing the last access date and time of the file (`atime`) to the retention end time, and setting the file to read-only.

Change `atime` so that the period of time from the date and time when the file is changed to read-only until the retention end date and time is within the range of the minimum and maximum retention periods that were specified when the WORM file system was configured.

To change `atime` from a client, the user must create their own custom application. For details about the API used to create custom applications for WORM operations, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

After a file is changed to a WORM file, the retention period can be extended by changing `atime`. For files for which the retention period has expired, you can set the retention period again by canceling the read-only attribute, changing `atime` to the retention end time, and then setting the read-only attribute again. Note that WORM files for which the retention period has expired can be deleted by canceling the read-only attribute, but the data cannot be modified.

If you change a file to a WORM file or change the retention period from an NFSv4 client using Linux, use Linux kernel version 2.6.35 or later, or apply the following patch:

Patch name

```
NFSv4: Fix an embarassing typo in encode_attrs()
```

Commit ID

```
d3f6baaa34c54040b3ef30950e59b54ac0624b21
```

If the period of time from when a file is set to read-only until the retention end time is not within the range of the minimum and maximum retention periods, the following settings are configured:

- If the period of time from when read-only was set until the specified retention end time is greater than the maximum retention period, the maximum retention period is used as the retention period.

- If the period of time from when read-only was set until the specified retention end time is less than the minimum retention period, the minimum retention period is used as the retention period.
- If read-only is set more than 24 hours after the specified retention end time, system operation is affected as noted below. System operation is affected differently when the maximum retention period is set to infinite:
  - If the maximum retention period is infinite, the retention period is also infinite.
  - If the maximum retention period is not infinite, the file is not changed to a WORM file.
- If read-only is set 24 hours or less after the specified retention end time, the file is not changed to a WORM file.

Setting a file to read-only

The methods used to a) change a file into a WORM file by setting the read-only attribute or b) delete a WORM file with an expired retention period by canceling the read-only attribute differ depending on the type of file shared. The differences are described below.

For a file with a CIFS share:

Can set or cancel the read-only attribute by modifying the file attribute (not the ACL setting).

For a file with an NFS share:

Can set the read-only attribute by disabling the write permission (w) for all file users (user), groups (group), and others (other). Note that the read-only attribute can be canceled by granting write permission (w) to any of the above, but the read permission (r) and execution permission (x) cannot be modified.

Precautions regarding WORM file system operation

Keep the following in mind for WORM file system operation:

- Once a file system is created, whether the WORM functionality is enabled cannot be changed for the file system.
- To change the name of a directory in a WORM file system, set the WORM settings of the file system to allow the names of empty directories to be changed. Note that the default settings for WORM file systems that have been set up in version 4.0.0-00 or later do not allow directory names to be changed.
- ACL types cannot be changed after a WORM file system is set up.
- `atime` is not updated when a WORM file for which the retention period has not expired is accessed.
- Even if the creation time of a file is set to be recorded in a WORM file system, the creation time of the WORM file is not recorded.
- You cannot delete a file system that contains a WORM file whose retention period has not expired.

- Empty files of 0 bytes cannot be changed to WORM files.
- If a WORM file system has been restored on an HDI system from data migrated to an HCP system, files for which the retention periods have not expired are not turned into WORM files until the files are accessed to be deleted or changed.

Using CIFS bypass traverse checking

The CIFS bypass traverse checking functionality enables the user to access CIFS by specifying an absolute path to the target object (such as a directory or a file) where the user has access permission, regardless of not having access permission to the higher-level directories.

The following shows an example of the objects.
`/mnt/fs01/dir1/dir12/access.txt`

In this case, if the user does not have access permission to the `dir1` and `dir12` directories but has access permission to the `access.txt` file, the user can access the `access.txt` file by specifying its absolute path.

The CIFS bypass traverse checking functionality can be enabled or disabled for each file system.

If the CIFS bypass traverse checking functionality is disabled, in the HDI system, the user needs to have the Traverse Folder/Execute File permission (file permissions are `1 (--x)` for Advanced ACL type, and `4 (r--)` for Classic ACL type) for all the higher-level directories to access the target object. Also, if different administrators are assigned according to the directory structure, you need to ask the administrator of each directory to change the ACL configuration.

Other than that stated above, the following are several things to note:

- For version 4.2.0-00 and later, CIFS bypass traverse checking is enabled by default when the file system is created. However, the CIFS bypass traverse checking is disabled for the home-directory-roaming file systems.
- When update installation is performed to the HDI system of a version earlier than 4.2.0-00, the CIFS bypass traverse checking for each file system becomes disabled.
- If the system is restored by using the system configuration information that was stored in the system LU of a version earlier than 4.2.0-00, the CIFS bypass traverse checking becomes disabled.
- If data that was migrated on the HCP system by a system with a version earlier than 4.2.0-00 is restored to a file system where CIFS bypass traverse checking was enabled by using the `arcrestore` command, the CIFS bypass traverse checking becomes enabled.

Change the file system settings, if necessary.

About setting quotas

The HDI system also provides quota management for each file system or each directory.

This section explains how to limit capacity for each file system or directory, based on the HDI block usage amount or inode usage amount. For more information about how to limit usage capacity for each file share based on the hard quota for the HCP namespace capacity at the migration destination (setting a namespace quota), see Limiting file share capacity based on hard namespace quotas on page 6-20.

Managing quotas for each file system

Managing quotas for each file system enables the system administrator to set file system-specific quotas for users and groups, as well as set the default quota for a file system.

Managing quotas for each directory (subtree quota)

A quota set up for individual directories within a file system is called a *subtree quota*. Subtree quotas enable the system administrator to manage quotas for each directory of a file system. Managing subtree quotas enables the system administrator to set quotas on directories for users and groups, as well as set quotas or default quotas for directories.

A subtree quota can be set for any directory in a file system. You can set subtree quotas in up to three locations anywhere in a directory tree as long as the locations are in a range of directories that have a parent-child relationship from the highest level to the lowest level. When using the GUI, you can set quotas for directories immediately under a mount point by managing the file share capacity.

If multiple file shares are to be created for a single file system, setting the subtree quota for a shared directory immediately below the mount point enables you to flexibly manage the capacity of each file share. Quotas can be specified for a maximum of 1,023 directories in a file system. Note that there is no upper limit for the number of users or groups that can set quotas.

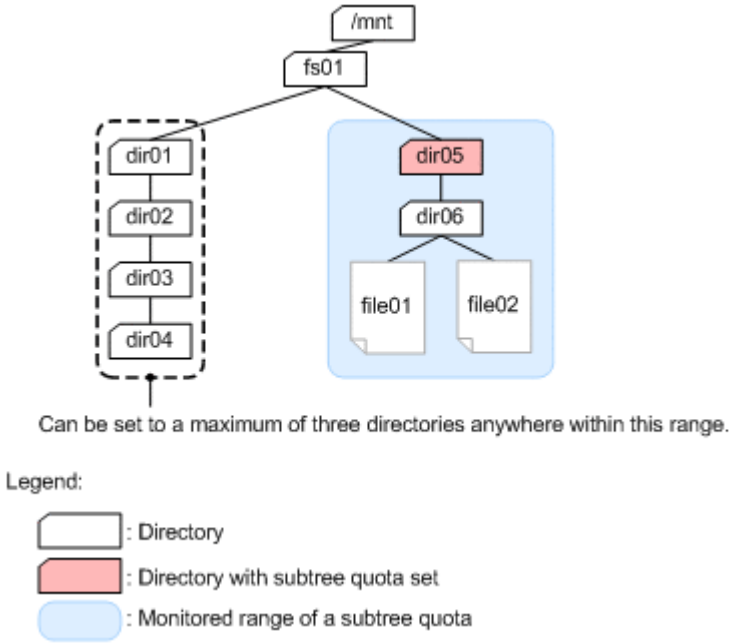


Figure 4-19 Managing subtree quotas

Using a quota for an entire file system with subtree quotas complicates quota management. When a user cannot create or update a file or directory, the information for both types of quotas must be checked to determine the cause. Therefore, we recommend that you specify only one type of quota in an HDI system.

The user's block usage includes the amount of space actually occupied by files. The user's block usage can unexpectedly reach the limit if the file system is set up to migrate files to the HCP system and files are recalled. If the file system is set up to change the files migrated to the HCP system into stub files, do not specify any quotas (including subtree quotas). Also, subtree quotas cannot be set when usage capacity for each file share is limited based on the hard quota of the HCP namespace capacity at the migration destination.

We recommend that you use SNMP trap or email error notifications to monitor file system usage when no quotas are set. Also, you can use the `fsfullmsg` command to enable warning notifications to be sent when the usage of the file system exceeds a certain threshold.

For details about the MIB objects used for SNMP trap notifications, see the *Administrator's Guide*.

In a range of directories of a directory tree that has a parent-child relationship from the highest-level directory to the lowest-level directory, if you rename a higher-level directory of a directory for which a subtree quota has been specified, quota information can no longer be managed correctly. Therefore, if you want to rename a higher-level directory of a directory for which a subtree quota is specified, first cancel the subtree quota setting, then rename the directory, and then specify the subtree quota again. Note that, if you do not follow this procedure and quota information cannot be managed

correctly due to a renamed directory, you can correct the problem by changing the directory name back to its previous name.

Information that can be specified for quota management

The information that can be specified for quota management via an HDI system can be summarized as follows:

- Specifying a quota for each user, group, or directory
- Specifying a default quota
- Specifying a grace period
- Specifying a monitoring method for quotas

The following table shows information that can be specified for each management method for quotas and subtree quotas specified in each file system.

Table 4-4 Information specified for the quota management functionality

Information to be set	Managing quotas for each file system		Managing subtree quotas	
	GUI	Command	GUI	Command
Quota for each user	Specifiable	Specifiable	Not specifiable	Specifiable
Quota for each group	Specifiable	Specifiable	Not specifiable	Specifiable
Quota for each directory	Not specifiable	Not specifiable	Specifiable#	Specifiable
Default quota	Specifiable	Specifiable	Not specifiable	Specifiable
Grace period	Specifiable	Specifiable	Not specifiable	Specifiable
Quota monitoring method	Specifiable	Specifiable	Not specifiable	Specifiable
Disabling quotas set for a directory	Not specifiable	Not specifiable	Not specifiable	Specifiable

#

Managed as the file share capacity immediately under a mount point

This subsection explains the individual settings related to quotas as well as the notes to be taken when specifying quotas.

Specifying a quota for each user, group, or directory

A quota can be specified for each user or group. When subtree quotas are being managed, a quota can also be specified for each directory. The following items are specified for the quota for each user, group, or directory:

Hard limit

You can specify an upper limit (*hard limit*) on the block capacity and the number of inodes available to a user, group, or directory. If the hard limit is exceeded, it is no longer possible to allocate a new block or create a file or directory.

Soft limit

You can specify a warning value (*soft limit*) on the block capacity and the number of inodes available to a user, group, or directory. If the soft limit is exceeded, and a fixed duration (*grace period*) has elapsed, it is no longer possible to allocate a new block or create a file or directory.

When a user or group is no longer able to create or update files, the user or group must delete files until both block and inode usage falls below the soft limits, upon which files can be created or updated again.

The value specified for a soft limit must be equal to or less than the value specified for a hard limit.

When you use the GUI to specify the file share capacity, only the hard limit (i.e., the limit on the block capacity) is set for the directory.

Specifying a default quota

The default quota prevents users that do not have a quota from overusing block capacity and inodes. Hard and soft limits can be specified using a method similar to the method that is used for specifying a quota for each user or group.

The value specified for the default quota is applied when a user, for whom a quota has not been specified, uses a file system or directory for the first time that has the default quota (i.e. when the user creates the file).

The default quota is applied to all users, including users registered by user mapping.

Specifying a grace period

You can specify a fixed duration (*grace period*) to allow a user or group to create a file and allocate blocks after that user or group has exceeded the soft limit.

Specifying a quota monitoring method

Quota information is monitored at specified times. You can use SNMP traps notifications, email notifications, or the `management.log` file to view information on any users or groups that have exceeded the soft limit or grace period.

The *quota monitoring times* and the SNMP trap notification mode (when users or groups exceeding the soft limit or grace period are detected) can be specified for each file system. If a quota is specified, the disk usage will be restricted when either the specified hard limit or grace period is reached, regardless of the quota monitoring time.

There are two SNMP trap notification modes:

Summary notification mode (recommended)

If a state that exceeds the soft limit or grace period is detected for users, groups, or directories, the number of such users, groups, or directories is reported. The `management.log` file and the email notification contain the same information as the summary notification.

Individual notification mode

If a state that exceeds the soft limit or grace period is detected for users, groups, or directories, the quota information of each of the users, groups, or directories will be reported. If the number of users, groups, or directories exceeding the soft limit or grace period exceeds 100, respectively, the individual notifications are suppressed, and only the number of users, groups, or directories exceeding the soft limit or grace period will be reported to the SNMP manager. When managing subtree quotas, the individual notification mode is not available for quotas specified for users and groups.

The following table lists the information items reported if an exceeded soft limit or grace period is detected.

Table 4-5 Information reported if an exceeded soft limit or grace period is detected

Item	Summary notification	Individual notification		
		When a soft limit is exceeded	When a grace period is exceeded	When the individual notification mode is suppressed
Notification time	Yes	Yes	Yes	Yes
Host name	Yes	Yes	Yes	Yes
Node number	Yes	Yes	Yes	Yes
Device identification number	Yes	Yes	Yes	Yes
File system name	Yes#1	Yes#2	Yes#2	Yes
Management type#3	--	Yes	Yes	Yes
User name or group name	--	Yes	Yes	--
User ID or group ID	--	Yes	Yes	--
Type of limit exceeded (`block`/`inode`)	--	Yes	Yes	--
Current usage (units of block usage: KB)	--	Yes	Yes	--

Item	Summary notification	Individual notification		
		When a soft limit is exceeded	When a grace period is exceeded	When the individual notification mode is suppressed
Soft limit value (units of block usage: KB)	--	Yes	Yes	--
Hard limit value (units of block usage: KB)	--	Yes	Yes	--
Remaining grace period (units: seconds)	--	Yes	--	--
Grace period (units: days)	--	--	Yes	--
Number of users, groups, or directories exceeding the soft limit for block usage	Yes	--	--	Yes
Number of users, groups, or directories exceeding the grace period for block usage	Yes	--	--	Yes
Number of users, groups, or directories exceeding the soft limit for inode usage	Yes	--	--	Yes
Number of users, groups, or directories exceeding the grace period for inode usage	Yes	--	--	Yes

Legend: Yes = Reported, -- = Not reported

#1:

If a subtree quota is set for a user or group, this item is displayed in the following format:

file-system-name/directory-name

#2:

If a subtree quota is set for a user, group, or directory, this item is displayed in the following format:
file-system-name/directory-name

#3:
If quotas are managed by a file system, either `user` or `group` will be notified. If subtree quotas are managed, `subtree`, `subtree_user`, or `subtree_group` will be notified.

Notes on specifying quotas

Keep the following in mind when specifying quotas:

- Block usage is managed by file systems in 4-KB units. An allocated block is not only used to write data, but it is also used for system management. As such, even if the total size of some files is less than the block usage limit, the block usage itself might exceed the limit. For this reason, specify a limit value that is at least 1 MB larger than what is needed.
- There are no user, group, or directory quota or default quota restrictions either on root users who are not mapped as anonymous users (NFS clients) or on CIFS administrators. Similarly, there are no group quota restrictions on root group users who are not mapped as anonymous users (NFS clients). In addition, there are no user, group, or directory quota or default quota restrictions when the following operations are performed:
  - Save CIFS access logs. (This includes the automatic collection of logs under certain conditions.)
  - Perform a GUI operation or execute a command as a system administrator
  - Use the NDMP functionality to restore data
- When quotas are set both for a specific user and for a group to which that user belongs, the smaller of the two quotas is applied. The following table shows an example of user quota settings.

Table 4-6 Example of user quota settings

User name	Quota set for the user	Primary group	Groups the user is in
User A	20 GB	Group 1	Group 1
User B	20 GB	Group 1	Group 1
User C	20 GB	Group 1	Group 1
User D	30 GB	Group 2	Groups 1 and 2

Using the example above, if the quota set for group 1 is 25 GB, the block capacity that each user can use is as follows:

A quota of 20 GB is set for users A, B, and C. As such, users A, B, or C can only use 20 GB of block capacity. Furthermore, if user A is using 20 GB, then users B and C can only use 5 GB of block capacity between them.

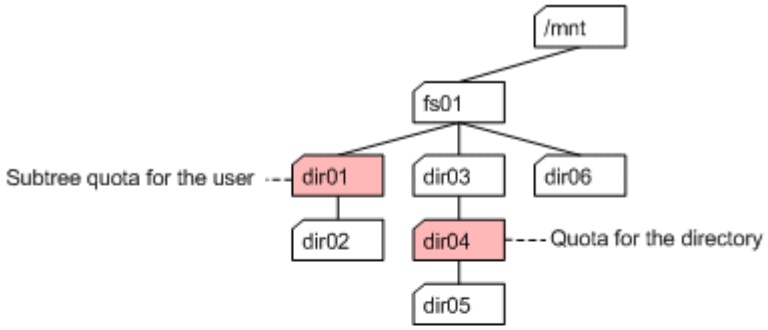
User D can use up to 30 GB of block capacity, assuming that no quota is specified for user D's primary group (group 2). However, if user D updates a group 1 file by using the group's execution permission, then user D will be restricted to a 25 GB block capacity, which is the limit for group 1.

- Subtree quotas cannot be set for directories whose names contain any of the following characters:

  `" * : < > ? \ |`

- When a subtree quota for a user (or group) or the default quota has been specified for a directory in a range of directories that have a parent-child relationship from the highest level to the lowest level in a directory tree, you cannot set subtree quotas for directories under that directory.

  For example, as shown below, if subtree quotas are set to `dir01` for the user, then subtree quotas cannot be set to `dir02`. If quotas are set to `dir04` for the directory, quotas can be set to `dir03` for the directory, but subtree quotas for the user or group, or default cannot be set.



Directory name	Possibility of setting subtree quota
dir02	×
dir03	△
dir05	○
dir06	○

Legend:

: Directory

: Directory with subtree quota set

○ : Yes

△ : Partial (quota for the directory only)

× : No

Specifying quotas for each file system

When many users share a file system, you can specify quotas for users or groups to prevent them from putting too much of a load on the system because they are using too much disk space.

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

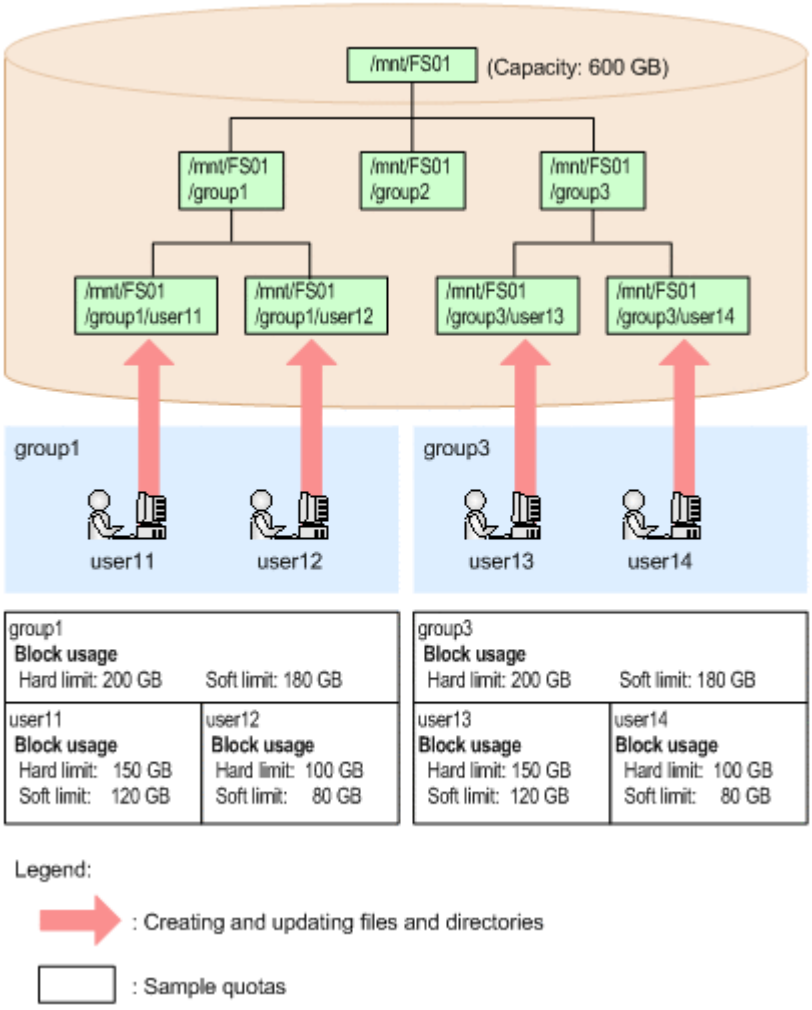


Figure 4-20 Example of specifying quotas for a file system

For example, you can specify quotas for `user11` and `group1` in order to limit the block usage of the `FS01` file system.

Specifying subtree quotas

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

When you specify a subtree quota, you can limit the capacity available in the directory. This enables you to operate a directory in the same way as a file system, allowing you to freely change the capacity.

The following is an example of specifying subtree quotas for these purposes:

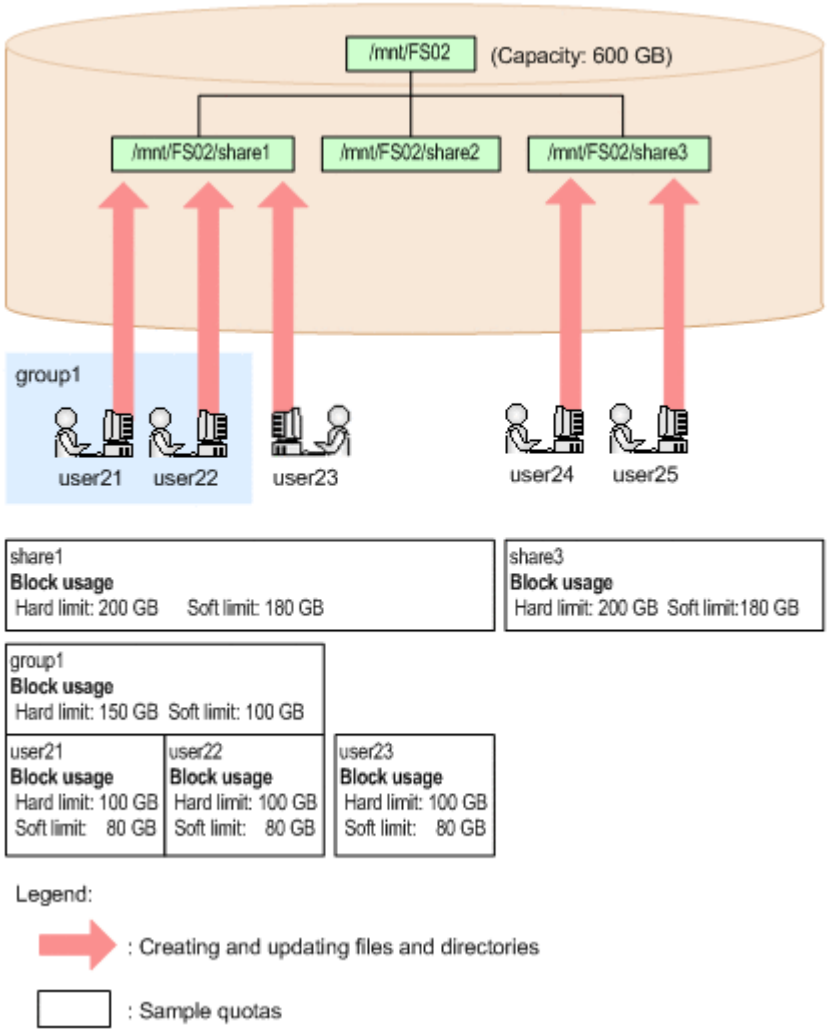


Figure 4-21 Example of setting subtree quotas for directories immediately under the mount point

For example, you can specify quotas for the `share1` directory in the `FS02` file system to limit the available block usage for the directory. You can also set quotas for `user21` and `group1`, which use the `share1` directory, to limit the block usage available in this directory to `user21` and `group1`.

In this example, the available block usage for the `share3` directory in the `FS02` file system is limited to a maximum of 200 GB, but it can be expanded depending on the file system operation.

Notes on quota management

Note the following when managing quotas:

- To manage quotas on a file system, the quota functionality must be enabled when the file system is mounted.
- To start quota management for a file system being mounted, unmount the file system, and then re-mount the file system with the quota

functionality enabled. If the capacity of the file system is insufficient for quota management, the quota management functionality cannot be used. The system administrator must either expand the file system or delete unnecessary files from it in order to increase free space, and then re-mount the file system.

Internal system checks take place when a file system is re-mounted. As a result, the larger the used capacity of a file system, the longer it will take to mount the file system.

- You can view quota information from the SNMP trap. When too many users or groups are registered in the file system, it will take a long time to view the quota information from the SNMP manager. By directly editing the `/etc/snmp/snmpd.conf` file, you can disable the SNMP manager, if there is a large number of users and groups registered in the file system.
- During the process of monitoring quota information, the entire HDI system might become less responsive. If this negatively affects operations, revise the setting of the quota monitoring time.

Also note the following about managing quotas for each file system:

- When File Services Manager is in GUI operation mode, the system administrator cannot display the **List of Quota Information** page of the **Edit Quota** dialog box in the following environments. Place File Services Manager in command operation mode or use commands to perform quota management.
  - An environment in which the total number of users registered by File Services Manager, the NIS server, and the LDAP server for user authentication exceeds 10,000
  - An environment in which the total number of groups registered by File Services Manager, the NIS server, and the LDAP server for user authentication exceeds 10,000
- When File Services Manager is in command operation mode, the system administrator cannot use the GUI to perform the following operations:
  - View quota information for a user or group
  - Specify a user-based or group-based quota

  Instead of using the GUI, use commands to perform the above operations.
- Use commands to manage quotas for users and groups registered by user mapping.
- If you specify a quota for users registered by user mapping, we recommend that you specify quota monitoring times.

Note the following when managing subtree quotas:

- You cannot obtain subtree quota information by executing the command for obtaining quota information from an NFS client.
- For subtree quota information, clients must contact the system administrator.

Typical example of quota management

The following figure shows a typical example of quota management.

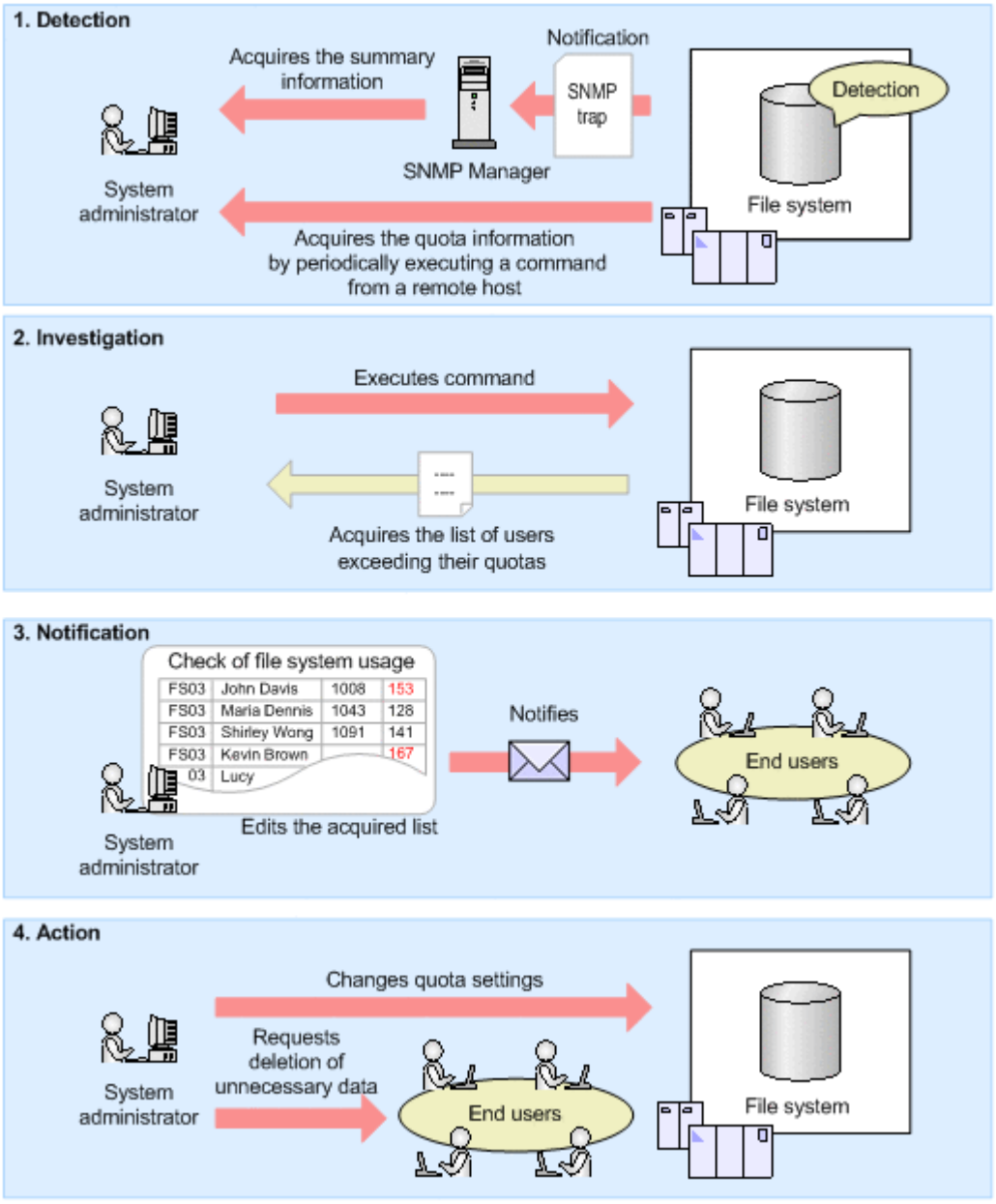


Figure 4-22 Typical example of quota management

1. Detection

   Based on an SNMP trap, an email notification, or the quota information periodically acquired by executing a command from a remote host, the system administrator detects that HDI system users who are using the file system have exceeded a quota.

2. Investigation

   After detecting that a quota has been exceeded, the system administrator checks the file system usage by using commands to obtain the quota

information (including the user names) of those users who have exceeded their quotas.

3. Notification

   The system administrator checks the quota information and then contacts the users who have exceeded their quotas.

4. Action

   The system administrator can take either of the following actions, according to the end users' usage of the file system:

   - Change the quota settings.
   - Ask users to delete unnecessary data.

By using SNMP trap summary notifications or email notifications together with quota-management commands, the system administrator has a comparatively easy way to individually manage file system usage for users and groups even in environments that contain many such users and groups.

About file sharing

For users of different platforms such as UNIX or Windows to be able to access file systems and directories stored in storage systems via NFS or CIFS services, you need to create file shares.

This section describes what system administrators need to know in order to manage file shares.

What to check before using NFS shares

Before operating NFS shares, check the following:

- The NFSv2 protocol is not available for files systems that handle 64-bit inodes. Before setting a file system to handle 64-bit inodes, make sure that no clients are using the NFSv2 protocol for the file system.
- To write a file into a file system by using root user permissions after mounting the file system from an NFS client, you must check and, if necessary, change the following settings:

  Users who are subject to Anonymous Mapping

  In the **Create and Share File System** dialog box, in the **NFS** subtab in the **Access Control** tab, **For root user** is specified for **Anonymous Mapping** by default when a file system is configured from the GUI.

  Note that the default access permissions when the NFS share is created are as follows:

  - File system of the Classic ACL type: `755`
  - File system of the Advanced ACL type: `Everyone full control`
- When Kerberos authentication is used, if you perform time-consuming batch processing for the file system from an NFS client, or if you access the file system from an NFS client that uses Linux, check and, if

necessary, change the expiration time for the ticket, and change the settings of the KDC policy. The expiration time for the ticket is usually set to 8 to 10 hours.

What to check before using CIFS shares

The maximum number of CIFS clients that can connect to an HDI system at the same time in a cluster configuration is set for the cluster. The maximum number in a single-node configuration is set for each node. The maximum number differs depending on whether the CIFS service configuration is set to automatically reload and apply the CIFS share settings to the CIFS client environment. The maximum number also differs depending on the product model or the memory size of the node. For details about the maximum number of concurrent CIFS client connections and the maximum number of CIFS shares, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

Note that the maximum number of concurrent CIFS client connections is the maximum number of clients that can be logically connected. Depending on the flow of inquiries from individual CIFS clients, the CPU usage rate increases and the CIFS service response to CIFS clients might degrade even if the number of concurrent CIFS client connections does not reach the maximum. In particular, this occurs when the following operations are performed from multiple clients:

- Reading or writing to a large file
- Reading or writing to many files
- Frequently displaying a list of folders, or acquiring or changing the attributes of files and folders
- Monitoring the changes to the same folder from multiple clients by using Explorer or similar applications

  The `cifsoptset` command can be used to change settings so that requests from clients to monitor folders are not responded to. Doing so will prevent the CIFS service response time from degrading.

  After changing the configuration definition of the CIFS service by using the `cifsoptset` command to set `change_notify` to `no`, 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.

By default, automatic reloading is enabled. If automatic reload is disabled, you must perform some operations, such as restarting the CIFS service or logging in again to the CIFS client machine, in order to apply changes made to the CIFS share settings to the CIFS client environment. Note the following points when you restart the CIFS service:

- If you change the CIFS share settings while the system is in the failed-over state, you must perform a failback, and then restart the CIFS services.
- If you used commands to change the CIFS share settings, you will need to restart the CIFS service after the changes are made.

Items to check before creating a CIFS share

Check the following items before creating a CIFS share:

- For a CIFS share provided by an HDI system, Unicode (UTF-8) characters are used for file or directory names.
- To configure a CIFS share's access permissions separately for each user and group registered under user mapping, you must use the command line. You cannot configure access permissions for each user and group using the GUI.
- We recommend that you enable the recording of file creation times in the file system before creating CIFS shares. When the system administrator enables the recording of file creation times in the file system, CIFS clients can check the creation times of files in the file system.

  When you create a file system using the GUI, the settings are automatically configured so that the time and date are recorded. When creating a file system by using commands, be sure to specify the option that records the time and date as well. For existing file systems, you can change the time and date settings by using commands.

Setting home drives

Directories in a CIFS share provided by an HDI system can be used for the home drives of CIFS clients.

For details about this setting, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

Linking with MMC

An HDI system enables you to manage CIFS shares by using the Shared Folders functions provided by Computer Management, which is one of Windows administrative tools, from the Microsoft Management Console (MMC). For details about this linkage, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

Using CIFS access logs

System administrators and CIFS administrators can review CIFS access logs to monitor the access history of a CIFS share. For details about using CIFS access logs, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

Configuring ACLs in a file system using the Classic ACL type

On an HDI system, by using commands to configure an ACL, you can configure access permissions for files and directories, not only for the file owner, owner group, or others, but also for specific users and groups. By using File Services Manager to configure an ACL, you can control access to a finer degree than is possible by only using the directory access modes.

There are three types of ACLs available to a file system using the Classic ACL type:

- Access ACL
  An ACL set for a specified directory
- Default ACL
  An ACL set for the files and directories created under a specified directory
- Mask
  A mask is an ACL for limiting enabled access permissions to owner group, specific users, and specific groups. Normally, you do not need to set up this item.

For details about how to perform operations on ACLs from a CIFS client, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

Using the TFTP service

Using the TFTP service enables you to store the boot image files used to boot the network in a file system share so that you can use them from a client machine. This section explains the required settings and notes for using the TFTP service.

TFTP service configuration settings

- Before starting the TFTP service, use the `tftpset` command to set an access directory to the TFTP client. For cluster configurations, both nodes must be set the same.
- While the TFTP service is running, do not delete access directories or unmount file systems that have access directories.
- When the TFTP service is started, we recommend that you use the `svstartupset` command to set the TFTP service to automatically startup when the OS of the node is started or restarted.

Security settings

- Permit others (`Everyone`) to be able to read or write to the public files for the TFTP client.
- If write permission is set to others (`Everyone`), the TFTP client can update the file in the access directory. However, the TFTP client cannot create a new file or directory.
- Do not store files that are not public for the TFTP client in the access directory. If there are files that are not made public for the TFTP client in the access directory, make sure to set the access permission to files so that others (`Everyone`) cannot read or write to the file.
- Set execution permission for the files used for PXE booting to others (`Everyone`).
- To reduce the risk of the access directory being accessed by an unspecified number of clients, we recommend that the TFTP client and the nodes be connected by LAN. Please avoid using WAN connections.

Settings related to TFTP clients and external servers

- If you are performing network booting, you might have to use an external server, such as DHCP server, in order to obtain information such as the IP address of HDI system, or the path to the boot image file to the client machine. For cluster configurations, configure the settings so that the nodes uses the virtual IP addresses to access HDI system from the client machine.

  For details about environment settings, such as for external servers or software used for network booting, see the documentation for each server and software.
- If you are performing operations on files or directories from the TFTP client, specify the path from (but not including) the access directory.

  For example, when the access directory is `/mnt/filesystem01/tftp` and you want to perform operations on the `pxelinux.0` file in the `boot` directory that is right below the access directory, specify `/boot/pxelinux.0`.

  Example specifications for performing operations on files from the TFTP client:

  – Access directory: `/mnt/filesystem01/tftp`

  – File to perform operation: `/mnt/filesystem01/tftp/boot/pxelinux.0`

  – TFTP client specifications: `/boot/pxelinux.0`
- Operations cannot be performed on files or directories whose names contain backslashes (\) or non-ASCII characters.
- For single-node configurations, if TFTP access requests are repeated during the startup processing of a node, the TFTP access request might fail even when the startup processing completes. If you want to restart the node, make sure to ask the client to stop TFTP access requests until the node startup processing completes.

About real-time virus scanning

File Services Manager can link with a scan server on the network to perform real-time virus scanning and provide notifications of the scan results.

When using the real-time virus scanning functionality, a scan is performed from the scan server on the corresponding file when a CIFS client accesses files in the storage systems or stores files in the storage system.

If a file with a virus is detected, the virus information and the information about the client that has been manipulating the infected file is output to the system log (syslog). If the relevant settings are enabled, the information can be also sent via SNMP traps or email notifications.

Notes on using the real-time virus scanning functionality

Keep the following in mind when using the real-time virus scanning functionality.

Real-time virus scanning operations

The following explains how the real-time virus scanning functionality operates:

- Real-time virus scanning scans the entire file even if the CIFS client has only read or updated a part of the file. This type of scanning is not suitable in an environment in which only parts of files are read or updated, such as in a database environment.
- Real-time virus scanning is performed even if the user only left or right-clicks on a file in Windows Explorer on a CIFS client.
- Real-time virus scanning is performed for ordinary files (as determined by `stat()`). Any other files, such as character device files and FIFO files, will not be scanned. These types of files can still be accessed.
- When a single CIFS client accesses multiple files at the same time, real-time virus scanning is performed for each file. Since the time required to accept all of the CIFS access requests is higher, a timeout might occur while scanning on the CIFS client, which will result in the scan ending with an error. Because this can be a problem, make sure that the CIFS client operates so that multiple files cannot be accessed at the same time. Even if a timeout occurs on a CIFS client, the scanning in the HDI system continues until processing of all of the files being scanned has been completed.
- Real-time virus scanning is not suitable for environments in which Windows roaming user profiles are in use. If roaming user profiles are in use, after the CIFS client finishes logging on or off, processing to browse or update a large number of files in CIFS shares takes place. Real-time scanning is performed on each file, and several tens of milliseconds is required for scanning a 1-KB file. Therefore, if more than several hundred files are to be scanned, scanning takes more than several tens of seconds in total, and logon or logoff processing might seem to be taking a long time.
- 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 the access type for scanning to Read Only.

When an error occurs during real-time virus scanning

Keep the following in mind when an error occurs during real-time virus scanning.

- If an error occurs during real-time virus scanning, even if the scan for a file has not finished, the file might still be stored in a CIFS share, depending on the settings. If an error occurs during real-time virus scanning, an SNMP trap or email notification is sent. The system

administrator must check the error information. If the error is caused by the configuration of the settings for the real-time virus scanning or the scan server settings, the system administrator must reconfigure the settings appropriately.

- An error that occurs during real-time virus scanning might not be reported to the CIFS client, depending on the application that the CIFS client is using. If the CIFS client reports that a file was not copied correctly or that data was not properly updated, the system administrator must check the error information to confirm that there is neither a virus nor a scanning error.
  - From the **Scan Conditions** page of the **Virus Scan Server Configuration** dialog box, if in **Procedure if scanning fails**, **Deny access** is selected, and a scan fails after a CIFS client has copied some files, the copied files will be deleted from the storage system.

    If a scan fails after a CIFS client has updated some files, the updates will be canceled and the files will be returned to their original state.
  - From the **Scan Conditions** page of the **Virus Scan Server Configuration** dialog box, if in **Maximum size for scanning**, the **Permit access to files that have exceeded the maximum size** check box is not selected, and the CIFS client copies files whose size exceeds the value specified in **Maximum file size**, the copied files are deleted once they have been copied.

    If the file size when the CIFS client updates a file exceeds the value specified in **Maximum file size**, the update will be canceled the file is returned to its original state.
  - If **Deny access** is selected in **Method of dealing with infected file** on the **Scan Conditions** page of the **Virus Scan Server Configuration** dialog box when files copied by the CIFS client have viruses, the copied files will be deleted from the storage system.

    If files updated by a CIFS client have viruses, the updates will be canceled and the files will be returned to their original state.
- If a timeout or error occurs while attempting to connect to a scan server, a different scan server will be selected and used, according to the value specified on the **Scan Conditions** page in the **Virus Scan Server Configuration** dialog box, so that real-time virus scanning can continue. However, if an error occurs in a scan server during a scan, real-time virus scanning will end and no other scan servers will not take over for the one where the error occurred. When a CIFS client accesses a file, if the scan operation fails, the way the system reacts is determined by the action that was specified on the **Scan Conditions** page in the **Virus Scan Server Configuration** dialog box.
- If the file path accessed by a CIFS client contains special characters, a real time scan might not finish successfully. In such a case, if necessary, change the file path to a path that does not contain any special characters and then run the scan again.

Temporary files

Depending on the virus-scanning conditions, Symantec virus scan software, McAfee virus scan software, and Trend Micro InterScan Web Security Virtual Appliance sometimes create temporary files. The operation notes when creating temporary files are shown below.

- If **Read and write** or **Write only** has been specified for **Scan timing** on the **Scan Conditions** page of the **Virus Scan Server Configuration** dialog box and one of the following settings is specified, a temporary file will be created. The file, which is created in the same folder as that of the file to be scanned, is used in the event that a file gets infected when it is updated or when a virus scanning error occurs.
  - In **Method of dealing with infected file**, **Deny access** is selected.
  - In **Maximum size for scanning, Specify** is selected and the **Permit access to files that have exceeded the maximum size** check box is not selected.
  - In **Procedure if scanning fails**, **Deny access** is selected.

  The naming convention used for temporary files is:

  `.ava`*`process-id`*`unique-string_name-of-scan-target-file_`bak

  The variable *process-id* is 5 characters long, and the *unique-string* is 6 characters long.

  When the CIFS client updates files and real-time virus scanning operates, the amount of free space on the file system must not be less than the size of the files to be scanned. If free space is insufficient, files cannot be updated.
- If a system error occurs, sometimes a temporary file will remain. If too many temporary files remain, it might cause a problem with the available disk space. Check whether the file to be scanned has been infected by a virus or the data has been damaged, and then delete or restore the file.
- The length of the created temporary file will be 20 characters longer than the name of the file to be scanned. Therefore, if the length of the file path to the temporary file is longer than the allowable maximum for Windows (255 characters), sometimes the temporary file cannot be accessed. If the temporary file cannot be accessed, adjust the name of the parent folder so that the length of the file path becomes 255 characters or less, and then delete or restore the temporary file.
- If the Details pane of Explorer is enabled on the CIFS client, files are opened and scanned in real time to obtain the information to be displayed in the Details pane. If you configure the system to create temporary files, every time a temporary file is created or deleted, the file to be displayed in the Details pane of Explorer (the file selected on Explorer) is opened to re-obtain the information, and the target file is repeatedly scanned.

  If you configure the system to create temporary files, we recommend that you disable the Details pane, or change the configuration definition of the CIFS service by using the `cifsoptset` command to set `change_notify` to `no` in order to prevent the file that will be displayed in the Details pane from being internally opened.

WORM files

Keep the following in mind when scanning WORM files:

- Because the data in WORM files is not updated, the WORM files are not scanned by default. If you want to scan all files when a scan server is replaced or virus definition files are updated, you can specify the scanning of WORM files. For details about how to specify the scanning of WORM files, see the *CLI Administrator's Guide*.
- If an infected WORM file is detected, the files within the retention period cannot be deleted.
- A WORM file infected with a virus cannot be restored even if the virus detected during scanning can be corrected by the scan server. Accordingly, access from a client to the infected WORM file is rejected regardless of the specified scan conditions. If you need the contents of the infected file, specify **Write only** for **Scan timing**, and then copy the file. The copy of the file is restored and can be viewed from the client.

Stub files

Scanning stub files might take some time because data must be recalled from the HCP to an HDI system. Stub files are scanned by default. You can specify the setting that disables the scanning of the stub files. For details about this setting, see the *CLI Administrator's Guide*.

Managing the Anti-Virus Enabler library trace log file (antiviruslib.trace)

The Anti-Virus Enabler library trace log file (`antiviruslib.trace`) contains the paths to all of the files that will be scanned. Because the file paths contain CIFS client user information, be sure to properly take care of and manage the Anti-Virus Enabler library trace log file.

You can download the Anti-Virus Enabler library trace log file from the **List of RAS Information** page (for `Batch-download`) of the **Check for Errors** dialog box.

Displaying the number of logged-in CIFS clients

When using Trend Micro ServerProtect, the number of logged-in CIFS clients and the number of current sessions for MIB information, which are displayed for **Current number of CIFS login clients** in the **CIFS Service Maintenance** page of the **Access Protocol Configuration** dialog box, includes the number of the registered scan server.

Notes on registering a scan server

If too many virus-scanning requests are sent to a single scan server, virus scanning on the scan server might fail. If the performance of real-time virus scanning deteriorates, adjust the setting so that a sufficient number of scan servers are available in an HDI environment. For details about planning real-time virus scanning operations, see Planning real-time virus scanning operations on page 4-69.

Anti-Virus Enabler uses the server (from among all of the registered scan servers) executing the smallest number of virus scanning processes. Therefore, you can prevent a virus scanning failure by increasing the number of registered scan servers, which will distribute the load among all of the scan servers.

The required number of scan servers varies depending on environment factors, including the type or size of files to be scanned, the number of clients that access the HDI system simultaneously, and system requirements for a scan server. When designing a system, make sure that a sufficient number of scan servers are available in the HDI system environment.

In addition, we recommend that, regardless of environment factors, you register two or more scan servers, so that if an error occurs on one, you can still use the other one.

Reference:

For a scan server with the following specifications, if 2,000 or more virus-scanning requests occur at the same time for 100 KB of plain text, or if 60 or more virus-scanning requests occur at the same time for a compressed file of 15 MB (30 MB after decompression), virus scan processing on the scan server might fail:

CPU: Intel (R) Core(TM)2 Duo 2.4GHz

Memory: 2 GB

Scan server settings: Default

Planning real-time virus scanning operations

When real-time virus scanning is enabled, things like creating temporary files and transferring files to scan servers will occur each time any sort of operation is performed on a file in a CIFS share. As a result, the performance of the entire HDI system will go down when compared to the CIFS service operating while the real-time virus scanning functionality is disabled.

The performance of real-time virus scanning can also decrease as a result of file system usage and changes in the network environment. Real-time virus scanning performance is affected by the number of performed scans, the types and sizes of files that are scanned, the overall load on the HDI system, the network status, scan server performance, and the number of scan servers.

When real-time virus scanning performance decreases, connection errors for scan servers and scan timeouts are much more likely to occur. In addition, it might take a little longer than usual to perform operations on a file in a CIFS share.

The system administrator must therefore check log files and other information and review the hardware configuration or adjust the scanning conditions to ensure the continued efficient operation of an HDI system when using the real-time virus scanning functionality.

Problems caused by a decrease in the performance of real-time virus scanning

A decrease in the performance of real-time virus scanning causes the following problems in an HDI system:

- Scan timeouts occur frequently.
- Connection errors occur frequently for scan servers.
- File operations take longer.

The system administrator can detect a decrease in the performance of real-time virus scanning based on the SNMP traps, email notifications, or notifications received from CIFS clients regarding the decrease in system performance.

Checking the scanning conditions and log files

To identify the cause of a decrease in the performance of real-time virus scanning, you need to check the scanning conditions and collect the log files.

Use the **Scan Conditions** page of the **Virus Scan Server Configuration** dialog box to check the information specified for the scanning conditions, such as the scan timeout period and the types of files that are scanned. You can download the log files you need to identify the cause of the decrease in performance from the **List of RAS Information** page (for `Batch-download`) of the **Check for Errors** dialog box.

The following table describes problems that might occur when there is a decrease in the performance of real-time virus scanning and the information you need to check in the log files.

Table 4-7 Information that must be checked when there is a decrease in the performance of real-time virus scanning

Problem	Log file	Information to be checked
Frequent scan timeouts	Report information file (`/enas/log/antivirus_report.csv`)#1	• Size of the file for which a scan timeout occurred • Name of the scan server used
	User statistics file (`/enas/log/antivirus_stat.csv`)#1	• Number of times a connection could not be established • Number of times a scan timeout occurred • Scanning throughput
	System activity data#2	Network usage rate
Frequent connection errors to scan servers	Report information file (`/enas/log/antivirus_report.csv`)#1	• Size of the file for which a scan timeout occurred • Name of the scan server used

Problem	Log file	Information to be checked
	User statistics file (`/enas/log/antivirus_stat.csv`)#1	• Number of times a connection could not be established • Number of scan timeouts
	System activity data#2	Network usage rate
Slow file operations	Report information file (`/enas/log/antivirus_report.csv`)#1	• Size of the file for which a scan timeout occurred • Name of the scan server used
	User statistics file (`/enas/log/antivirus_stat.csv`)#1	• Number of times a connection could not be established • Time required for creating a temporary file • Size of a created temporary file • Number of scan timeouts
	System activity data#2	• Network usage rate • Amount of I/O for the disk drive

#1:

Included in the Anti-Virus Enabler log group.

#2:

Included in the system activity data log group. An environment in which sar log files can be analyzed is required to check the data in the logs.

For details about the information output to the report information file, see Checking the report information file (antivirus_report.csv) on page 4-71. For details about the information output to the user statistics file, see Checking the user statistics file (antivirus_stat.csv) on page 4-75.

Checking the report information file (antivirus_report.csv)

Information about a file in which an error occurred during real-time virus scanning, such as a file for which scanning has not been completed due to the scan server settings or a file infected with a virus, is output to the report information file (`antivirus_report.csv`). By checking the report information file, you can obtain information about the files that might be infected, thereby understanding the causes and tendency of errors that occur during real-time virus scanning.

Check the report information file to identify the files in which errors occurred during real-time virus scanning, and then take the necessary action. After action has been taken, scan these files again.

You can use an SNMP trap or email notification to report that the report information file has been updated. You can also specify whether to send a

notification each time the report information file is output or whether to send a notification once a day at a specified time. Notification of updates is disabled by default. For details about how to change the SNMP trap notification method, see the *CLI Administrator's Guide*.

The following shows an output example of the report information file.

```
Date,Factor,FilePath,PID,AdditionalInfo
Tue Jun 22 15:01:03 2010,container violation,"/mnt/test/long.zip",
27372,"ViolationInfo = Container extract time violation - scan incomplete.,
ScanServer = 10.213.89.12"
Tue Jun 22 15:14:29 2010,container violation,"/mnt/test/level5.zip",
32386,"ViolationInfo = Container depth violation - scan incomplete.,
ScanServer = 10.213.89.12"
Thu Aug  5 08:48:08 2010,container violation,"/mnt/test/sample.doc",
4900,"ViolationInfo = Container size violation - scan incomplete., ScanServer
= 192.168.10.60"
Wed Jul 28 06:14:30 2010,virus found,"/mnt/test/eicar.txt",6142,"Action = The
infected file has been deleted."
Wed Jul 28 07:59:21 2010,virus found,"/mnt/test/hydra.com",30971,"Action = The
infected file has been repaired."
Wed Jul 28 02:19:30 2010,server connect error,"/mnt/test/1M.txt",24483,""
```

The following table describes the information that is output to the report information file.

Table 4-8 Information output to the report information file (antivirus_report.csv)

Item	Description
`Date`	The time that the file information was obtained, in *MM DD hh :mm:ss* format

`Factor`	The cause of the real-time virus scanning error.
	`scan size exceeded`
	The size of the scanned file exceeded the limit.
	`scan timeout`
	A scan timeout occurred.
	`Internal error`
	An error occurred during internal processing.
	`server connect error`
	An attempt to establish a connection with the scan server failed.
	`container violation`
	The container file could not be scanned due to the scan server settings.
	`server too busy`
	The scan server could not perform a scan due to too many scan requests.
	`Scan server error`
	An error occurred on the scan server.
	`virus found`
	An infected file was detected.
	`Suspected virus`

Item	Description
	An infected file was detected, or virus scanning terminated abnormally. Access to a file from a client was blocked. It is output when an access from a client to a file is blocked due to the scan server setting.
FilePath	The path to the file in which an error occurred during real-time virus scanning
PID	The process ID of the CIFS client that accessed the file
AdditionalInfo	Additional information. FileSize If a scan timeout occurred, the size of the file for which scanning timed out is output. ScanServer If a scan timeout occurred, if the container file could not be scanned, if the scan server could not perform operations, or if an error occurred on the scan server, the IP address or host name of the scan server is output. ViolationInfo If the container file could not be scanned, the cause is output. This cause depends on the scan policies set by using scan software. ErrorInfo If an error occurred on the scan server, the contents of the error are output. For details about the output information, see Table 4-9 Information output as additional information (ErrorInfo) in the report information file when an error occurs on page 4-73. Action The taken action is output when a virus infected file is detected, or an access from a client to a file is blocked due to the scan server setting. For details about the output information, see Table 4-10 Information output as additional information (Action) in the report information file when an infected file is detected on page 4-74.

Table 4-9 Information output as additional information (ErrorInfo) in the report information file when an error occurs

Item	Description
No scanning software is installed.	No virus scan software is installed on the scan server.
The scanning software service has stopped.	The virus scan software service has stopped.
No information about the CIFS share access user is registered.	The user information for CIFS share access is not registered on the scan server.

Item	Description
The information about the CIFS share access user is incorrect.	The user information for CIFS share access that is registered on the scan server is invalid.
An internal processing error occurred on the scan server.	An internal error occurred on the scan server.

Table 4-10 Information output as additional information (Action) in the report information file when an infected file is detected

Item	Output when:
The infected file has been repaired.	The infected file is repaired.
The infected file has been rolled back.	The infected file is replaced with the version of the file (contained in a temporary file) existing before the infection.
The infected file has been deleted.	The infected file is deleted.
A setting allowed access to the file.#	Access from the client to the infected file is permitted in accordance with the scan conditions because the infected file cannot be repaired.
A setting denied access to the file.#	Access from the client to the infected file is rejected in accordance with the scan conditions because the infected file cannot be repaired.
The file is a protected file and cannot be repaired.	The infected file cannot be repaired because the file is a WORM file, or because the file is a non-WORM file that cannot be updated or deleted.
The file is a protected file and cannot be rolled back.	The infected file is a WORM file and cannot be replaced with the previously existing version of the file (contained in a temporary file).
The file is a protected file and cannot be deleted.#	The infected file cannot be deleted because the file is a WORM file within the retention period, or because the file is a non-WORM file that cannot be updated or deleted.
No action taken.#	An infected file that cannot be repaired remains because the scan conditions do not permit any action to be taken.
The blocked file has been deleted.	It is output when a file that is blocked due to the scan server setting is deleted.
The blocked file has been rolled back.	It is output when a file that is blocked due to the scan server setting is replaced with the file of before update.

#

If an access from a client to a file is blocked due to the scan server setting, the action same as that taken at infected file detection is taken.

Checking the user statistics file (antivirus_stat.csv)

Information such as the number of times real-time virus scanning is performed and the scanning throughput is output to the user statistics file (`antivirus_stat.csv`). By checking the user statistics file, you can understand how real-time virus scanning is being used and obtain the information required for improving real-time virus scanning performance.

The user statistics file is not output by default. For details about how to set the `avaconfedit` command to output the user statistics file, see the *CLI Administrator's Guide*. Note that because the user statistics file is output periodically, the performance of real-time virus scanning might be affected. Revise the setting if necessary.

The following shows an output example of the user statistics file.

```
StartTime,EndTime,PID,IPAddress,ScanCount,AvoidScanCount,CacheHit,Throughput,Cr
eateBackupTime,CreateBackupSize,ConnectRetry,ScanTimeout,RequestOpen,RequestClo
se
Thu Aug 19 09:21:17 2010,Thu Aug 19 09:25:20
2010,16776,10.213.77.238,0,16,0,0,0.000,0,0,0,16,0
Thu Aug 19 09:26:15 2010,Thu Aug 19 10:23:04
2010,20868,10.213.77.238,0,35,0,0,0.000,0,0,0,32,3
```

The following table describes the information that is output to the user statistics file.

Table 4-11 Information output to the user statistics file (antivirus_stat.csv)

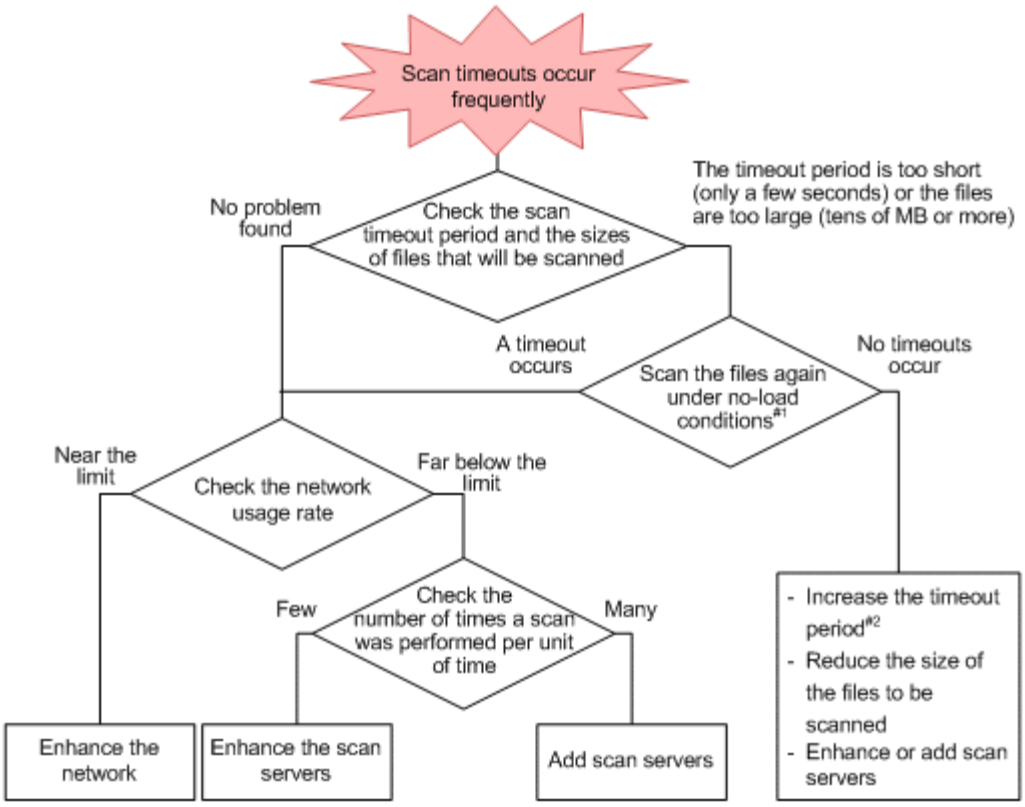
Item	Description
`StartTime`	The time that the collection of information started, in *MM DD hh*:*mm*:*ss* format
`EndTime`	The time that the collection of information ended and the information was output to the user statistics file, in *MM DD hh*:*mm*:*ss* format
`PID`	The process ID of the process that output the information
`IPAddress`	The IP address of the CIFS client
`ScanCount`	The number of times real-time virus scanning was performed
`AvoidScanCount`	The number of times real-time virus scanning was skipped due to the scan conditions
`CacheHit`	The cache hit ratio (unit: %)
`Throughput`	The real-time virus scanning throughput (unit: KB/second)
`CreateBackupTime`	The total time required for creating a temporary file (unit: second)
`CreateBackupSize`	The total size of the created temporary file (unit: MB)
`ConnectRetry`	The retry count for connecting to the scan server
`ScanTimeout`	The number of times scanning timed out
`RequestOpen`	The number real-time virus scanning requests when a file was referenced

Item	Description
RequestClose	The number of real-time virus scanning requests when a file was updated

Determining how to improve the performance

After collecting the required information, the system administrator needs to determine how to improve the performance of real-time virus scanning based on the cause of the decrease in performance.

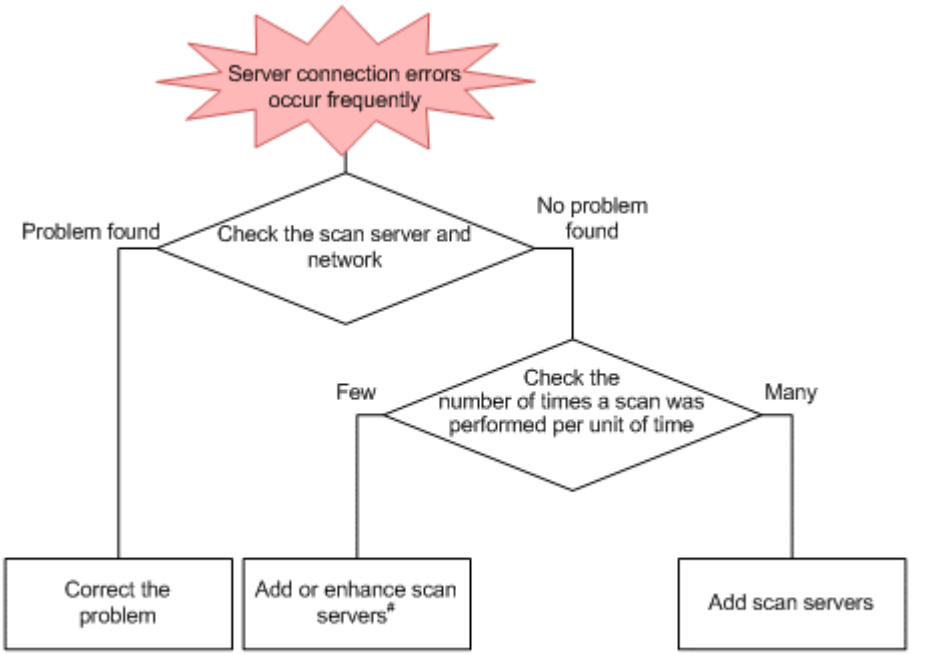
Figure 4-23 Flowchart for improving the performance of real-time virus scanning (when scan timeouts occur frequently) on page 4-76 to Figure 4-25 Flowchart for improving the performance of real-time virus scanning (when file operations take a long time) on page 4-77 are flowcharts that can be used for improving the performance of real-time virus scanning according to the type of problem that occurred.



#1: When you keep indexes for the network and scan server processing times, you can use them to make sure that the timeout period is sufficient for the file size without having to scan the files again.

#2: Even when the timeout period is increased, a timeout might occur on the CIFS client. In this case, you will need to change the maximum size of the files that will be scanned, so that it is smaller than the file that caused the scan timeout, or else enhance the scan servers.

Figure 4-23 Flowchart for improving the performance of real-time virus scanning (when scan timeouts occur frequently)



#: The low number of scans might be a result of long queues caused by the low performance of the scan servers. The scan servers might need to be enhanced.

Figure 4-24 Flowchart for improving the performance of real-time virus scanning (when connection errors occur frequently for scan servers)

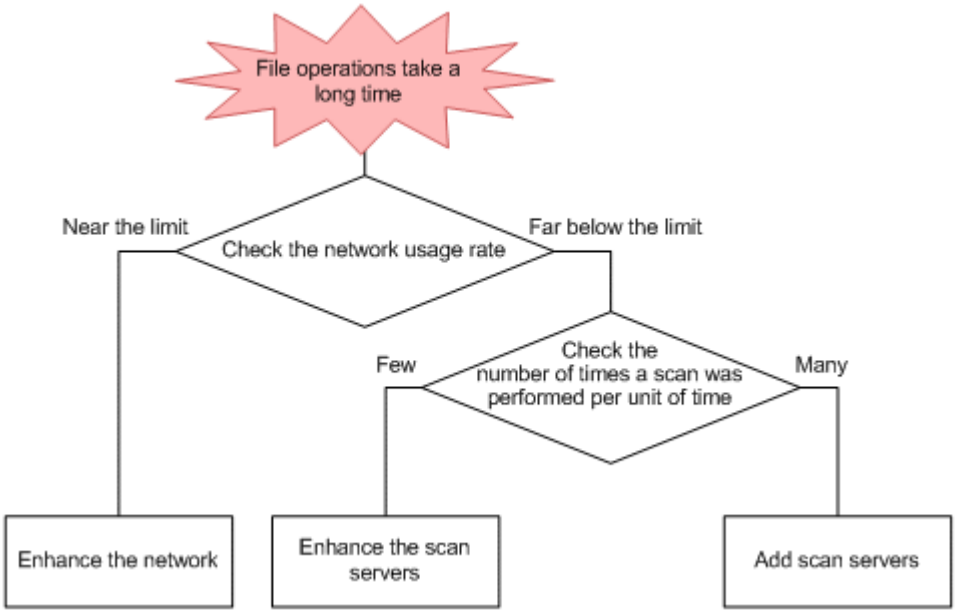


Figure 4-25 Flowchart for improving the performance of real-time virus scanning (when file operations take a long time)

Keep the following in mind when attempting to improve the performance of real-time virus scanning:

When adding scan servers

If errors occur frequently because connections with scan servers cannot be established, there might not be enough scan servers. In this case, add scan servers after reviewing the types and sizes of files that will be scanned, the number of clients that will concurrently access the HDI system, and the machine requirements for the scan servers.

When enhancing scan servers

When connections for scan servers can be established without any problems and the network usage rate is far below the limit, the processing efficiency of the scan servers might be insufficient. In this case, enhance the scan servers to meet the operation needs of an HDI system. For the relation between the processing efficiency of scan servers and the time required for scanning viruses, contact your scan software vendor.

When enhancing the network

If the network usage rate is near the limit and the scanning throughput has decreased, a decrease in network performance is affecting the performance of real-time virus scanning. In this case, enhance the network to ensure that it can handle the traffic necessary for an HDI system.

If you add or enhance the scan servers or enhance the network, but the performance does not improve, revise the scanning conditions. Revising the scanning conditions can reduce the load on the HDI system and improve real-time virus scanning performance. For details on revising the scanning conditions, see Revising the scanning conditions for the real-time virus scanning functionality on page 4-78.

Revising the scanning conditions for the real-time virus scanning functionality

The system administrator can revise the scanning conditions in the **Scan Conditions** page of the **Virus Scan Server Configuration** dialog box to improve the performance of real-time virus scanning. To do so, download the log files from the **List of RAS Information** page (for `Batch-download`) of the **Check for Errors** dialog box and change the settings so that the real-time virus scanning functionality runs effectively.

Increasing the cache size

When you are using Symantec virus scan software, McAfee virus scan software, or Trend Micro InterScan Web Security Virtual Appliance, you can reduce I/O load on the HDI system by efficiently using the cache that stores information about files determined to be free of viruses.

The system administrator must check the cache hit rate in the user statistics file and, if the cache hit rate is low, increase the cache size specified for **Cache size of scanning result**. Note that an HDI system is able to cache information for approximately 430 files with 1 MB.

Increasing the scan timeout period

If scan timeouts occur frequently when network usage is low, increasing the period of time before a timeout occurs can reduce the timeout frequency. The system administrator must check the log files for system activity data and, if network usage is low, increase the scan timeout periods specified for **Connection time-out period** and **Scanning time-out period**.

Reducing the number of times a virus scan is performed

In the default scanning conditions, **Read and Write** is the condition for performing virus scanning. By setting **Read only** or **Write only**, you can reduce the number of times virus scanning is performed.

When **Read only** is set:

Since virus scanning is performed when a file is being accessed, CIFS clients will not be infected.

However, infected files might be stored in the storage system.

When **Write only** is set:

Since virus scanning is performed when a file is being updated, infected files will not be stored in the storage system.

However, even when virus definition files are up to date, a virus undetectable during scanning might be sent to a CIFS client.

Suppressing the creation of temporary files

When you are using Symantec virus scan software, McAfee virus scan software, or Trend Micro InterScan Web Security Virtual Appliance, temporary files are created in the same folder as the files to be scanned, in case files are infected or a virus scan error occurs during an update.

You must use the user statistics file to check the times at which temporary files were created and the sizes of such files. You must also use the system information log files to check the amount of disk drive I/O. If the I/O load on the disk drive has increased due to the creation of temporary files, you can reduce the load by suppressing the creation of temporary files.

To suppress the creation of temporary files, specify scanning conditions as follows:

When **Read only** is set for **Scan timing**:

Temporary files are not created, regardless of the other settings.

When an item other than **Read only** is set for **Scan timing**:

Temporary files are not created when the following items are specified:

- In **Method of dealing with infected file**, set **Delete the file** or **Allow access**.#
- When **Specify** is selected for **Maximum size for scanning**, select the **Permit access to files that have exceeded the maximum size** check box.
- In **Procedure if scanning fails**, set **Allow access**.

#:

When **Delete the file** is specified, any infected files that cannot be restored are deleted. Use backup data to restore the file.

Note that when the above settings are applied, files are not restored by using temporary files.

Selecting scan targets

When a CIFS share contains many files whose size exceeds several hundreds of megabytes (MB) or contains files in the gigabytes (GB), increased disk drive I/O can reduce response performance throughout the entire HDI system. In addition, depending on the file type, virus scanning might not be effective.

If problems like these occur, you can reduce the I/O load on the disk drive by selecting scan targets:

Exclude files that have a specific extension from the scan targets

Contact to your scan software vendor to check the types of files for which virus scan is effective. On the **Scan Conditions** page of the **Virus Scan Server Configuration** dialog box, specify extensions to exclude from the scan targets.

Exclude specific files or paths in a CIFS share from the scan targets

If you can identify the large files that cause a scan timeout from the report information file, you can exclude these files and paths from the scan targets. For details on how to exclude specific files or paths in a CIFS share from the scan targets, see the *CLI Administrator's Guide*.

Reducing the sizes of files to be scanned

When you are using Symantec virus scan software, McAfee virus scan software, or Trend Micro InterScan Web Security Virtual Appliance, you can exclude large files from scans by checking the size of the files that caused timeouts from the report information file, and by changing the settings for the size of files to be scanned. In **Maximum file size** of **Maximum size for scanning**, check the sizes of the files to be scanned.

Note that you must consider another method for scanning the files excluded from real-time virus scans. For example, virus scan software is installed on another computer, and then the excluded files are periodically scanned for viruses on the computer.

About system settings

HDI systems provide functionality to recover the system settings saved on *system LUs* (a collective term for a cluster management LU and OS disks on both nodes) in the event of failure.

OS disk

A logical disk area where the OS on the node and programs that run on the OS are stored. One OS disk is allocated per node.

Cluster management LU

An LU, in the storage system, where settings such as those related to a cluster configuration and file system are stored. One cluster management LU is allocated per cluster.

In an HDI system, a batch operation can be used to save system LUs. The system settings files that contain the information extracted from saved system LUs can also be saved to user LUs.

You can manually save system LUs and the system settings files, or can set them to be automatically saved according to a specified schedule. To recover the system LUs if an error occurs, follow the instructions from maintenance personnel and upload the saved system settings file to the node.

Caution:

- You (the system administrator) must download the node settings file to storage media outside the system after specifying the settings required to start HDI system operations, such as defining a cluster configuration or creating a file system.
- While the HDI system is in operation, make sure that you manually download the node settings file whenever you change the configuration of the HDI system.
- If the settings file is not downloaded, the system LUs and storage system might not be recoverable if an error occurs.
- If the latest data for the node settings file is not saved, the system LUs might not be recoverable if an error occurs.
- You cannot save the system configuration information when any of the following conditions apply:
  - A failover occurred in the resource group.
  - A cluster, node, or resource group is stopped or an error has occurred in the cluster, node, or resource group.

For system LUs, only one generation can be retained respectively per cluster.

The system administrator can specify any directory as the location for saving the system settings file. In addition, the system settings file can automatically be saved at specified intervals (periodic saving).

By default, the system settings information are periodically saved every day at 00:07. Make sure that you set the time for periodic saving to a time period during which no jobs of the NDMP functionality are running. Do not execute any commands or perform any GUI operations when periodic saving of the settings takes place.

Locations in which the system settings file is saved when saved manually

When the system settings file is saved manually, it is saved in a location specified by the system administrator and in another location (the system LU or the SSH account's home directory (`/home/nasroot`)), which differs according to the configuration of the system. The following table describes the locations in which the system settings file is saved when it is saved manually.

Table 4-12 Locations in which the system settings file is saved when saved manually (for cluster configurations)

Specified location	Location of the system settings file				
	HCP	User LU	System LU	Home directory	Management console
HCP	Yes	--	Yes	--	--
User LU	--	Yes	Yes	--	--
System LU	--	--	Yes	--	--
Home directory	--	--	Yes	Yes	--
Management console	--	--	Yes	--	Yes

Legend: Yes = Saved, -- = Not saved

Table 4-13 Locations in which the system settings file is saved when saved manually (for single node configurations)

Specified location	Location of the system settings file				
	HCP	User LU	FTP server	Home directory	Management console
HCP	Yes	--	--	--	--
User LU	--	Yes	--	--	--
FTP server	--	--	Yes	--	--
Home directory	--	--	--	Yes	--
Management console	--	--	--	--	Yes

Legend: Yes = Saved, -- = Not saved

Locations in which the system settings file is saved when saved periodically

When the system settings file is saved periodically, it is saved in the location specified by the system administrator and in another location (the system LU

or the SSH account's home directory (`/home/nasroot`)), which differs according to the configuration of the system. The following table describes the locations in which the system settings file is saved when it is saved periodically.

Table 4-14 Locations in which the system settings file is saved when saved periodically (for cluster configurations)

Preset location	Location of the system settings file		
	HCP	User LU	System LU
HCP#	Yes	--	Yes
User LU#	--	Yes	Yes
System LU	--	--	Yes

Legend: Yes = Saved, -- = Not saved

#

Even if the system settings file cannot be saved in the preset location, the file is saved on the system LU.

Table 4-15 Locations in which the system settings file is saved when saved periodically (for single node configurations)

Preset location	Location of the system settings file			
	HCP	User LU	FTP server	Home directory
HCP#	Yes	--	--	Yes
User LU#	--	Yes	--	Yes
FTP server#	--	--	Yes	Yes
Home directory	--	--	--	Yes

Legend: Yes = Saved, -- = Not saved

#

Even if the system settings file cannot be saved in the preset location, the file is saved on the home directory.

About errors

In the event of a failure in an HDI system, the system administrator must obtain and review the error information from the management server and the nodes.

By using SNMP, you can send traps that contain messages indicating, for example, error information. If either the KAQG46040-E or the KAQG46041-W message was received, please contact maintenance personnel. Also, please

regularly obtain from the SNMP manager the MIB information for both of the nodes, and make sure that the nodes are reachable.

You can also use email error notifications to send error information to the email addresses specified in the `/enas/conf/email_alert.conf` email alert file.

Note that, if a node stops because of an error in the output of a log file or a core file, garbled text might be output.

For details about how to use SNMP or email notifications, see the *Administrator's Guide*.

For details about messages sent by using SNMP traps or emails, see the manual *Error Codes*.

Error information on the management server

Hitachi Command Suite Common Component and the Hitachi File Services Manager both write log files to the management server.

Hitachi Command Suite Common Component log files:

- Integrated trace log file
- Event log

Hitachi File Services Manager log file:

- Message log

The system administrator can change various log file settings, such as the maximum size or output level of the Hitachi File Services Manager trace log.

Node error information

If an error occurs in an HDI system or a user performs an improper operation, log files such as the system messages and system log data, along with the core file will be output.

You can use the File Services Manager GUI to view, download, or delete error information on the nodes.

The system administrator can specify the number and size of log files to save, and the amount of time to save the core file.

About monitoring systems with SNMP

The SNMP manager installed in the management LAN as an external server can obtain MIB objects as system operating information from SNMP agents in an HDI system. You can also send traps to the SNMP manager that contain messages indicating, for example, error information.

For the HDI system, use SNMPv2 or SNMPv3. If you use SNMPv1, some information cannot be obtained.

For details about the environment settings for the SNMP manager, see Environment settings for the SNMP manager on page 3-30.

For details about how to use SNMP in the HDI system and details about MIB objects that can be used, see the *Administrator's Guide*.

About importing data from other file servers

The HDI system can import files and directories from other file servers while minimizing the period in which the services are stopped.

Two methods are provided to import files and directories: all files and directories in the shares of other file servers are imported, or only the files and directories accessed by clients are imported on demand.

When on-demand importing is enabled, only the files and directories to which access is requested are imported when clients access files and directories to be imported. By using an HDI system with the source file servers, the capacity of the file system in an HDI system can be minimized.

When all-data importing is enabled, all files and directories are imported to the HDI system in parallel with on-demand importing regardless of access from clients. All data in the shares can be imported within the period in which an HDI system is used with the source file servers. If you want to remove other file servers, you need to perform all-data import.

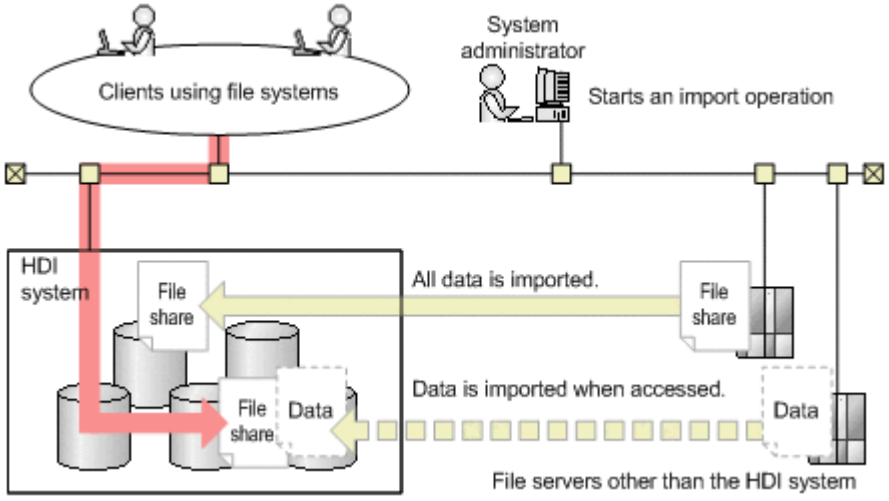


Figure 4-26 Overview of importing from other file servers

If the capacity of an HDI system is insufficient during an import operation, the data being imported from the source file servers to the HDI system will be paused. During that time, the import operation from the HDI system to an HCP system will still continue. After files are turned into stub files and more unused capacity is made available in the HDI system, the data being imported from the source file servers to the HDI system will start again.

System configurations when data is imported from other file servers

The figure below shows an example system configuration when files and directories are imported from other file servers.

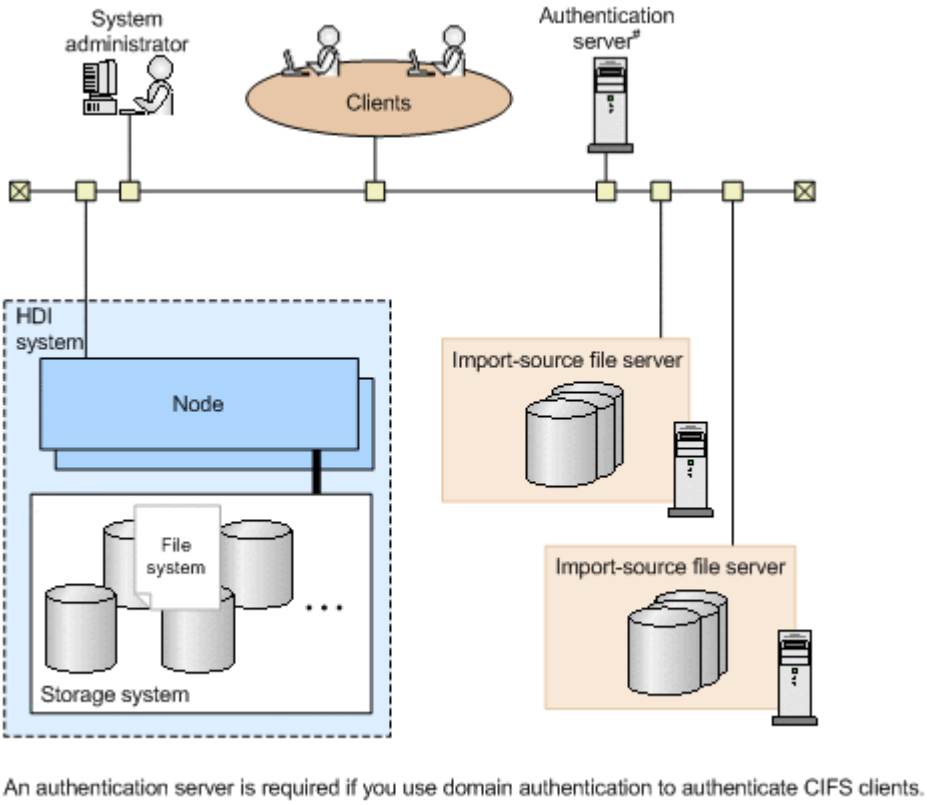


Figure 4-27 Example system configuration when data is imported from other file servers

Both local authentication and domain authentication can be used for CIFS client authentication. For external authentication servers, domain controllers and LDAP servers can be used.

The tasks required for system configuration are as follows:

- Connect the HDI system to the network that can access the source file servers. You can connect multiple source file servers to an HDI node.
- When an LDAP server is used to authenticate users, register the user account associated with the data to be imported to the LDAP server ahead of time.
- If LDAP user mapping is used, the LDAP user mapping information set on the import source must also be set in the HDI system.
- If the NFS protocol is used to import data, use the NFSv2 or NFSv3 protocol.

The tasks required before importing that are related to the import-source file server are as follows:

- Stop client access to the import-source file server.

- Set the file shares of the import source to read-only. If a file-import operation is started while writing is permitted, data might become corrupted.
- Do not use share-level security. Import processing from a file server that uses share-level security will cause an error.

Points to be checked before importing data from another file server

The file system specified as the import destination must meet the following requirements:

- The file system is mounted with read and write permissions granted.
- The file system does not use the WORM functionality.
- The file system shares no data with any other HDI system via a linked HCP system.
- The file system is the Advanced ACL type (when the CIFS protocol is used to import data).

A maximum of 10 KB per file is required in the management area on the target file system. Take this into account when considering the file system capacity.

Check the following points related to operation of the import-destination file system:

- If you want to set subtree quotas for the import-target directories, specify the settings so that only the files and directories accessed by clients are imported on demand for the share that is the highest in the hierarchy, and then start the import operation. After that, set subtree quotas. After setting the quotas, change the import method so that all files and directories are imported.
- When the Backup Restore functionality is used for the target file system, files cannot be accessed unless they have been imported by the time the Backup Restore functionality acquires a backup.

Check the following points related to importing data:

- When a directory that has not yet been imported is accessed for the first time, the data is imported from the import-source file server on demand. If the number of files or directories in the directory is large, importing the data takes a long time. As a result, Explorer or other applications used on the client side might timeout. However, because the import processing will still continue even if a timeout occurs, wait a while until the processing completes, and then access the target directory again.
- For file systems that are importing data, if you perform operations that recursively scan the directory (for example, searching all files, displaying the properties of Explorer, or using the **Show pop-up description for folder and desktop items** function to display pop-ups), the processing takes a long time because data is imported for a large number of

directories on demand. Therefore, do not perform operations that recursively scan the directory. Note that you can disable the **Show pop-up description for folder and desktop items** function by using the **Folder Options** dialog box of Explorer.

- When on-demand imports (for which files and directories are only imported when they are accessed by clients) are enabled, some data might not be imported into the HDI system. When removing source file servers, change the settings in advance so that all files and directories are imported by using the `datamigratestart` command for cluster configurations or by using the GUI or the `datamigratestart` command for single-node configurations.
- If the first character of a file or directory name is a period (.), the hidden-file attribute is applied to the import target.
- If the settings are configured so that only the data accessed by clients is imported, all files in the target file system are managed as files that have the offline attribute. For details about the offline attribute, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.
- When migrating the target-file-system data to the HCP system during import processing, the offline attribute is set for the files that have not been migrated to the HCP system. For details about the offline attribute, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.
- After a file or directory in the target file system is updated, you cannot import the file or directory before an update, even if you perform a re-import.
- If the path name of the file to which data is to be imported exceeds 4,095 bytes, the import fails. Specify a path name that does not exceed 4,095 bytes.

If you are using the CIFS protocol to import data, check the following points:

  - If source file servers are in a Windows environment, you might not be able to access imported files due to the differences in the ACL specifications between Windows and the HDI system. For details on the differences in specifications when user resources are migrated from a Windows environment, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.
  - Specify the shared directory at the highest level as the source CIFS shares. Other CIFS shares under the CIFS shares specified in the import source are imported at the same time.
  - Disable access based enumeration for the import-source CIFS share. If access based enumeration is enabled for the import-source CIFS share, files without access permissions cannot be detected.
  - If a directory in an import-source share is mapped to a client network drive and access from the client is stopped, ask the client to disconnect the network drive. When starting access from a client, ask the client to map the directory in the import-target share to a network drive.
  - When shortcuts are imported, the link destinations of the shortcuts must be changed as necessary. If a client specifies the host name or

IP address of an import-source file server as a link destination, ask the client to change the host name or IP address to the host name or IP address of the target node.

- Even if real-time scanning is set to be performed when CIFS clients update a file, we recommend that you perform virus scans for the files to be imported. For all-data imports, real-time scanning is not performed for the files that are being imported.

  If CIFS clients access files before the import operation is completed, it might take a long time to scan files. If clients access large files, which can cause scans to timeout, consider reducing the maximum size of files to be scanned, or allowing access to the files for which scanning failed. Note that scan timeouts do not affect import operations.
- To import data by using domain authentication, the CIFS service needs to be running. If the CIFS service stops while the data is being imported, the import process might result in an error. In such a case, start the CIFS service, and then import the data again.
- Make sure that the import-source file server supports the versions of the SMB protocol that the CIFS service uses to communicate with file servers. If the file server does not support those versions of the SMB protocol, change the values specified for the options `client_max_protocol` and `client_min_protocol`, of the command `cifsoptset`, that determine the versions of the SMB protocol that the CIFS service uses to communicate with the import-source file server.

If you are using the NFS protocol to import data, check the following points:

- Hard link information is also imported. Imported hard links that are migrated to the HCP system are migrated as one file.
- If hard links exist under an import-source share directory and you want to set a subtree quota under the corresponding import-target share directory, set the subtree quota so that all the hard links are imported under the same subtree quota directory. Hard links are not imported if different subtree quotas are set.
- When importing data from NFS shares on other file servers, if the directory structure to be imported is more than 128 directories deep, import processing may terminate abnormally and fail to import data. To prevent this situation, make sure that the depth of directory structures to be imported does not exceed 128.

If you are migrating the data of the import-destination file system to an HCP system, check the following points:

- Importing of all data stops temporarily, and importing of only the data accessed by HDI from the client takes place if migration occurs during import or if the remaining file system capacity of the import-target falls to or below the threshold specified by the `datamigratelimitset` command (the initial threshold is 10 percent). After migration to HCP finishes, stub processing of files starts and continues until the remaining file system capacity of the import-target reaches or exceeds the threshold for resuming the stopped import of all data (the initial threshold is 20

percent). The stub processing is based on the setting by the `datamigratelimitset` command regardless of the stub processing threshold specified by the `arcreplimitset` command. Ensure that the file system capacity of the import-target is sufficiently larger than the import-source.

- Specify migration tasks after all file and directories are imported, or configure the settings so that a migration is performed on a regular basis during import processing so as not to affect the migration processing time. Note that, if a migration is performed during import processing, the processing to import all the files and directories temporarily stops but the processing to import the files and directories accessed by the HDI system client is performed. After the migration finishes, the processing to import all the files and directories resumes.
- When data that has just been imported is then immediately migrated, files for referencing the data on the import-source server are created in the `.history` directory. These files cannot be referenced if import definition information (which is created when data is imported from another file server) is deleted. If this happens, reference the files created in the `.history` directory after the migration to the HCP system is completed.
- After all files and directories are imported, immediately delete import definition information. If you do not delete import definition information, the processing required to restore data from the HCP system or reference the `.history` directory takes time, because the number of communications increases.

About clients using file systems

This section describes what the system administrator needs to know before clients start using file systems.

Notes on using a file system from an NFS client

Note the following points when you change the settings in the HDI system, you want to use a file system from an NFS client:

- To recreate an HDI system file system mounted from an NFS client, first use the NFS client to unmount the file system, and then after the file system has been recreated, mount it.
- If you delete an NFS share for the HDI system file system mounted from an NFS client, it might not be possible to unmount that file system depending on the implementation of the NFS client. If you cannot unmount the file system, restart the NFS client to release the file system from the mount state.
- Even if you change the attribute of the NFS mount point of the file system to which you mount from an NFS client, the result of the change might not be able to be checked from the NFS client side. In such cases, mount the file system again from an NFS client.

- The NFS client host's administrator must unmount the HDI file system from the NFS client before the HDI system administrator changes the maximum buffer size for the NFS shares. Remount the HDI file system only after the change has been checked.

If a file system is used from an NFS client, there are several things to note in the situations below. For details, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

- When mounting a file system from an NFS client
- When locking a file from an NFS client
- When operating a file system from an NFS client

Notes on using a file system from a CIFS client

For notes on using a file system from a CIFS client, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

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

Note on using a file system from an FTP client

The following are notes on using a file system from an FTP client.

- Use ASCII character encoding for file names and directory names. To perform an operation from an FTP client for a file or directory whose name contains non-ASCII characters, you need to specify a character-encoding scheme for the operating environment on the client that properly displays all of the characters.
- The characters that can be used for the file name are 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 (.), 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. The characters that can be used for the directory name are alphanumeric characters and symbols.
- The maximum length for file names and directory names is 1,023 bytes. In addition, if a file is specified from an FTP client by using an absolute path, the maximum length of the file path that can be specified in the command is 4,095 bytes, including the path of the login directory for the FTP service.
- The maximum size for each file is the same as the maximum size of a file that can be stored in the file system. For the maximum file size that can be stored in the file system, see Appendix I, Maximum Values for HDI on page I-1.

- The number of files that can be created in a directory is the same as the total number of files and directories that can be stored in the file system. For details about the total number of files and directories that can be stored in the file system, see Appendix I, Maximum Values for HDI on page I-1.
- If a failover or failback occurs while an FTP client is accessing a file system that belongs to the target resource group, the connection will be forcibly disconnected or placed in the response-wait status. To restart access to the file system, reconnect to the file system.
- When using the FTP service, an `anonymous` user cannot upload a file if the file name contains non-ASCII characters.
- If the name of a file or directory in the HDI system is *~ftp-user-name*, and that file or directory is specified for the `ftp` command, make sure to specify the file or directory name either with an absolute path or with a relative path starting from a higher level before executing the command from an FTP client.

  If the `ftp` command is executed with only a file or directory name of the format *~character-string* (and without an absolute path or without a relative path starting from a higher level), the following occurs:

  - If *character-string* is a user name registered in an HDI system:

    If the home directory of the specified user is under the FTP login directory, the home directory of the specified user or a file with the same name as the home directory becomes the processing target.

    If the home directory of the specified user does not appear under the FTP login directory, an error occurs.
  - If *character-string* is not a user name registered in an HDI system:

    ~character-string becomes the processing target.
- If a user account registered on the HDI system is used for FTP, the user account is granted the data access permissions that are set for all groups to which the account is assigned, including those for the primary group to which the user account is assigned.
- If the `ftp` command is executed from an FTP client and with only a tilde (`~`) specified for the directory or file name, the FTP login directory becomes the processing target.
- The SFTP service supports SSH2 only.
- For the SFTP service, make sure that the maximum number of clients that can log in simultaneously is 500. If over 500 clients log in simultaneously, the system becomes unstable.

5

Backup Operations in an HDI System

This chapter describes what system administrators must understand and take into consideration before performing backup operations in an HDI system.

- ☐ Overview of the backup functionality
- ☐ Using the NDMP functionality

Overview of the backup functionality

You can use the NDMP (Network Data Management Protocol) functionality provided by Backup Restore, to work together with backup management software (that supports the NDMP functionality) to save file system data to a tape device on the network. This functionality can be used for file systems that do not synchronize with the data of other HDI systems via HCP systems.

If the NDMP functionality is used while applications are using data, consider the integrity of the data that is being used and the data to be backed up or restored.

Using the NDMP functionality

This section contains information for the system administrator to be aware of before using the NDMP functionality.

Overview of the NDMP functionality

In conjunction with backup management software, the NDMP functionality can copy file system data to backup media, and also restore backed up data stored on media to a file system.

Because this functionality is designed to copy data to backup media not in a storage system, you will be able to recover file system data from the copied data even if the hardware in a storage system fails.

The figure below illustrates the NDMP functionality.

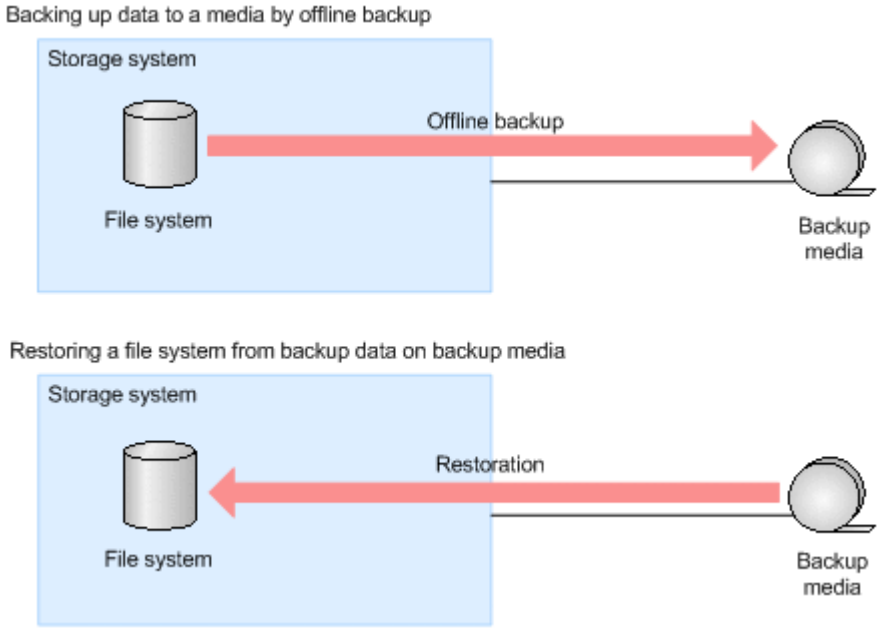


Figure 5-1 Overview of the NDMP functionality

The NDMP functionality supports the following tape devices:

- A tape device connected to the media server
- A tape device connected to a node via a SAN#

#:

This functionality can only be used in cluster configurations.

We recommend that you stop file system operations before performing a backup, but you can also perform a backup for an active file system. In this manual, a backup performed by using the NDMP functionality is called an offline backup.

If an offline backup is performed without stopping file system operations, offline backup processing will continue even if a file is modified or deleted during the offline backup because the accuracy check of the offline backup is not enhanced by default. By changing the conditions for interrupting an offline backup by using the `ndmpfsconfig` command, you can enhance the accuracy check of the offline backup. The differences in offline backup processing operations when the offline backup accuracy check is enhanced and when it is not enhanced are shown below.

- When the accuracy check of an offline backup is not enhanced (default)

  Offline backup processing ends successfully even if a file is modified or deleted during an offline backup. However, the integrity of the backed up files is not guaranteed.

  You can use this setting when you do not want to interrupt offline backup processing even if the offline backup performed at night does not end by the time the workday operations start.
- When the accuracy check of an offline backup is enhanced

  Offline backup processing ends with an error if a file is modified or deleted during an offline backup.

Estimating the capacity of the backup media

You must prepare backup media that can store quota information, inode information, and ACL information, in addition to the directories and files to be backed up. If the capacity of the backup media is insufficient, the backup operation fails and an error occurs. Use the estimated value calculated by the following formula as a guideline, and then prepare a tape device that has sufficient capacity.

When a migration is performed that links to the HCP system, only files that are excluded as migration targets and files that have not been updated since a migration are backed up to media. Therefore, when you consider the capacity of the backup media, subtract the capacity of files that are not backed up to media (files that have not been updated since migration) from the capacity estimated by the formula below. For example, if the percentage of files that are not backed up to the total capacity is 60%, prepare backup media with 40% of the estimated capacity as a rough indication.

Formula for estimating the backup media capacity (Advanced ACL type)

Backup media capacity (units: bytes)

$$= \uparrow \frac{252\,(A+B)+456}{512} \uparrow \times 512 + \left(\uparrow \frac{260\,(G+H)+586}{512} \uparrow \times 512 \right) \times I + \uparrow \frac{2048 + J \times 88}{512} \uparrow \times 512 \times C + D$$

Legend:

↑ ↑ : Round up to an integer
A : Number of users with a file system quota set
B : Number of groups with a file system quota set
C : Total number of directories and files to be backed up
D : Disk volume used for backup target volume (units: bytes)
G : Average number of users with a subtree quota set in each directory immediately below the file system
H : Average number of groups with a subtree quota set in each directory immediately below the file system
I : Number of directories with a subtree quota set
J : Average number of ACE set for the operation of each directory or file

Formula for estimating the backup media capacity (Classic ACL type)

Backup media capacity (units: bytes)

$$= \uparrow \frac{252\,(A+B)+456}{512} \uparrow \times 512 + \left(\uparrow \frac{260\,(G+H)+586}{512} \uparrow \times 512 \right) \times I + \uparrow \frac{2048 + F\ (E+5)}{512} \uparrow \times 512 \times C + D$$

Legend:

↑ ↑ : Round up to an integer
A : Number of users with a file system quota set
B : Number of groups with a file system quota set
C : Total number of directories and files to be backed up
D : Disk volume used for backup target volume (units: bytes)
E : Average number of digits for the operation of user or group names with ACL set
F : Average number of ACLs set for the operation of each directory or file
G : Average number of users with a subtree quota set in each directory immediately below the file system
H : Average number of groups with a subtree quota set in each directory immediately below the file system
I : Number of directories with a subtree quota set

Note that, to check the disk volume used for a backup-target volume and the total number of directories and files to be backed up, use the file system usage and inode usage displayed in the File Services Manager GUI or the values for `Block used(GB)` and `I-node used` displayed by using the `fslist` command.

Data to be backed up or restored

The NDMP functionality backs up the following types of data to media:

- File system information (quota information and WORM function settings)
- Directory and file information (inode, ACL information, and file attributes)
- Directories and files

  Sometimes a directory or file whose path contains one or more linefeed codes is not backed up. To ensure that the directory or file is backed up, we recommend editing the path and removing the linefeed codes.

  Reference note:

  For details on directory and file attributes to be backed up, see Attributes to be backed up on page E-2.

The NDMP functionality allows data backed up to media to be restored to a node that is in the same cluster as the backup target. Data can only be restored within the cluster where the backup target node is located.

When backup data obtained by using NDMP functionality within a file system that supports 64-bit inodes is restored to a file system configured with a version earlier than 4.2.3-03, some files might not be restored.

Recommended time to perform backup and restore operation

To minimize impact on user operations due to service stopping and degradation of response time, we recommend that you perform backup and restore operations when the entire system has a light load.

When performing a backup or restore operation while the client frequently accesses the volume in the storage system (such as file systems), it might take some time before the processing completes.

Performing an incremental backup

The incremental backup method backs up data that has been changed since the previous backup.

There are two types of incremental backup, which are as follows:

Differential-data backup

A differential-data backup backs up all data that has been changed since the previous full backup.

Incremental-data backup

An incremental-data backup backs up data that has been changed since the previous full backup, differential-data backup, or incremental-data backup.

When performing an incremental backup, keep the following points in mind:

- Even if you perform the following operations on directories and files that have not been changed since the previous backup, an incremental backup will not back up those directory and files.
  - Changing a path (moving directories and files)
  - Changing a name

- Deleting

  We recommend that you perform a full backup when the file system configuration has been changed without change to the directories and files. If you do not perform a full backup, you might not be able to recover data from just before the time that an error occurred.

- If a file system or directory in which quota information has been set is specified as a backup source, an incremental backup backs up all quota information.
- Backup Restore manages the incremental backup history information for each file system.

  For example, assume an offline backup was performed at 06:00 for the file system `filesystem01`, in which a file system is specified as the backup source.

  In this case, history information will be recorded as illustrated in the following figure.

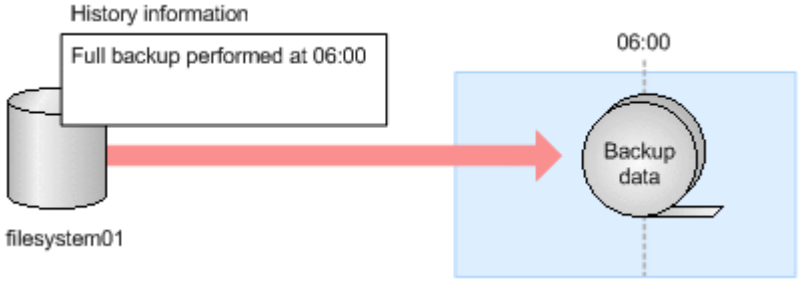


Figure 5-2 Backup history information

History information for `filesystem01` is recorded as an offline backup performed at 06:00.

- For one file system, an incremental backup be performed with one NDMP policy. The following shows an example of an incremental-data backup performed with one NDMP policy.

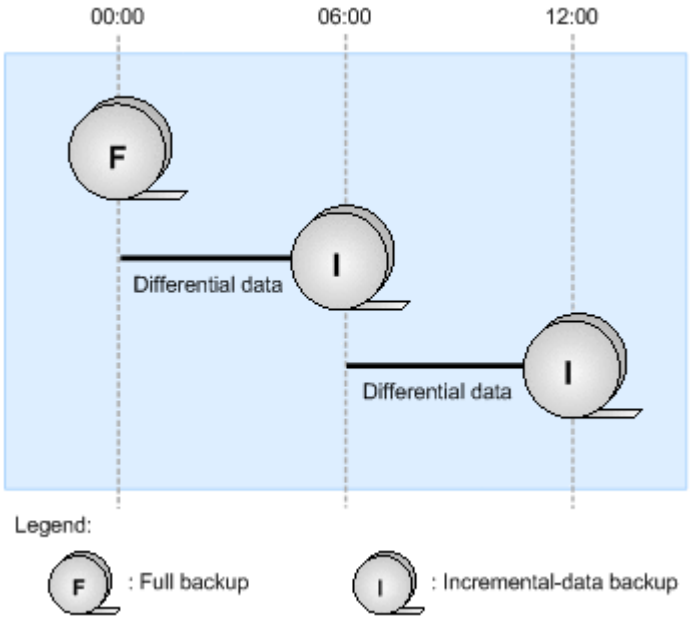


Figure 5-3 Incremental-data backup performed with one NDMP policy

When performing an incremental-data backup with one NDMP policy, the differential data from the previous full backup or incremental-data backup, acquired with the same policy, is backed up. An incremental-data backup at 06:00 will back up the differential data for the period after 00:00. Similarly, an incremental-data backup at 12:00 will back up the differential data for the period after 06:00.

About access control for the NDMP server

Registering the IP addresses and host names of backup servers in the `/etc/hosts` file enables you to restrict the clients that can access the NDMP server to only those backup servers registered in the `/etc/hosts` file. Note that if you do not register any information about backup servers in the `/etc/hosts` file, any client can access the NDMP server. When a client other than a backup server registered in the `/etc/hosts` file attempts to access the NDMP server, the KAQB14211-W and KAQB14213-W messages are output to the NDMP server log (`/enas/log/ndmpserver.log`).

To prevent unauthorized accesses, you can register information about backup servers in the `/etc/hosts` file in the following format, depending on how the HDI system will be used.

IP-address host-name backup-server-name [*host-name-alias* ...]

Backup server names must begin with `BackupServer`. Backup server names can only contain alphanumeric characters and underscores (_). A maximum of 256 information items of backup servers can be registered in the `/etc/hosts` file. If 257 or more items are registered, items from 257 onward are invalid.

The following is an example of adding information items in the /etc/hosts file.

```
#
# BACKUP SERVER ADDRESS
#
10.208.151.19  back-1  BackupServer01
10.208.151.197 back-2  BackupServer02
```

The information registered in the /etc/hosts file is applied to both nodes in the cluster.

Also, after editing the /etc/hosts file, you need to restart the NDMP servers on both of the nodes in the cluster. For details on how to restart an NDMP server, see the *CLI Administrator's Guide*.

Communication path used for backup or restore operations

The communication path between the NDMP server and media server, and the communication path between the NDMP server and backup server are determined based on the routing information set in File Services Manager. Therefore, depending on the set information, communication between the NDMP server and media server, and communication between the NDMP server and backup server might use different ports or paths during backup or restoration.

Operations that cannot be executed during backup or restoration

If you execute the ndmpcontrol command, or if the NDMP server is automatically restarted by executing the ndmpconfig, tapeadd, or tapedel command, the backup or restore operation being performed on the node where you executed the command might terminate with an error.

In addition, when processing is being performed for a backup or restore operation that is using a tape device connected to a node via a SAN, do not perform any of the following operations:

- Executing the tapeadd command on a node#
- Executing the tapelist command in which the -A, -D, or -d option is specified on a node#
- Using the backup management software to perform GUI operations or execute commands that manage tape devices.

#:

If any of these commands are executed on a node on which a backup or restore operation is not being performed, a backup or restore operation being performed on the other node might terminate with an error.

Notes on operations using File Services Manager

Do not perform any of the following File Services Manager operations and a Backup Restore operation at the same time:

- Starting or stopping a cluster
- Performing a forced stop for a cluster
- Changing a cluster configuration
- Starting or stopping a node
- Performing a forced stop for a node
- Starting or stopping a resource group
- Performing a forced stop for a resource group
- Disabling or restarting resource group monitoring
- Changing the execution node of a resource group
- Unmounting the target file system

Doing so might cause the File Services Manager operation or the Backup Restore operation to terminate with an error.

Precautions on starting the OS on a node

When a tape device is connected to nodes via a SAN, the tape device is shared among the nodes. If the OS on one of the nodes is started or restarted, a backup or a restoration being performed on the other node might terminate with an error. When performing a backup or a restoration, make sure that the OS on the other node that shares the tape device is not being started or restarted.

Limitations on the functionality of the backup management software

The NDMP functionality does not support some functionalities provided by backup management software. The following table shows the functionalities (provided by backup management software) that are available to the NDMP functionality.

Table 5-1 Backup management software functionalities and whether they are supported by the NDMP functionality

Functionality		Supported
Backup execution	Manual	Yes
	Automatic (scheduled)	Yes
Backup type	Full backup	Yes
	Cumulative incremental	Yes[#1]
	Differential incremental	Yes[#1]
Backup and restore by[#2]	Volume	Yes

Functionality		Supported
	Directory	Yes
	File	Yes
	Path-based history#3	Yes
Direct Access Recovery (DAR)		Yes
Restore destination	The node that has the volume to be backed up	Yes
	The node for the failover destination	Yes
	Redirected Restore to a different client (a node in another cluster)	--

Legend: Yes = Supported. -- = Not supported.

Note:

Depending on the backup management software used, different functions are available. For details about which the functions are available with which backup management software, see the corresponding documentation.

#1:

In an HDI system, the incremental backup only backs up the directories and files whose contents are modified.

#2:

The maximum length of the path for the directory or file, to be specified for a backup or restore operation, varies depending on which backup management software is used. For details, see the supplementary Backup Restore documentation that is provided with HDI.

#3:

Path-based history is a functionality used for sending file history information from an NDMP server to backup management software during a backup operation. This file history information consists of path names for backed-up directories and files.

Depending on the file history information, you can restore in either directory or file units.

Notes on backing up and restoring WORM file systems

This subsection describes the precautions to take when backing up or restoring a WORM file system.

Notes on backing up a WORM file system

If the autocommit functionality is enabled for a WORM file system, files that have not been accessed by clients since their autocommit intervals have elapsed are not yet WORM files. Any such files are backed up as WORM files.

A WORM file system can be backed up only by performing an offline backup that uses the NDMP functionality.

Notes on restoring a WORM file system

Backup data from a WORM file system can only be restored to the file system from which the data came.

Sometimes, files with the same path in both the backup data and on the restore-destination file system cannot be restored. The following table describes whether a file can be restored when it has the same path in the backup data and in a restore-destination WORM file system.

Table 5-2 Whether a file with the same path in the backup data and in a restore-destination WORM file system can be restored

Type of file in the restore-destination file system		Type of backup data file	
		Normal file	WORM file
Normal file		Yes	Yes
WORM file	The retention period has elapsed.	Maybe#1	Maybe#1
	The retention period has not yet elapsed.	No	Maybe#2

Legend: Yes = Can be restored. Maybe = Restoration might be possible. No = Cannot be restored.

#1:

A file can be restored only if write permission is set for it in the restore-destination file system.

#2:

A file can be restored if the following conditions are met:

- The file data is the same except for the retention period, write permission, and read-only attribute settings.
- The retention period set for the file in the backup data ends at a later date than the retention period set for the file at the restore destination.

6

Linking HDI and HCP

This chapter explains what system administrators must understand or consider before using HDI systems linking with an HCP system as a combined system.

- ☐ Correspondence between file systems and namespaces
- ☐ Functionalities for managing migration
- ☐ Using and operating data migrated to an HCP system
- ☐ Points to be checked before linking an HDI system with an HCP system
- ☐ Referencing the data of another HDI system in read-only mode
- ☐ Performing the roaming of home-directory data among HDI systems
- ☐ Sharing data among HDI systems using the read-write-content-sharing functionality
- ☐ Recovering HDI systems by restoring HCP data

Correspondence between file systems and namespaces

By linking an HDI system to an HCP system, you can migrate HDI data to an HCP namespace according to the tasks set by the system administrator. An HDI system can share data with another HDI system via a linked HCP system through the following methods:

- Referencing data from another HDI system as read-only.
- Enabling roaming among HDI systems for the data from the home directory created for each end user.
- Sharing data among HDI systems using the read-write-content-sharing functionality.

To link with an HCP system, you must assign one HCP tenant to each HDI system. You must also assign one migration-destination namespace to each HDI file system or each file share immediately under the mount point. To share data with another HDI system via a linked HCP system, you must assign the same namespace to multiple HDI systems. If the data-sharing method differs between the HDI systems, the same namespace cannot be assigned.

The following figure shows the correspondence between HDI file systems and migration-destination namespaces.

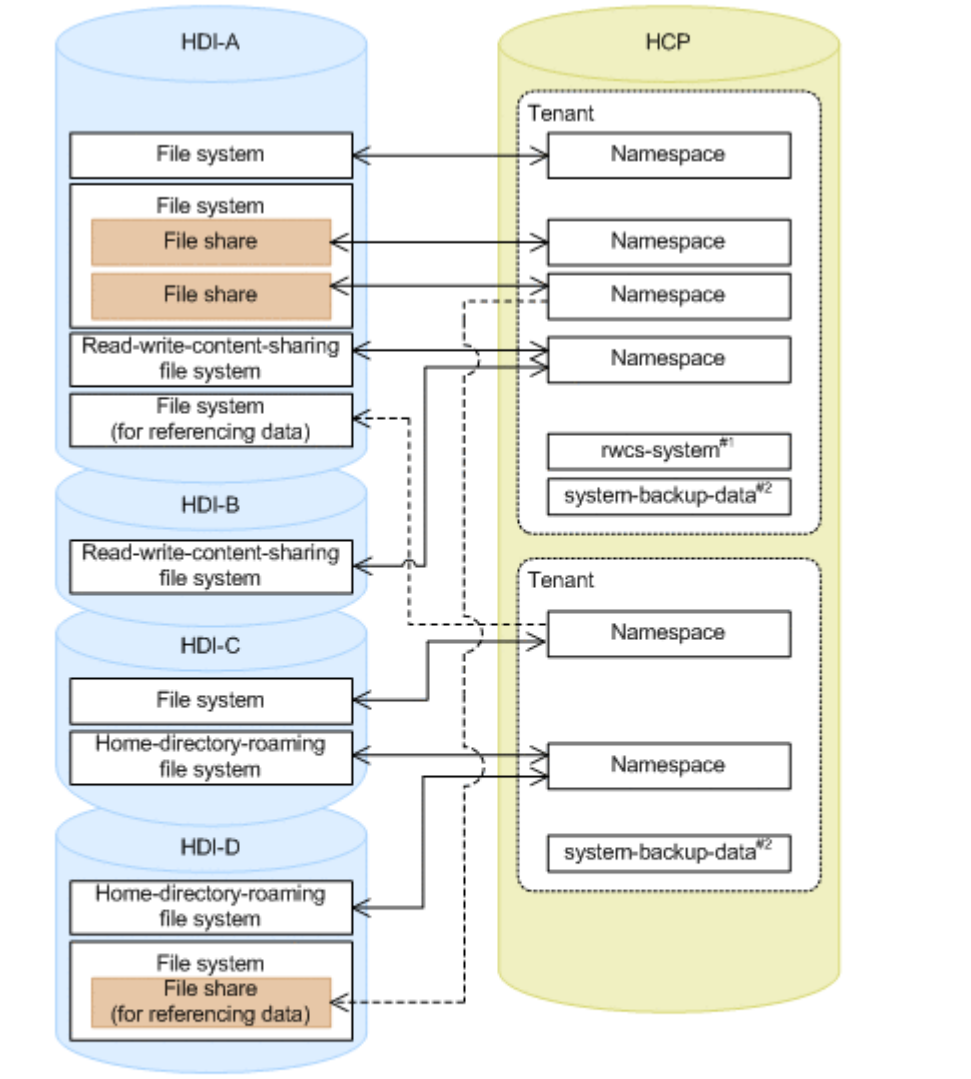


Figure 6-1 Correspondence between file systems, tenants, and namespaces

Functionalities for managing migration

This section describes functionality for managing migration from an HDI system to an HCP system.

Data migration to an HCP system

System administrators must define the migration conditions in the policy (migration policy) for each file system. The defined policy is executed according to the schedule specified as a migration task. The data of the specified files on the file system is migrated to an HCP system based on the schedule defined in the policy.

Before migration starts, the data of the specified files is copied to the work space created for each file system. Because the data copied to the work space is migrated to the HCP system, files can be modified during the migration without affecting the processing (Active File Migration functionality).

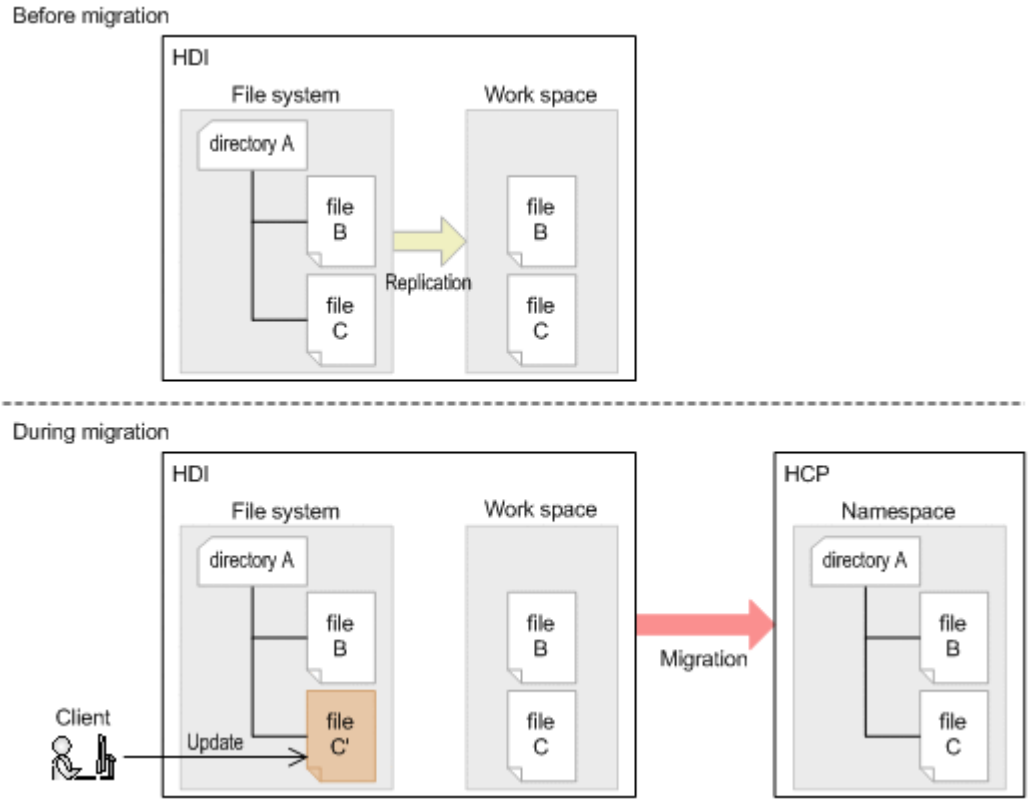


Figure 6-2 Data migration to HCP (when Active File Migration functionality is used)

If you do not use Active File Migration functionality, the data of files modified during the migration will not be migrated to the HCP system until the next migration.

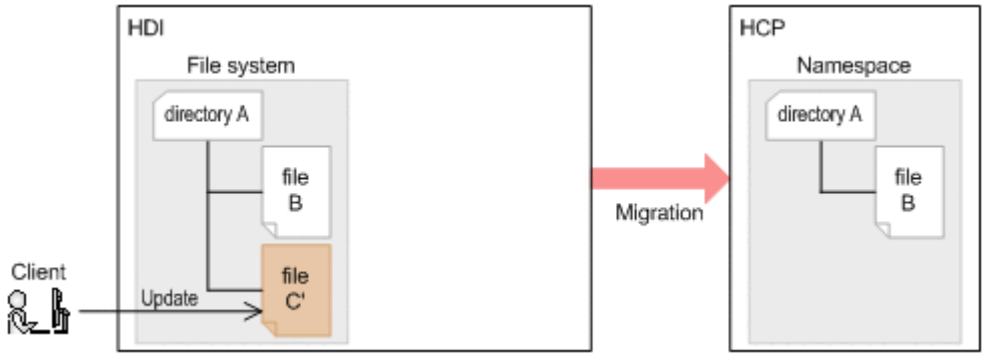


Figure 6-3 Data migration to HCP (when Active File Migration functionality is not used)

The Large File Transfer function can divide a file into pieces and migrate each piece if the file is too large to be migrated at one time. The function migrates only the data that has been updated since the previous migration. Therefore, you can use this function to reduce the time required for migration. If a file for which the function is applied is smaller in size than the preset lower threshold, the function migrates the file to the HCP system without dividing the file data.

For example, assume that you use the Large File Transfer function to migrate file A, as shown in the following figure. In this case, only the updated parts are migrated and the other parts are copied from the past version of the file in the HCP system. As a result, file A is reproduced in the HCP system.

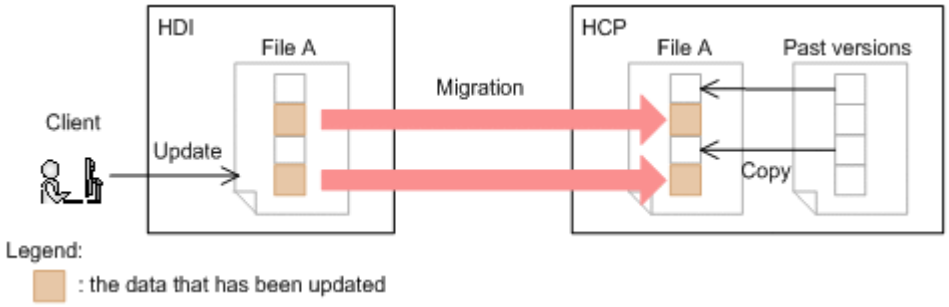


Figure 6-4 Data migration to HCP(when Large File Transfer functionality is used)

If the file to migrate is large, migration might not be able to finish within the specified time and the processing might stop. If you use the Large File Transfer function, even if migration does not finish within the time limit, migration will resume when the next migration is performed.

The Large File Transfer function can be used if all of the following conditions are met:

- The Active File Migration function is enabled.
- The file system has a capacity of 100 GB or more.
- The version of the HCP system is 8.0 or later.
- The ACL is enabled (Enable ACLs) for the namespace.

- The HS3 API is enabled (Enable HS3 API) for the namespace.
- All of the following conditions are met for the file system:
  - The file system does not use the home-directory-roaming functionality.
  - The file system does not use the read-write-content-sharing functionality.
  - The file system is not used for referencing other HDI data as read-only.

Note that the Large File Transfer function is not applied to a file that is larger than 5 TB.

Note: The Large File Transfer function is not applied to stubbed files. For this reason, before using the function, make sure that the lower limit on the size of files to be cache-resident (*B*) is not more than the lower threshold of the file size for applying the function (*A*).

```
B <= A
```

If you use the Large File Transfer function, processing for the following migrations might take a long time:

- The migration performed first after the settings are changed to use the Large File Transfer function

  In such a migration, all of the data subject to migration (including data that was not updated after the previous migration) is migrated.
- A migration in which there exists a large amount of data to be migrated

  This case applies, for example, when all the file system data is to be migrated. In this case, change to the settings that do not use the Large File Transfer function, and also specify settings so that the migration processing does not halt before completion.

For a file system created using an HDI system earlier than version 6.1.0-00, use the GUI or the `arcactmigctl` command to enable the Active File Migration function to create a work space.

The files or directories that could not be migrated last time are migrated first, and the files or directories to be migrated are migrated in ascending order by name. Note that directories are migrated after all the files are migrated in a read-write-content-sharing file system.

For details about the priority of migration tasks executed according to a schedule, see Priority of migration tasks executed according to a schedule on page 6-6. For details about the internal processing before and after data transfer to the HCP system, see Internal processing before and after transferring data on page 6-7. For details about how to determine the capacity of the work space, see Capacity of the work space on page 6-8.

Priority of migration tasks executed according to a schedule

Migration tasks are executed based on the priority set by the system administrator. The following figure shows an example of migration tasks executed according to the priority.

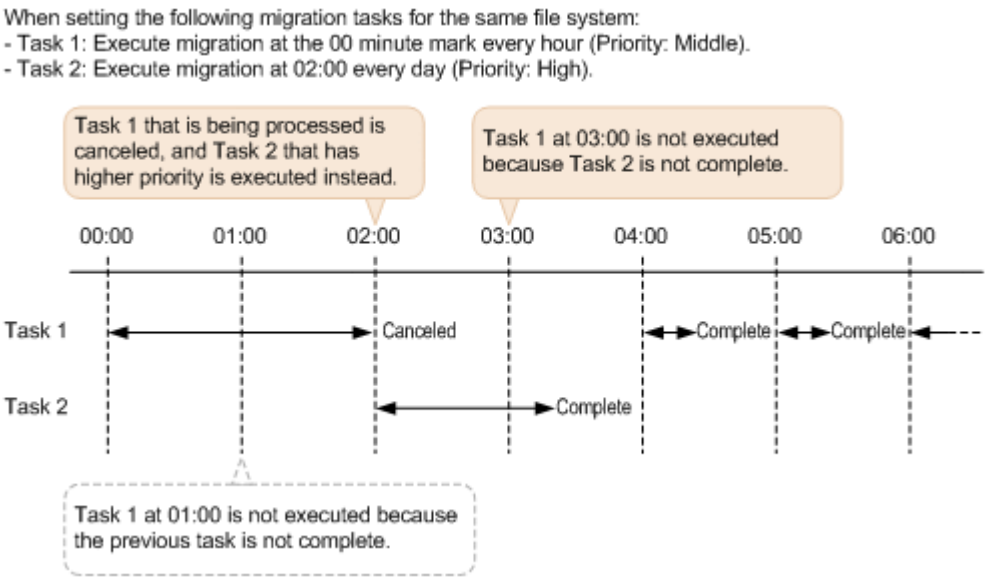


Figure 6-5 Example of migration tasks executed according to the priority

At the date and time specified for execution of a migration task, if a migration task that has higher priority is being processed, a migration task that has lower priority is not executed. If a migration task that has lower priority is being processed, this task is canceled, and the migration task that has higher priority is executed. If migration tasks have the same priority, processing of the task being processed continues.

Internal processing before and after transferring data

To reduce the execution time even when a large number of files are being migrated, the internal processing to create a list of the files to be migrated is executed before and after the processing to transfer data to the HCP system.

During preprocessing, a list of the candidate files for migration is created based on the following file and directory information:

- Files and directories that were updated, created, or renamed after the start of the last migration processing
- Files and directories that did not meet the migration conditions during the last migration processing
- Files and directories for which migration failed during the last migration processing

Then, the files and directories that do not meet the migration conditions are eliminated from the list of the candidate files to create a list of the files to be migrated.

The time required for transferring the data to the HCP system depends on the amount of data in the files, the network environment, and other conditions. In addition, the processing time for generating a list of target files increases as the number of candidate files and directories for migration increases.

Note that, in the post-processing, a list of the files that failed to migrate will be created for the next migration.

The following table shows the processing status of migration tasks, the status to be displayed in the GUI, and the factors that affect the processing time.

Table 6-1 The processing status of tasks, the status to be displayed in the GUI, and the factors that affect the processing time

Processing status of tasks	Information to be displayed in the *migration-task* pages of the Migration Tasks dialog box		Factors that affect the processing time
	Present status	Progress	
Not executed	`Standby` or `Scheduled`	`-/- (-)`	None
Pre-processing	`Running`	`calculating`	Number of events, such as updating files or directories
Transferring data		*number-of-processed-files-and-directories*`/`*total-number-of-files-and-directories*`(`*progress*`%)`	The amount of data of the target files and the network environment
Backing up quota information		`post-command executing`	
Post-processing	`Standby` or `Scheduled`	`-/- (-)`	Number of events, such as updating files or directories

If a migration task is performed during pre- or post-processing, the KAQM37142-E message is output and the task fails. Use the `arctaskstatus` command to check the progress of the pre- or post-processing. If the pre- or post-processing takes a long time, make the maximum duration longer when you set the task schedule, or use the `arcmodectl` command to specify the settings so that the initial mode is used when executing a task.

Capacity of the work space

The recommended value for the work space depends on the file system capacity and the functions to be used. If both the Active File Migration and Large File Transfer functions are to be used, estimate the recommended value by using the appropriate formula in the following table.

Table 6-2 Recommended values for the capacity of the work space (when Active File Migration function and Large File Transfer function are used)

Capacity of the file system (m: capacity of the file system)	Recommended values for the capacity of the work space
m < 0.25TB	(0.0909GB x the number of end users) + (8 x capacity of the file system(TB)) + 0.73GB
0.25TB <= m < 64TB	(0.0909GB x the number of end users) + (0.6508 x capacity of the file system(TB)) + 8.0792GB
64TB <= m	(0.284GB x the number of end users) + (0.6875 x capacity of the file system(TB)) + 8.5GB

If only the Active File Migration function is to be used, the following table shows the recommended values for the capacity of the work space.

Table 6-3 Recommended values for the capacity of the work space (when only Active File Migration function is used)

Capacity of the file system (m: capacity of the file system)	Recommended values for the capacity of the work space
m <= 17TB	10GB
17TB < m <= 256TB	25GB
256TB < m	50GB

If the free capacity of the work space becomes insufficient during migration, the KAQM37753-W or KAQM37772-W message is output, and data is migrated from the file system to the HCP system. In this case, the data of files modified during the migration will not be migrated to the HCP system until the next migration. You can check the used work space capacity in the execution results of the migration task. If the free capacity of the work space becomes insufficient, we recommend that you expand the capacity as follows:

When Active File Migration function and Large File Transfer function are used

```
Extended work space capacity = Used work space capacity x
(The interval at which the migration task is executed /
Time before the work space capacity becomes insufficient#1) x
1.25
```

When only Active File Migration function is used

```
Extended work space capacity = Used work space capacity x
(Time required for migration#2/
Time before the work space capacity becomes insufficient#1) x
1.25
```

#1:

Use the following formula to determine this value:

A = *B* – *C*

A: Time before the work space capacity becomes insufficient

B: Time when the work space capacity became insufficient

C: Time when migration started

The time when the work space capacity became insufficient (B) is the time when the KAQM37750-W or KAQM37775-W message was output. The time when migration started (C) can be checked by using the `arcmigstatus` command or from the GUI.

#2:

Use the following formula to determine this value:

A = *B* – *C*

A: Time required for migration

B: Current time

C: Time when data was replicated in the work space

Also, the KAQM37753-W, KAQM37772-W, or KAQS19001-W message is output when the used work space capacity exceeds 80%. If the used work space capacity exceeds 80%, we recommend that you extend the capacity as follows:

```
Extended work space capacity = Used work space capacity x 1.25
```

Changing files to stub files

If a migrated file is turned into a stub file, only the attribute information of the file will remain. HDI periodically (at times when a migration task is not scheduled) turns files into stub files. At the time of the conversion, if the remaining file system capacity is less than the threshold (initial value: 10%), the system turns files into stub files in order from the least recently accessed until the remaining capacity rises above the threshold.

If the replication functionality is not enabled for the HCP system, use the `arcreplimitset` command to set the threshold file system capacity at which the HDI system turns files into stub files to 0 GB (to disable the stub file functionality). If the stub file functionality is enabled and a failure occurs on both the HCP system and the HDI system, the data for stub files might not be restored.

The following figure shows the process of a file being turned into a stub file.

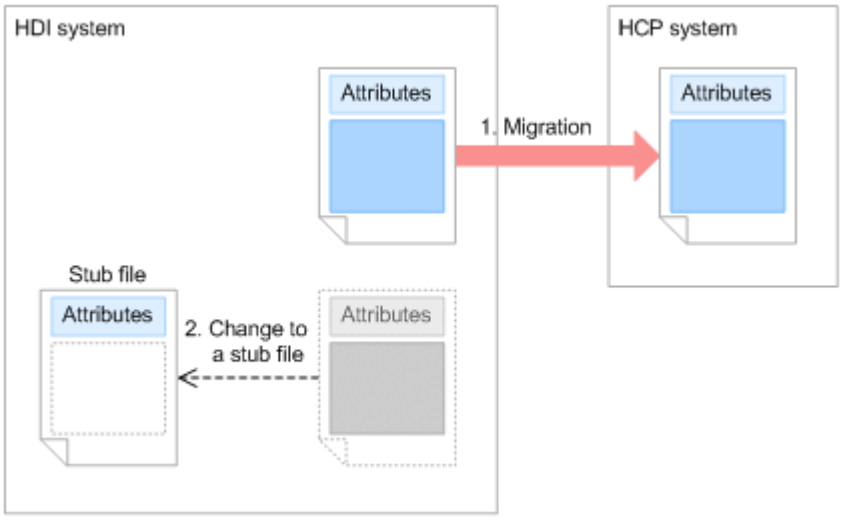


Figure 6-6 Turning a file into a stub file

Recalling data to an HDI system

When a stub file is accessed from an HDI client, the file can be viewed or edited because the data migrated to an HCP system is written in the stub file.

The process in which the data migrated to an HCP system is written to a stub file on an HDI system is called *recall*.

The first time a stub file is accessed, the stub file is recalled. In addition to the time needed to access the file, time is needed to recall the file.

It is possible to keep file data in an HDI system (for example, stop files from being turned into stub files). This practice is called cache residency, and prevents access performance from decreasing. By setting conditions so that files are not turned into stub files, the processing time associated with recalling files that meet the conditions decreases, and access performance is better than that of stub files. To prevent a shortage of space in the file system, make sure the number of cache-resident files does not exceed 2,000,000 files per file system. Note, however, that cache residency cannot be set up for file systems that share data with other HDI systems via a linked HCP system.

If a recall fails because of a failure on the primary HCP system, the HCP replication function can be used to automatically switch the system to the replica HCP system by setting the replica system information in the HDI system, allowing you to continue recall processing.

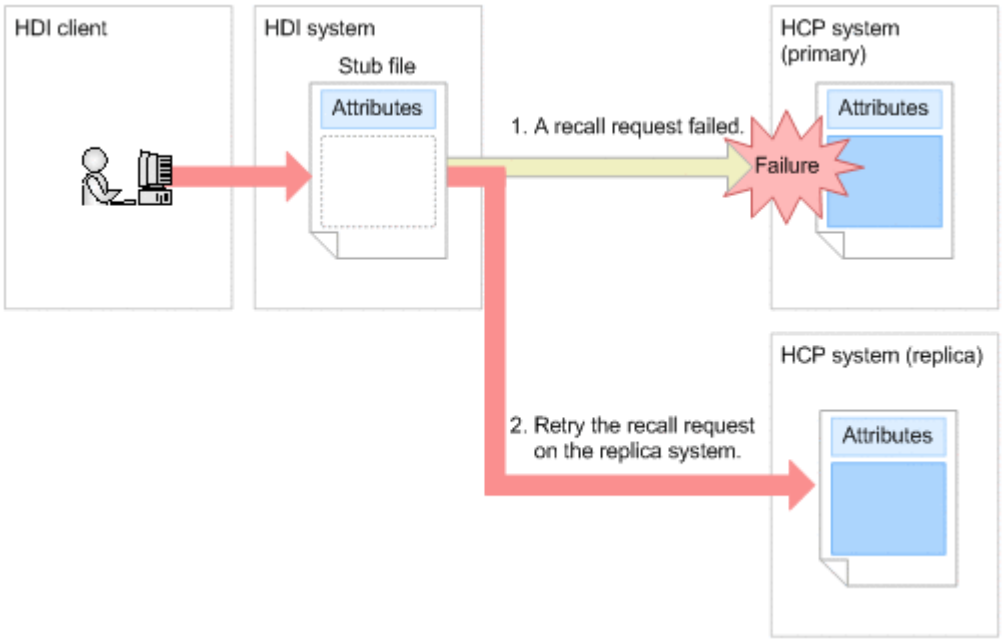


Figure 6-7 Continued recall processing by the replica HCP system

Using and operating data migrated to an HCP system

This section describes the functions to be used and how to operate data that has been migrated to an HCP system.

Making past versions of files that have been migrated to an HCP system available

Generations of the data migrated to an HCP system are managed for each date and time when migration was performed by using version management (versioning). In HDI systems, you can use the data whose generations are managed to re-create the directory structure at the time when a migration was performed. By making the re-created directory available to HDI clients, you can restore data on a file basis, even if a client accidentally deleted a file. (File version restore functionality)

If you specify the setting so that the directory structure at the time when a migration was performed is re-created, a read-only directory named `.history` will be created under the shared directory of the file system. Under the `.history` directory, a directory that indicates the date and time when the migration was performed will be created (past version directory). Attribute information of this directory, such as directory type and update time and date, is restored from the information of the shared directory when migration was performed. If a client accesses a file in the directory, data is recalled from the HCP system, and then the client can view the data at the time when the migration was performed. Only the data of the accessed file is recalled and the recalled data will be deleted when the file is closed, thereby minimizing file system usage.

Note that, immediately after a resource group is started, data in the directory might be temporarily inaccessible from the client. When data in the directory becomes accessible, a KAQM37470-I or KAQM37473-I message is output. If the relevant settings are enabled, you can also receive an SNMP trap notification.

When setting up migration tasks and creating file systems by using the GUI or commands, specify whether to provide clients with past versions of files that have been migrated to an HCP system.

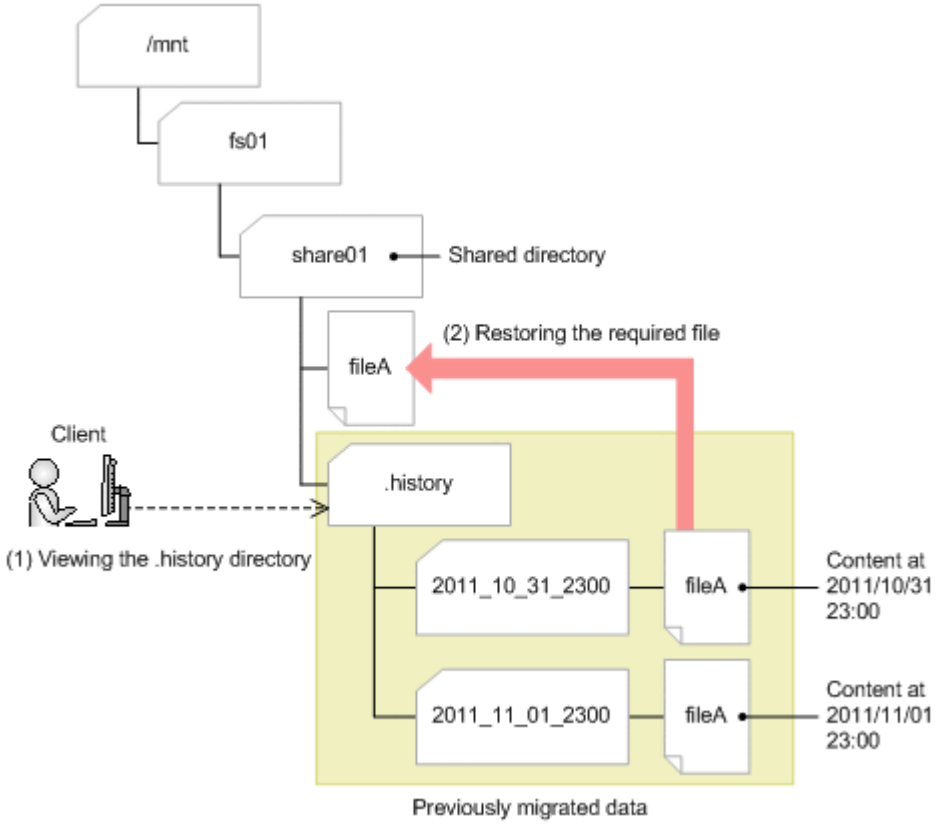


Figure 6-8 Making past versions of files that have been migrated to an HCP system available

The past versions of files migrated to the HCP system are set by default, in the CIFS service configuration definition, to be published by the Volume Shadow Copy Service. Therefore, CIFS clients can view the past version in the `.history` directory or can view the past version shown in the **Previous Versions** tab from the folder or file properties in the share. Note that in the **Previous Versions** tab, the most recent versions from the last seven days are displayed. Past versions older than seven days are viewed in the `.history` directory. Also, if files have the offline attribute, view them in the `.history` directory because the **Previous Versions** tab does not display them. For details about the offline attribute, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

Note the following before making past versions of files that have been migrated to an HCP system available:

- When data is restored because a failure occurred on the target file system, the `.history` directory is also restored. However, the files and directories whose period to hold has elapsed are not restored.
- To allow CIFS clients to view to the `.history` directory, change the settings for the shared directory so that all files and folders are displayed.
- The past version directories whose specified retention period has elapsed are deleted when migration is executed. At this time, if a client is accessing a past version directory to be deleted, the KAQM37236-W error message might be output and the deletion fails. The deletion processing is executed the next time a migration is performed.

If the number of the past-version directories in the `.history` directory becomes large, you can control the file system usage by using a custom schedule.

Note: When you use a custom schedule, the past-version directories, other than those kept according to the schedule, are deleted. In the default settings, the "respective mode" method is configured to be used for selecting the past-version directories to be kept. To change the method of selecting past-version directories to be kept, use the `arccustomschlctl` command. This section describes the processing when the respective mode is used. For details about processing when the cumulative mode is used, see Appendix F, Processing Executed According to the Settings of Custom Scheduling of the File Version Restore Functionality (in Cumulative Mode) on page F-1.

Behavior when a custom schedule is used

If you use a custom schedule, the past-version directories, other than those kept according to the schedule, are deleted in the following situations:

- When migration is executed
- When a value smaller than the value currently specified for the retention period of the past version directories is set
- When the custom schedule is configured for use
- When the custom schedule is changed

As shown in the table below, you can specify schedules in intervals of 15 minutes, 1 hour, 1 day, 1 week, 1 month, and 1 year.

Schedule	Unit
Every 15 minutes	Hour *n*, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59
Hourly	Hour *n*, minutes 00 to 59
Daily	Day *n*, 00:00 to 23:59
Weekly	Week *n*, Sunday, 00:00 to Saturday, 23:59
Monthly	Month *n*, 1st day, 00:00 to *last-day*, 23:59
Yearly	Year *n*, Jan 1, 00:00 to Dec 31, 23:59

Starting from the interval within which past-version directories are deleted, past-version directories of the specified number of intervals are retained in reverse chronological order. For each interval, only the oldest past-version directory is retained.

When you use a custom schedule, specify a number of days greater than or equal to the longest value of recommended values (in days) calculated by the following formulas for the retention period of the past-version directories. Note that if you use the GUI to configure a custom schedule to be used, the retention period is automatically set.

Formula for the recommended value of a retention period

- (<*minutes*> / 60) / 24 (decimals are rounded up)
- <*hours*> / 24 (decimals are rounded up)
- <*days*> x 1
- <*weeks*> x 7
- <*months*> x 31
- <*years*> x 366#

  #: When you specify "100" for <*years*>, the recommended value is "36,500".

When using a custom schedule, we recommend that you specify settings so that directories are created every time a migration is performed. If you change the settings by using the `arcconfedit` command so that the past-version directories are created only when a migration is performed for the first time in a single day, the past-version directories might not be kept as intended when the custom schedule was configured for use.

Example of processing executed according to a custom schedule

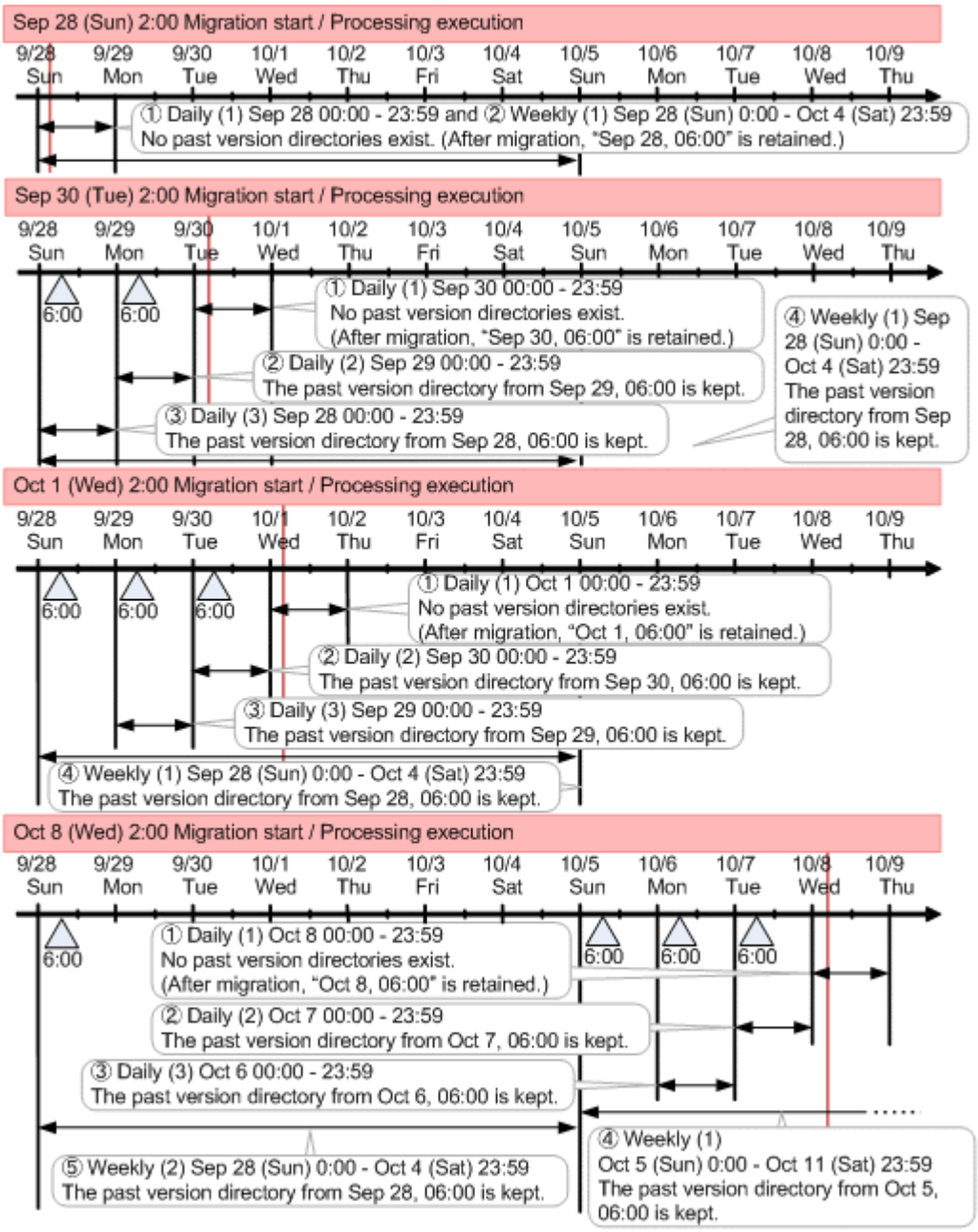
This section gives an example of processing executed according to a custom schedule.

If processing is executed when migration is executed:

If a custom schedule is used with the schedules set as described as follows, migration would take 4 hours to complete and be performed at 2:00 AM daily.

Schedule	Number of units the past directories are kept
Every 15 minutes	0
Hourly	0
Daily	3
Weekly	2
Monthly	0
Yearly	0

The following figure shows the result of keeping the past-version directories when a migration is performed:



The past-version directories are created at 6:00, when migration is complete. Therefore, the interval in which the first processing is executed as per the schedule setting does not yet have a past-version directory. Even in this case, the interval is regarded as one retaining its past-version directory.

When processing is executed on Sept. 30, past-version directories for the three intervals (Sept. 28-30) are retained in accordance with the daily schedule. In addition, the past-version directory for Sept. 28 is retained by the weekly schedule.

As some processing is executed on Oct. 1, past-version directories for the three intervals (Sept. 29-Oct. 1) are retained in accordance with the daily

schedule. In addition, the past-version directory for Sept. 28 (which is not retained by the daily schedule) is retained by the weekly schedule.

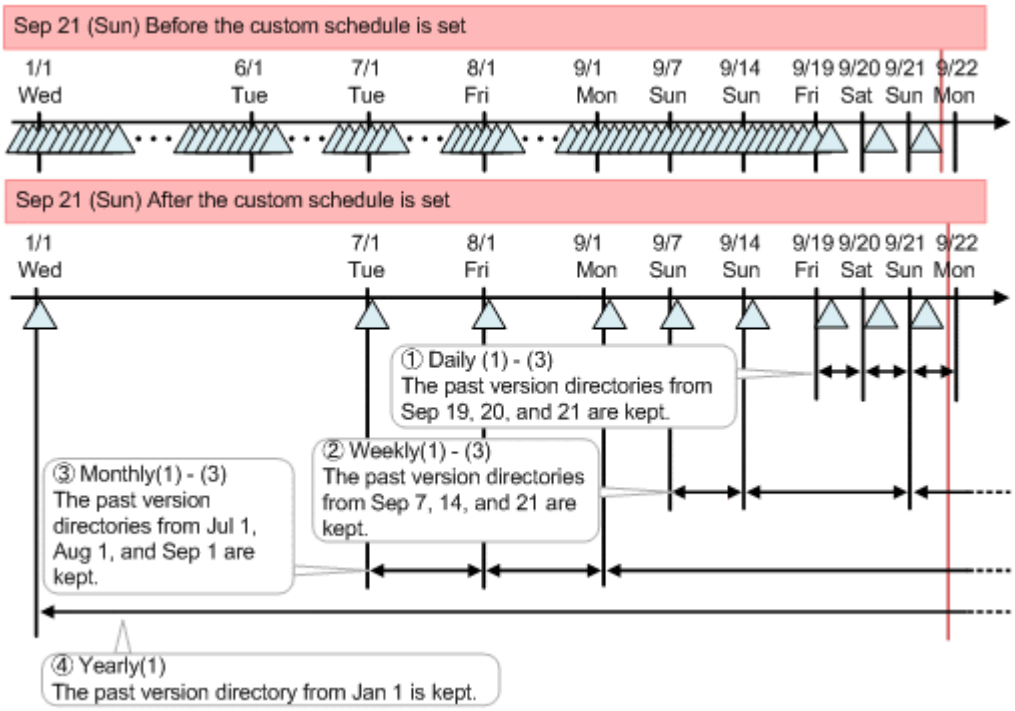
As some processing is executed on Oct. 8, past-version directories for the three intervals (Oct. 6-8) are retained in accordance with the daily schedule. In addition, the past-version directories for the two intervals of Sept. 28 and Oct. 5 (which are not retained by the daily schedule) are retained by the weekly schedule.

If processing is executed when a custom schedule is set:

For example, specify the schedules as described as follows for a file system in which migration is performed daily at 2:00 AM.

Schedule	Number of units the past directories are kept
Every 15 minutes	0
Hourly	0
Daily	3
Weekly	3
Monthly	3
Yearly	1

The following figure shows the result of keeping the past-version directories when a custom schedule is set after the migration on Sept. 21 is complete:



The past-version directories for three intervals (Sept. 19-21) are retained by the daily schedule.

In addition, the past-version directories for Sept. 7 and Sept. 14 (which are not retained by the daily schedule), and Sept. 21 (which is retained by the daily schedule) are retained by the weekly schedule.

Furthermore, the past-version directories for three intervals of Jul. 1, Aug. 1, and Sept. 1 (which are retained by neither the daily nor the weekly schedule) are retained by the monthly schedule.

Finally, the past-version directory for Jan. 1 (which is not retained by any of the daily, weekly, or monthly schedules) is retained by the yearly schedule.

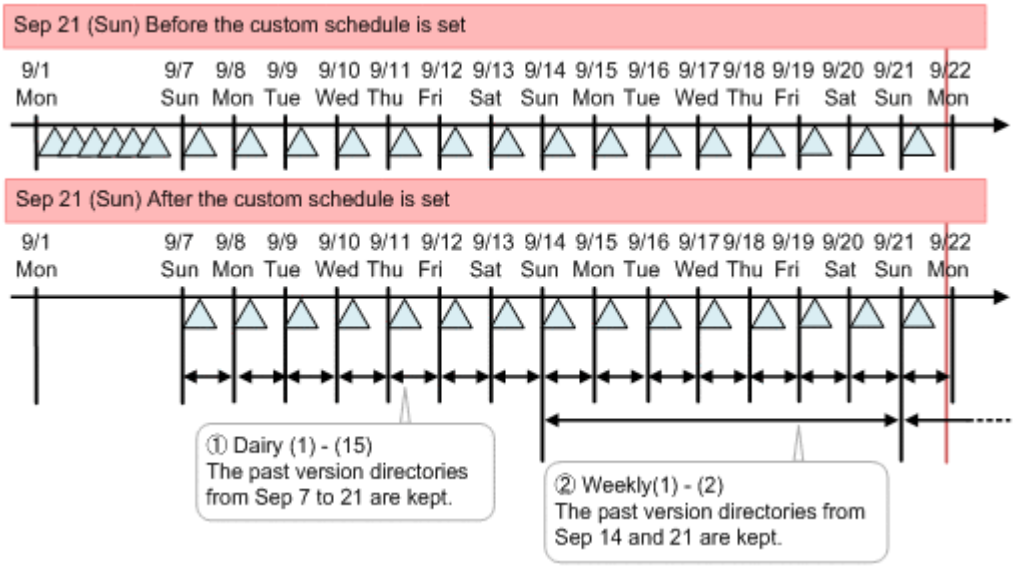
Referential note:

If you set multiple schedules for different intervals, we recommend that you specify the settings so that past-version directories that are retained by each schedule overlap as little as possible.

For example, specify the schedules as described as follows for a file system in which migration is performed daily at 2:00 AM.

Schedule	Number of units the past directories are kept
Every 15 minutes	0
Hourly	0
Daily	15
Weekly	2
Monthly	0
Yearly	0

The following figure shows the result of keeping the past-version directories when a custom schedule is set after the migration on Sept. 21 is complete:



In this example, the past-version directories of Sept. 14 and Sept. 21 that have already been retained by the daily schedule are retained by the weekly schedule. Make an adjustment such as setting a monthly schedule

rather than a weekly schedule and revising the retention interval for the daily schedule to prevent the same past-version directories from being retained by multiple schedules.

Encrypting data to be stored in an HCP system

Data encrypted by using an HDI system can be stored in an HCP system (HCP payload encryption function). Data stored in an HCP system is encrypted; therefore, the risk of information leakage can be reduced even if there is unauthorized access to the HCP system.

HDI uses the common key encryption method (XTS-AES encryption, key length of 256 bits) to encrypt data to be stored in an HCP system. Only file data that is a target of migration is encrypted. Attributes are not encrypted. Note that data is decrypted on an HDI system when the data is recalled from the HCP system.

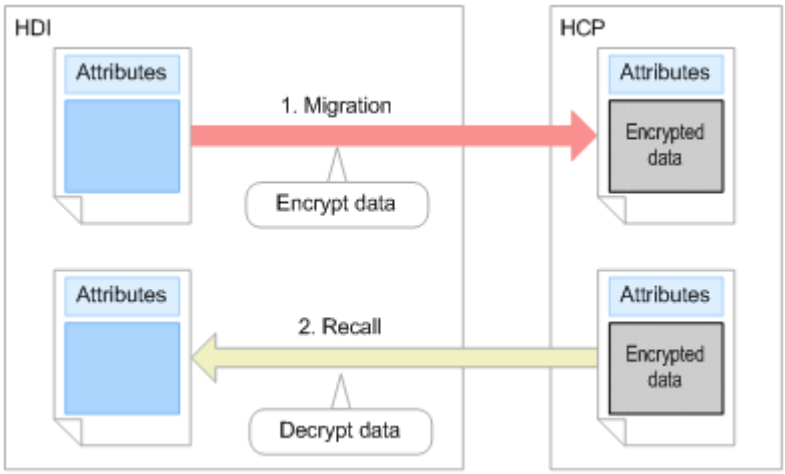


Figure 6-9 Encryption of data to be stored in an HCP system

Note: The common keys used for encryption will be different for each node in the case of a single-node configuration, and for each cluster in the case of a cluster configuration. Each node making up a cluster uses the same common key.
The common key will be saved on the OS disk of a node. If the common key is disabled, you cannot migrate data to an HCP system or recall data from an HCP system. If the system is set to encrypt data to be stored in an HCP system, for each node you need to display the key to be saved on an external storage media and save the key. In the case of a cluster configuration, execute the `hcpdisplaykey` command for either of the nodes. After saving the key on the external storage media, verify the common key saved on the OS disk and the key saved on the external storage media by using the `hcpverifykey` command.

Before encrypting the data to be stored in an HCP system, confirm the following:

- To encrypt data to be stored in an HCP system, an encryption license is necessary.

- When configuring an HDI system, specify whether to encrypt data to be stored in an HCP system for each node in the case of a single-node configuration and for each cluster in the case of a cluster configuration.
- The encryption function setting cannot be changed after starting system operation if the encryption function was set at the time the system was newly set up. To change the encryption function setting, you need to set up the system again.
- When sharing data with another HDI systems via a linked HCP system, do not encrypt data stored in the HCP systems. Encrypted data cannot be operated on at other locations.
- User LUs used by the file system will not be encrypted. For details on encrypting user LUs (local data encryption functionality), see Notes on using the local data encryption functionality on page 4-25.
- A longer time will be necessary for processing migrations and recalls in cases where the data to be stored in an HCP system is encrypted.
- When you encrypt data to be stored in an HCP system, to reduce system load, we recommend that you use the `arcconfedit` command to prevent compression of HTTP messages for communication with HCP systems.

Limiting file share capacity based on hard namespace quotas

Even if there is plenty of available capacity for file shares linked to an HCP system, if the namespace capacity at the migration destination is insufficient, data cannot be migrated to an HCP system. For this reason, when using HDI to migrate data to an HCP system at the share level, you can limit file share capacity by setting the migration destination's hard quota for namespace capacity as the limit (namespace quota).

File share capacity is monitored in 30 minute intervals. At each time, if the file share usage exceeds 85% of the hard namespace quota, a KAQM37505-W message will be output. If set up in advance, this notification can be sent through SNMP or email. After the first warning message, warnings will continually be sent out every 12 hours as long as the usage remains at over 85% of the namespace quota.

Points to be checked before limiting file share capacity based on the hard namespace quota

Before limiting file share capacity based on the hard namespace quota, note the following points about the file shares to be limited based on the hard namespace quota at the migration destination.

- When mounting a file system used to make file shares, the quota function must be enabled.
- For the following cases, the hard namespace quota and namespace usage will be used as the capacity of HDI file shares:
  - When a hard namespace quota has been set as a capacity limitation
  - When post-processing for data transfer to an HCP system has been implemented

    - When a resource group has been started after batch restoration of system setting and user data from an HCP system
    - When the file system has been restored using HCP data
- If you changed the hard namespace quota setting value in the HDI GUI, you can also modify the upper limits of file share capacity at the same time.

  If you changed the hard namespace quota setting value in an HCP system, the value will be applied as the file share upper limit the next time migration is executed. To apply changes prior to the next migration, first go to the HDI GUI and remove all hard namespace quota capacity limit settings, and then change the setting back again.
- Subtree quotas cannot be set for directories below a shared directory with capacity limited by a hard namespace quota.
- Do not specify a quota per file system for file systems that contain shared directories with capacity limited by a hard namespace quota.

  If the quota setting for each file system is smaller than the namespace capacity, a write operation might fail even if the namespace capacity does not exceed the hard quota.
- For file shares linked to an HCP system using an HDI system of version 5.2.0-00 or earlier, capacity cannot be limited based on hard namespace quotas.
- For files within shared directories with capacity limited based on hard namespace quotas, the capacity of files that have not been migrated to an HCP system is not part of the namespace usage. Keep this in mind when confirming usage amounts.
- When importing all the files and directories from another file server, even if the file share usage exceeds the hard namespace quota, usage will not be limited, and import processing will continue. After importation is complete, the files' usage capacity will be restricted.
- Performing any of the following operations in a file share where the usage exceeds the hard namespace quota might result in an error. If an error occurs, make sure that enough capacity is available in the file share, and then try again (see Ensuring sufficient available capacity of file shares on page 6-23).
    - Create or delete a directory, change the attribute of a directory, and set the ACL.
    - Create a login directory for the FTP and SFTP services.
    - Specify settings for collecting the CIFS-service performance analysis log
    - Save CIFS access log information
    - Output the operating information of the system and specify settings related to output
    - Save system LUs (if you set the storage destination of the system settings file to a directory in the file share)
    - Perform a restoration by using NDMP functionality
    - Perform real-time scanning by using Anti-Virus Enabler

- File version restore functionality
- Check the integrity of and recover the files in both the HDI and HCP systems
- Perform autocommit processing and auto-deletion processing of the WORM task

Confirm the following when setting up a linked HCP system.

- If the migration destination's namespace DPL (Data Protection Level) is set at "2", the namespace requires double the capacity of the actual data. Confirm the DPL settings with the HCP system administrator.

Also, inform the end users of the following.

- If capacity is set as limited based on hard namespace quotas, the HCP namespace capacity will be displayed as the CIFS client disk space. For details, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.
- If the capacity limitation settings based on the hard namespace quotas are changed and migration is implemented afterward, the correct disk usage will be displayed.

Check whether file share usage exceeds the hard namespace quotas

To check whether file share usage exceeds the hard namespace quotas, go to the **List of RAS Information** page (for `List of other log files`) from the **Check for Errors** dialog box, and view the XFS log `/var/log/xfs/xfslog`.

1. Choose `List of other log files` from the dropdown list **Info. Type** on the **Check for Errors** dialog box's **List of RAS Information** page, and then click the **Display** button.

   The **List of RAS Information** page (for `List of other log files`) will be displayed.
2. Select "`/var/log/xfs/xfslog`" from the dropdown list **File type**, and then click the **Display** button.

   XFS log information will be displayed.
3. Check whether the following message was output to the XFS log.

   ```
   XFS Namespace quota(block) : hardlimit , file-system-name(device-name)
   share-directory-path-with-namespace-quota-settings , uid : UIDs-of-users-
   who-have-exceeded-usage-limits
   ```

   If this message was not output, the hard namespace quota has not been exceeded, so there is no need to deal with this problem.

   If the message was output, the hard namespace quota for file shares has been exceeded. See If file share usage exceeds the hard namespace quota on page 6-23, and then take any necessary actions.

Ensuring sufficient available capacity of file shares

This section describes how to make sure enough capacity is available in a file share where the capacity limitation is set based on the hard quota of the migration destination namespace.

If file share usage exceeds the hard namespace quota

If file share usage exceeds the hard namespace quota limits, perform the following for the file share:

1. In the GUI, change the schedule to execute an immediate migration task.
2. After the migration task is complete, use the GUI to confirm the namespace usage at the migration destination.

   If the namespace has sufficient available capacity, the following steps are unnecessary.

   If the namespace does not have sufficient available capacity, carry out the following steps.
3. In the GUI, remove the capacity limitation based on the hard namespace quota setting.
4. In the GUI, disable migration task scheduling.
5. Make a request to the HCP system administrator to clear the required capacity on the namespace.
6. After the namespace capacity has been acquired, set the capacity limitation based on the hard namespace quota in the GUI.
7. In the GUI, enable migration task scheduling.

If the KAQM37505-W message is output

If the KAQM37505-W message is output because the file share usage exceeds 85% of the hard namespace quota, perform the following for the file share:

1. In the GUI, change the schedule to execute an immediate migration task.
2. After the migration task is complete, use the GUI to confirm the namespace usage at the migration destination.
3. If the namespace does not have sufficient available capacity, make a request to the HCP system administrator to clear the required capacity on the namespace.

Points to be checked before linking an HDI system with an HCP system

Check the following points before linking with an HCP system.

- Client access performance is degraded temporarily during migration process is ongoing. The performance degradation above is improved by disabling Active File Migration. If the performance degradation still persists even Active File Migration is disabled, please change migration schedule to avoid busy timeslot.

- The total number of file systems and file shares connected to an HCP system cannot exceed 1,023.
- If the KAQM37038-E message was output to the HSM Core log file (`hsmarc.log`), enable version management (versioning) on the HCP system, and then perform the migration again.
- To change the configuration of a tenant that is linked to an HDI system of a version earlier than 4.0.0-00 to share the tenant with multiple HDI systems, install updates for all the HDI systems that will share the tenant before using the tenant with the HDI systems.
- Changing the time on the NTP server might restart the HCP system. Migration and recall processing fails while the HCP system is being restarted. Make sure that no problem occurred after the HCP system restarted, and then change the time on the NTP server.
- To connect a file system that links with an HCP system to another node, you cannot use the `fsexport` command or `fsimport` command to inherit the HCP linkage settings. Re-create the file system on the connected node without executing the `fsexport` command or the `fsimport` command. Then, execute the `arcrestore` command to restore the data in the re-created file system.
- When an HCP system linked to an HDI system stops, users may be unable to access files and directories in the HDI system. If performing maintenance on an HCP system linked to an HDI system, request that clients re-attempt access after the maintenance is complete.

The following section describes the points to be checked before linking with an HCP system.

Operation of a file system or file share associated with a namespace

Check the following points regarding operation of the file system from which data is to be migrated to an HCP system:

- If you assign the namespace of a linked HCP system, the warning threshold for the usage of the file system will be set to 99%. Use the `fsfullmsg` command to change the warning threshold as needed.
- Up to 10 KB is required in the management area per file when migrating data to an HCP system. Take this into account when considering the file system capacity.
- When migration tasks are set, the creation of hard links is automatically disallowed. File systems must be set to disallow hard link creation.
- If you change the settings to allow hard link creation, you can create hard links in file systems. Note that the hard links are migrated to the HCP system as one file. As a result, hard links are not restored when data is restored from the HCP system to the HDI system.
- If a search is performed for files that have the offline attribute, because a large amount of data will be recalled to the HDI system, processing might take a while and the maximum capacity of the file system might be reached.

- If the names of files or directories are changed, the processing for extracting files to be migrated will be affected. For this reason, if you try to change a lot of file names, migration might take a long time.
- If you change the metadata of a file or directory, the metadata is migrated to an HCP system. If you change the metadata of many files, such as for ACL changes, migration of metadata might take a long time. We recommend that you use groups for ACL operations, so that the impact can be reduced even when changes are made to users.
- To prevent the used capacity of the file system from reaching the maximum, set a threshold value that starts changing files to stub files so that the increased amount of data per hour does not exceed the unused capacity of the file system.
- To stop operations linking with an HCP system, if necessary, ask the HCP system administrator to delete the data in the corresponding namespace.

If you are migrating data at the share level, check the following:

- Allocate a namespace to shares created in a directory directly under the mount point. When using the GUI, do not create file systems and shares at the same time. Create the file system first, and then create shares and allocate namespaces.
- The quota functionality must be enabled when mounting a file system whose data is migrated at the share level.
- Do not move, by using FTP or other means, any created files or directories to within different shares. Files and directories moved in this way might not be restored correctly.
- To allocate a namespace by editing a created share, you need to rebuild task management information for the file system by using the `arccorrection` command. It might take time to complete this task. Therefore, it is recommended that you allocate a namespace when creating a new share.
- For a WORM file system, you cannot end operation of a share for which data was migrated to the HCP system.
- To end operation of a share for which data was migrated to the HCP system, release the share, and then, if necessary, use the `arcstdel` command to delete the data in the directory and the mapping information. Before executing the `arcstdel` 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.

Data to be migrated

Check the following regarding the data to be migrated:

- In addition to regular files, directories and special files (excluding socket files) are subject to migration. Special files and directories are migrated regardless of the conditions set for migration policies.
- If a regular file meets any of the following conditions, it will not be migrated even if it meets the conditions set in the migration policy.
  - The file data has not been updated since it was migrated.
  - The path length is more than 4,095 bytes.
  - The file path contains a line feed code.
  - Files in the `.conflict`#, `.conflict_longpath`#, `.snaps`, `.history`, and `.lost+found` directories.
  - Files in directories that have the following names and that are located directly under the file system:

    `.arc`, `.system_gi`, `.system_reorganize`, `lost+found`
  - Files that have the following names and that are located directly under the file system:

    `.backupdates`, `.temp_backupdates`

  #: For a read-write-content-sharing file system only, files in the `.conflict` or `.conflict_longpath` directory will not be migrated.

Settings of policies and schedules for migration tasks

Check the following regarding the settings for policies and schedules for migration tasks:

- Increasing the number of migration tasks to be executed concurrently puts a heavier load on the system. If too many migration tasks are executing concurrently, putting a heavy load on the system, adjust the schedule so that fewer migration tasks execute concurrently.
- If migration tasks have already been set for a file system but a migration is not performed for the file system for a long time, it will take a long time the next time a migration is performed. To avoid this, configure the settings so that a migration is performed on regular basis after migration policies are set.
- To appropriately determine how often migration tasks are to be executed and the maximum number of past version directories to be retained, conditional expressions must be satisfied to prevent any timeouts that might occur if a failover occurs. The following inequality must be satisfied when performing this check. If you use the `arcconfedit` command to configure the settings so that a past version directory is created only when the first migration of the day is performed, you can calculate the settable retention period of the past versions of files by setting `1` for *number-of-migration-tasks-executed-per-day* in the inequality.

$\Sigma_1 (A \times B \times C) + \Sigma_2 (A \times D) \leq 4000$

Legend:

A: Number of shared directories[#1]

B: Retention period for the past versions of data (in days)

C: Number of migration tasks executed per day (times/day)

D: Number of past version directories to be retained for the custom schedule[#2]

Σ_1: The summation of the number of past version directories in a file system that uses the file version restore functionality, and where custom scheduling of the file version restore functionality is not used

Σ_2: The summation of the number of past version directories in a file system that uses the file version restore functionality, and where custom scheduling of the file version restore functionality is used

#1: If there are multiple destinations made available by the NFS protocol, this is the number of shared directories for all destinations (*number-of-shared-directories* x *number-of-destinations*). This is 1 when only the CIFS protocol is used.

#2: The number of past version directories retained for a custom schedule is calculated by the following expression.

Number of past version directories retained for a custom schedule
= <Value specified for interval of 15 minutes> / 15 + <Value specified for interval of an hour>
+ <Value specified for interval of a day> + <Value specified for interval of a week>
+ <Value specified for interval of a month> + <Value specified for interval of a year>

Examination cases are shown below.

Examination case when custom scheduling of the file version restore functionality is not used:

- There is a file system that uses the file version restore functionality.
- There are 10 shared directories in the file system that uses the file version restore functionality.
- There are 5 destinations made available by the NFS protocol in each share.
- Past versions of files are retained for 60 days.

For these assumed settings, use the following inequality to determine the execution interval for migration tasks:

$$(10 \times 5) \times 60 \times \textit{number-of-tasks-executed-per-day} \leq 4000$$

$$\textit{number-of-tasks-executed-per-day} \leq 1.33 \text{ (times/day)}$$

$$\text{Task execution interval} \geq 0.75 \text{ (days)}$$

Examination case when custom scheduling of the file version restore functionality is used:

- There is a file system that uses the file version restore functionality.
- There are 10 shared directories in the file system that uses the file version restore functionality.
- There are 5 destinations made available by the NFS protocol in each share.

Under these conditions, the number of past version directories to be retained for a custom schedule must satisfy the following conditional expression.

$$(10 \times 5) \times \textit{number-of-past-version-directories-to-be-retained} \leq 4000$$

$$\textit{number-of-past-version-directories-to-be-retained} \leq 80$$

Configure the custom schedule settings so that the number of past version directories to be retained does not exceed 80.

- In the following cases, a migration task is not executed even after the specified execution date and time of the migration task arrives. Check and, if necessary, revise the execution date and time, execution interval, and the priority.
  - When the previously executed migration processing is not finished
  - When the migration processing is not finished for a task that has the same or higher priority as a task for which the execution date and time has arrived
- To shorten the interval between migrations, you need to revise the number of days for which objects are stored until they are pruned from the HCP system.

Data migration

Check the following regarding the migration of data to an HCP system:

- If a directory is renamed during migration, data of the files in the directory is not migrated to the HCP system until the next migration.
- If a failover occurs during migration, the migration processing is canceled. Files that have not been migrated will be migrated the next time migration is performed.
- If an error occurs during a migration, any files not used by the HDI system might remain on the HCP system.
- If an error occurs after the `arcrestore` command is executed or during migration, files in an HCP system that can be viewed from a stub file in an HDI system might not be the latest version.
- If files migrated to the HCP system are deleted from the file system, those files are also deleted from the HCP system. Deleted files can be restored from past versions of the data.
- Even if you set the `hcpobjdelset` command so that the data on HCP is asynchronously deleted when the files migrated to HCP are deleted from the file system, when there is insufficient file system capacity, the deletion of data on HCP is synchronized with the deletion of files from the file system. At this time, if communication with HCP fails, the files are deleted from HDI but the data on HCP is not deleted. Check the HSM Core log (`hsmarc.log`) to see if the KAQM37070-E message has been issued. If it has, check the content of the message and ask the HCP administrator to delete the data.
- When files or directories are migrated to an HCP system, the last updated date and time (`ctime`) is not changed.
- When past versions of files migrated to an HCP system are made available to a client, the WORM-related attribute and the last access date and time (`atime`) and last updated date and time (`ctime`) might be different between the file at the time of migration and the file in the `.history` directory. However, the content of the files is the same.

- If past versions of files migrated to an HCP system are made available to a client and the time zone is changed, after restarting the node OS, the name of the directory under the `.history` directory that indicates the date and time that the migration was performed will be changed to the date and time in the new time zone.
- Files and directories that failed to be migrated cannot be viewed in the `.history` directory or in the file system that references the data of another HDI system as read-only. If this happens, files and directories are not displayed, or they are displayed as 0-byte files and empty directories.
- Note that using the Active File Migration function and the Large File Transfer function might negatively affect performance during file system accesses.
- When Large File Transfer function is not used, specify a value smaller than the maximum duration for communication timeouts with HCP systems so that processing is not stopped before migration of large files completes.

Active File Migration

Check the following regarding the Active File Migration functionality:

- When files are migrated to the HCP system by using the Active File Migration functionality, some files might not be migrated if there is insufficient work space or if the work space is affected by a failure. In this case, a message that starts with KAQM37 is output. To resolve this issue, either increase the size of the work space or eliminate the cause of the failure. The files that could not be migrated will be migrated during the next migration.
- Even when the Active File Migration functionality is used, if any of the following operations are performed while files are being migrated to the HCP system, files or directories affected by the operation cannot be migrated:
    - Updating a stub file
    - Renaming a directory
    - Creating or deleting a file under a directory

  The files or directories that could not be migrated will be migrated during the next migration.

Restoration of data

Check the following regarding the restoration of data that was migrated to an HCP system:

- When a directory that has not yet been restored is accessed for the first time, the data is restored from the HCP system on demand. If the number of files or directories in the directory is large, restoring data takes a long time. As a result, Explorer or other applications used on the client side might timeout. However, because the restoration processing will still

continue even if a timeout occurs, wait a while until the processing completes, and then access the target directory again.

- For file systems where restorations were performed, if you perform operations that recursively scan the directory (for example, searching all files, displaying the properties of Explorer, or using the **Show pop-up description for folder and desktop items** function to display pop-ups), the processing takes a long time because data is restored for a large number of directories on demand. Therefore, do not perform operations that recursively scan the directory. Note that you can disable the **Show pop-up description for folder and desktop items** function by using the **Folder Options** dialog box of Explorer.
- When data migrated to an HCP system from a file system that supports 64-bit inodes is restored to a file system that was configured with a version earlier than 4.2.3-03, some files might not be restored.

Accounts used for accessing the HCP system from HDI systems

The accounts used for accessing HCP tenants and namespaces from HDI systems require data access permissions and tenant management permissions. Even with data access permissions, you cannot create or edit namespaces. Likewise, even with tenant management permissions, you cannot access namespace data, making it impossible to perform data migrations or recalls.

The account management methods available differ depending on the HCP version you are using.

For HCP version 5.0 or later

When the HCP system is set up by using the HDI configuration wizard, specify the administrator information for the tenant created by using the HCP system. After the HCP system has been set up by using the configuration wizard, data access permissions are automatically created for the HCP tenant administrator.

If a tenant is shared by multiple HDI systems, we recommended assigning a different user account for each HDI system.

In addition, as part of the settings for a file system or file share that discloses its data to another HDI system via an HCP system, you can use the GUI to create user accounts that have permission to access HCP data in read-only mode. The information about the created account can be specified when you create a file system or file share that will reference the HCP data as read-only.

For HCP version 4.1 or earlier

Different accounts are required for tenant management and data access.

When the HCP system is set up by using the HDI configuration wizard, specify the administrator information for the tenant created by using the HCP system. After the HCP system has been set up by using the configuration

wizard, data access permissions are automatically created for the HCP data access account.

Because the HCP system is already linked to, if the data access account is set up in the HDI system, but the tenant administrator information is not set in the HDI system, perform either of the following:

- Create a user account for the tenant administrator by using the same name and password as the data access account.

  If a tenant is shared by multiple HDI systems, we recommended assigning a different user account for each HDI system.

  Ask the HCP administrator to do this, or refer to the manual of the HCP version you are using.
- Obtain the necessary information from the HCP administrator, and then specify the tenant administrator information yourself by using the HDI configuration wizard.

In addition, as part of the settings for a file system or file share that discloses its data to another HDI system via an HCP system, you can use the GUI to create data access accounts that have permission to access HCP data in read-only mode. The information about the created account can be specified when you create a file system or file share that will reference the HCP data as read-only.

Settings required on the HCP system when linking with the HCP system

This section describes the settings required on the HCP system when linking an HDI system with the HCP system.

Creating a tenant

Before setting up the HDI system, configure an HCP environment and prepare a tenant to be assigned to the HDI system. Ask the HCP administrator to prepare a tenant, or prepare a tenant yourself by referring to the HCP documentation.

The settings below are required to link an HDI system with the HCP system. For all other settings, use the defaults.

- Set the Monitor, Administrator, Compliance, and Security roles for the user account.
- Set a hard quota for the tenant capacity.
- Specify the settings so that the retention mode can be selected.
- Enable versioning.
- If the version of linked HCP system is 4.1 or later, specify a value of at least *number-of-file-system-namespaces* + 1 for the namespace hard quota.
- Enable the HCP management API (MAPI).

Creating a migration-destination namespace

A namespace is automatically created if the namespace information of an HCP system is set by using the GUI. Ask the HCP administrator to create a namespace or create it yourself by referring to the HCP documentation.

The settings below are required to migrate data on an HDI system. For all other settings, use the defaults.

Note that the default namespace cannot be used if an HDI system is linked.

- Set a hard quota for the namespace capacity.
- Select enterprise mode for the retention mode.
- Enable versioning and set a time for version pruning appropriate for system operation.

  In an HDI file system, data from past versions that was migrated to an HCP system is made available to clients by default. When making data from past versions available, set a time for version pruning 1 day longer than the period to hold for HDI versions (the default HDI period to hold is 7 days). To make data from past versions unavailable, set the time for version pruning to 2 days.
- Configure the settings so that custom metadata can be added, replaced, and deleted for objects still within their time for version pruning.
- If the version of linked HCP system is 5.0 or later, enable all namespace permissions for the user account (`Read`, `Write`, `Delete`, `Purge`, `Privileged`, and `Search`).
- If the version of linked HCP system is 4.1 or earlier, create a data access account.
- `Retention Class` is not set.

  If you are using the WORM functionality, configure the setting in the HDI system.
- If the version of linked HCP system is 7.1 or later, enable the namespace optimization option (`Optimized for cloud protocols only`).

In addition to the above settings, you need to set the namespace capacity. Use the following formula to estimate the maximum capacity of the namespace, and then determine the namespace capacity to set.

```
maximum-namespace-capacity =
 total-capacity-of-user-data-to-be-stored +
 total-capacity-of-files-to-be-updated-in-a-day x
 period-to-hold-the-past-versions x (1 +
 capacity-of-files-to-which-Large-File-Transfer-function-is-applied /
 total-capacity-of-user-data-to-be-stored)
```

When Large File Transfer function is not used, use the following formula to estimate the maximum capacity of the namespace, and then determine the namespace capacity to set.

```
maximum-namespace-capacity =
 total-capacity-of-user-data-to-be-stored +
 total-capacity-of-files-to-be-updated-in-a-day x
 period-to-hold-the-past-versions
```

To change the level at which namespaces are assigned from file systems to file shares, use the `arcrestore` command. Use this command to move the data of the file system linked to the HCP system at the file system level to a directory within a file system set to link to the HCP system at the share level.

Note:

- Do not create shares in the migration-destination directory before executing the `arcrestore` command.
- If, in the share directory at the migration-destination, you will make past versions of files migrated to an HCP system available to clients, reconsider the retention period for past data.
- Ask the end users not to access the file systems that will be operated on.
- If you delete the data in a file system before deleting that file system, the data migrated to the HCP system is also deleted. For this reason, ask the end users not to delete any data that exists within the applicable file system and that needs to be migrated.

The procedure for changing the level at which namespaces are assigned from file systems to file shares is described below.

1. Run the `archcpget` command by specifying the `--migrate-info` option.

   Record the name of the migration-destination namespace of the applicable file system.
2. Record the file share information.

   Run either the `cifslist` or `nfslist` command, and record the CIFS or NFS share information.

   To you want to be able to restore information about multiple file shares at once, execute the `cifsbackup` or `nfsbackup` command to back up the information about the CIFS or NFS shares at the file system level.
3. For CIFS shares, use the `cifsoptlist` command and record the information set for the CIFS shares.
4. Use the `cifsdelete` or `nfsdelete` command to delete all file shares within the applicable file system.
5. Use the `quotaset` command to remove the quota settings on the applicable file system.
6. Use the GUI to change the schedule for migration tasks of the applicable file system so that the tasks are executed immediately.
7. Use the GUI to verify that the migration task was successful.

   If migration of any files or directories failed, identify the cause of the failure, take the appropriate action, and then execute the task again.
8. Use the `fsumount` command to unmount the file system.
9. Use the `fsdelete` command to delete the file system.
10. Use the GUI to prepare a file system that is set to link to an HCP system at the share level.

    To make data of past versions that was migrated to an HCP system accessible to clients, set the retention period for past data when creating

or editing a file system, so that the required data in the `.history` directory in step 12 is also recovered.

11. Use the `dircreate` command to create a directory for namespace allocation directly under the mount point of the file system.

    Do not create file shares.

12. Use the `arcrestore` command to restore, to the directory created in step 11, the data that was migrated to the HCP system.

    Specify the options as follows:

    `arcrestore --namespace` *`name-of-namespace-recorded-in-step-1`* `--file-system` *`name-of-file-system-prepared-in-step-10`* `--dir` *`name-of-directory-created-in-step-11`*

13. Create file shares corresponding to the directory created in step 11.

    Based on the CIFS or NFS information recorded in step 2, execute the `cifscreate` or `nfscreate` command to create the file shares.

    To restore information about multiple file shares at once, execute the `cifsrestore` or `nfsrestore` command to output a template file for the restoration script. Edit the share directory path specified in the template file by following the example below. Then, execute the script to restore information about the CIFS and NFS shares.

    The following is an example of editing a template file for restoring information about CIFS shares, where the names of the applicable file systems and directory are as follows:

    - Name of the migration-source file system: `fs01`
    - Name of the migration-destination file system: `fs02`
    - Name of the migration-destination directory: `dirA`, which is directly under the mount point

    Template file before being revised

    ```
    $PRECMD sudo cifscreate -x cifsshare01 -d \/mnt\/fs01 -c ...
    ...
    $PRECMD sudo cifscreate -x cifsshare01 -d \/mnt\/fs01\/dir01 -c ...
    ```

    Template file after being revised

    ```
    $PRECMD sudo cifscreate -x cifsshare01 -d \/mnt\/fs02\/dirA -c ...
    ...
    $PRECMD sudo cifscreate -x cifsshare01 -d \/mnt\/fs02\/dirA\/dir01 -c ...
    ```

14. For CIFS file shares, use the `cifsoptset` command to change the CIFS share settings based on the information recorded in step 3.
15. When setting subtree quotas, change the settings in the GUI so that file shares including directories with subtree quotas are not subject to capacity limitations based on the hard namespace quota at the migration destination.
16. To set a subtree quota, use the `stquotaset` command to set the required information.

If you change the settings of a file system that discloses its data to another HDI system via an HCP system, you need to create a file system that accepts

migrated data at the share level in the HDI system referencing the data as read-only, and you need to restore the HCP data in the file system. If the level at which namespaces are allocated differs, you will not be able to view the most recent data that was migrated to the HCP system.

Creating a namespace for saving system settings

A namespace for saving system settings (`system-backup-data`) is automatically created when the HCP system is configured from the setup wizard of the HDI system.

The settings below are required to save system settings. For all other settings, use the defaults.

- Specify `system-backup-data` as the namespace name.
- Specify a hard quota for the namespace capacity as follows:

  `total-number-of-systems-using-tenants``#` `x 1 GB`

  #: This is equal to the total of the number of HDI systems in single-node and cluster configurations in those configurations.

  To import data from another file server to a file system linked to the HCP system at the share level, ensure that enough space is available by adding the capacity to be used for the imported data to the hard quota for the capacity of the namespace of the location in which system settings are normally saved. You can use the following formula to estimate the capacity that will be used by the data to be imported:

  `number-of-files-and-directories-to-be-imported` `x` *`average-path-length-for-import-source-shares`*

  For example, when there are 10 million files and directories to be imported, and the average path length is 256 bytes, add 2.38 GB to the value to be specified as the hard quota.
- Select enterprise mode for the retention mode.
- Enable versioning and set a time for version pruning appropriate for system operation.
- If the version of linked HCP system is 5.0 or later, enable all namespace permissions for the user account (`Read`, `Write`, `Delete`, `Purge`, `Privileged`, and `Search`).
- If the version of linked HCP system is 4.1 or earlier, create a data access account.

When using the replication functionality

If a failure occurs on a primary HCP system, the HCP replication function can be used to recall a file from the replica HCP system to the corresponding stub file on the HDI system.

To use the replication functionality on the HCP system after a migration to the HCP system has been started, the replication functionality must be enabled for all the namespaces, including the namespace that contains the system settings file (`system-backup-data`).

When upgrading software on a node by using an installation file on HCP

In a single-node HDI configuration, you can use an installation file that has been stored in HCP to upgrade the software on the node. Follow the directions below to store in HCP the installation file stored on the installation media.

Note: Register the installation file for each tenant that is assigned to the HDI system.

1. Obtain the necessary installation files from the HDI installation media.
   See Obtaining the necessary files on page 6-36.
2. Create a namespace to store the installation files.
   See Creating a namespace on page 6-36.
3. Set data access permissions for the user accounts.
   See Setting the data access permissions for user accounts on page 6-37.
4. Store the installation files in the namespace.
   See Storing the installation files on page 6-37.
5. Add custom metadata to the installation files stored in the namespace.
   See Adding custom metadata for the installation file on page 6-39.
6. Use the installation files stored in HCP to install updates for the software running on the node.
   See the *Administrator's Guide*.

Obtaining the necessary files

Obtain the installation files and the version management file from the HDI installation media. The following files are required for an update installation:

- `install_files.tar.gz`
- `install_files.tar.gz.md5`
- `version.xml`

Creating a namespace

The namespace settings that are required for storing the installation file are as follows:

- `system-install` is set as the namespace name.
- **MD5** is set for **Hash Algorithm**.
- Version management (**Versioning**) is enabled, and in **Prune versions older than**, `0` is set to both **Primary System** and **Replica System (if replicating)**.
- For the capacity (**Hard Quota**) of the storage to be allocated in the namespace, the following value (units: GB) is specified:
  `value-selected-to-'DPL' x 2`

Setting the data access permissions for user accounts

Set the data access permissions for the user account that is used to operate the installation files, and the user account that is used to access the client from HDI.

Enable the `Browse`, `Read`, `Write`, `Delete`, and `Purge` namespace permissions (**Assign Data Access Permissions for Selected Namespaces**).

If the primary HCP system is version 5.0 or later, and the replica HCP system version is 4.*x*, do not select **Change Owner**.

Storing the installation files

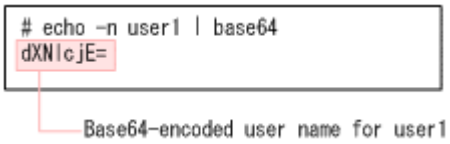
The following is the procedure to use the `curl` command from a client to store the installation files in the namespace:

1. On the client where you will execute the `curl` command, save the installation files (`install_files.tar.gz` and `install_files.tar.gz.md5`).
2. Generate a Base64-encoded user name and a MD5-hashed password.

   Base64-encoded user name

   Use Base64 to encode the user name for the user account that you use to access the namespace. Use a general Base64 encoding tool to generate the user name.

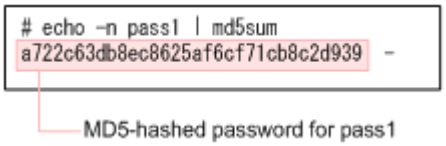
   The following is an example of a Base64-encoded user name:

   MD5-hashed password

   Use MD5 to hash the user name for the user account that you use to access the namespace. Use a general MD5 hashing tool to generate the user name.

   The following is an example of a MD5-hashed password:

3. If any installation files are already stored in the target namespace, delete the installation files.

   Execute the following command:

   ```
   curl -k -iX DELETE -b "hcp-ns-auth=Base64-encoded-user-name:password-
   created-from-the-MD5-hashing-function" "https://system-install.tenant-
   name.HCP-host-name (FQDN)-or-IP-address/rest/system/HDI/
   install_files.tar.gz?purge=true"
   ```

   The following is an example of the execution for the command:

```
# curl -k -iX DELETE -b "hcp-ns-
auth=c3RhcnQ=:a3b9c163f6c520407ff34cfdb83ca5c6"
"https://system-install.system-tenant.vm07.hcp.local/rest/system/HDI/
install_files.tar.gz?purge=true"
HTTP/1.1 200 OK
Set-Cookie: hcp-ns-auth="c3RhcnQ=:A3B9C163F6C520407FF34CFDB83CA5C6";
Version=1;Path=/;Domain=vm07.hcp.local;Discard
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-HCP-ServicedBySystem: vm07.hcp.local
X-RequestId: 73B37EEA1A6A85
X-HCP-Time: 1382409961
Content-Length: 0
```

4. Store the installation files in the namespace.

   Execute the command below. The execution results for the command are output to `result.txt`.

```
curl -k -# -b "hcp-ns-auth=Base64-encoded-user-name:password-created-from-
the-MD5-hashing-function" -iT storage-location-for-installation-files-
saved-in-step-1
"https://system-install.tenant-name.HCP-host-name (FQDN)-or-IP-address/
rest/system/HDI" > result.txt
```

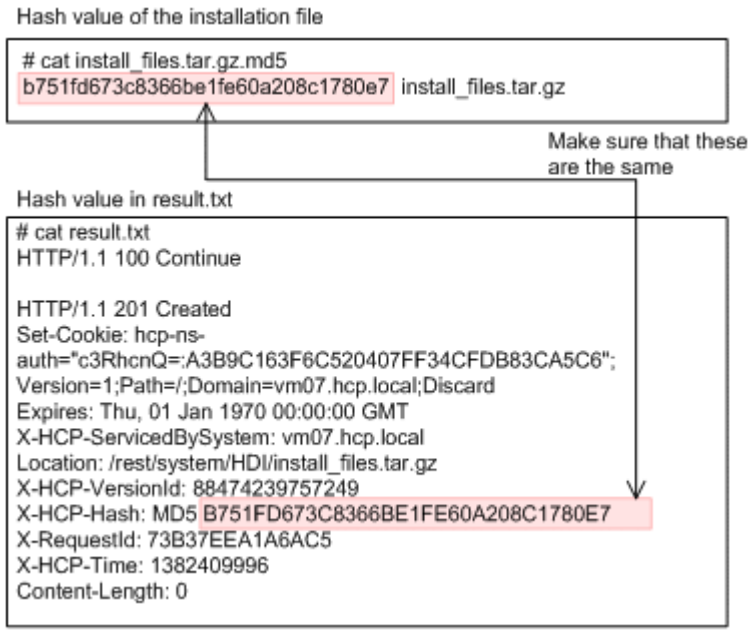
   Below is an example of the execution for the command. The progress is displayed during the execution, and the progress reaches 100% when the execution is completed.

```
# curl -k -# -b "hcp-ns-auth=c3RhcnQ=:a3b9c163f6c520407ff34cfdb83ca5c6" -
iT /HDI/install_files.tar.gz "https://system-install.system-
tenant.vm07.hcp.local/rest/system/HDI/" > result.txt
#######                                                                  10.8%
```

5. Make sure that the hash values for the installation files that were saved in step 1 are the same as the hash values in `result.txt` that was output in step 4.

   When you compare the hash values, note that they are not case-sensitive. If the values are different, repeat the procedure from step 1.

   The following is an example of the hash values to be checked:



Adding custom metadata for the installation file

The following is the procedure for adding custom metadata to an installation file that is stored in the namespace:

1. On the client where you will execute the `curl` command, save the version management file (`version.xml`).
2. Add custom metadata to an installation file.
   Execute the following command:

   ```
   curl -k -b "hcp-ns-auth=Base64-encoded-user-name:password-created-from-the-MD5-hashing-function" -iT storage-location-for-version-management-file-saved-in-step-1 "https://system-install.tenant-name.HCP-host-name (FQDN)-or-IP-address/rest/system/HDI/install_files.tar.gz?type=custom-metadata"
   ```

   The following is an example of the execution for the command:

   ```
   # curl -k -b "hcp-ns-auth=c3RhcnQ=:a3b9c163f6c520407ff34cfdb83ca5c6" -
   iT /HDI/version.xml "https://system-install.system-tenant.vm07.hcp.local/
   rest/system/HDI/install_files.tar.gz?type=custom-metadata"
   HTTP/1.1 100 Continue

   HTTP/1.1 201 Created
   Set-Cookie: hcp-ns-auth="c3RhcnQ=:A3B9C163F6C520407FF34CFDB83CA5C6";
   Version=1;Path=/;Domain=vm07.hcp.local;Discard
   Expires: Thu, 01 Jan 1970 00:00:00 GMT
   X-HCP-ServicedBySystem: vm07.hcp.local
   X-HCP-Hash: MD5 04A4B15797225D13F7911FEF86C3C464
   Location: /rest/system/HDI/install_files.tar.gz
   X-RequestId: 73B37EEA1A7778
   X-HCP-Time: 1382413082
   Content-Length: 0
   ```

3. Obtain the custom metadata information that was added to the installation file.

Execute the command below. The execution results for the command are output to `result_custom.txt`.

```
curl -k -b "hcp-ns-auth=Base64-encoded-user-name:password-created-from-the-MD5-hashing-function" -i "https://system-install.tenant-name.HCP-host-name (FQDN)-or-IP-address/rest/system/HDI/install_files.tar.gz?type=custom-metadata" > result_custom.txt
```

The following is an example of the execution for the command:

```
# curl -k -b "hcp-ns-auth=c3RhcnQ=:a3b9c163f6c520407ff34cfdb83ca5c6" -i
"https://system-install.system-tenant.vm07.hcp.local/rest/system/HDI/
install_files.tar.gz?type=custom-metadata" > result_custom.txt
    % Total    % Received % Xferd  Average Speed      Time      Time
Time      Current
                                   Dload   Upload     Total     Spent
Left      Speed
 100  426    100 426      0 0      5388    0          --:--:--  --:--:--
--:--:--  416k
```

4. Make sure that the custom metadata in the version management file that was saved in step 1 is the same as the custom metadata in `result_custom.txt` that was output in step 3.

   The following is an example of the custom metadata to be checked:

Load-balancing clusters for an HCP system

Check the following with respect to load-balancing clusters for an HCP system to be linked:

- HCP systems use round-robin DNS for load-balancing clusters. If the IPv4 address used by the system that stores data in an HCP system is resolved in compliance with RFC 3484, the round-robin DNS technique used on the HCP system might not operate properly, resulting in the inability to determine the performance of the HCP system.
- When the HDI system sends a query to the DNS about the IPv4 address of the HCP system for name resolution, a number of candidates are presented. Following the rules of RFC 3484, the HDI system selects, from the candidates presented from the DNS, the address that has the largest part matching its own address. Therefore, when the HCP and HDI systems are on the same network segment, the load will not be balanced and accesses might be concentrated on a specific node.

Table 6-4 Example of an IPv4 address for which accesses are concentrated on a specific node

Device	IPv4 address	Sequence of each bit in the fourth octet
HDI	192.168.0.194	11000010
HCP node097	192.168.0.195	11000011
HCP node098	192.168.0.196	11000100
HCP node099	192.168.0.197	11000101
HCP node100	192.168.0.198	11000110

In this example, accesses are concentrated on `HCP node097` for the IPv4 address `192.168.0.195`, which has the largest part matching between the HDI system addresses. To avoid not being able to determine the performance of the HCP system, change the IP address in the HDI system or in the HCP system, and change the settings so that accesses are not concentrated.

Referencing the data of another HDI system in read-only mode

Note the following points when referencing the data of another HDI system as read-only:

- Data sometimes cannot be properly referenced by a location because shortcuts and symbolic links in Windows are dependent on the configuration of the file system they were created in.
- HDI system version 03-01-00-00 or later must be used at all of the sites sharing data.
- Manage user information by using an external authentication server, and use the same user information for each HDI system.

- When editing file share attributes or canceling the file sharing in a file system disclosing its data, the system administrator of the HDI system that discloses its data must inform the system administrator of the HDI system referencing the shared data about the details of the change. The informed system administrator must change the settings on file shares according to the information.
- The cache residency policy is not available in any file systems that reference the data from other HDI systems as read-only.
- If synchronization fails (for example, because of an error in the communication with HCP), data might be restored from HCP the next time synchronization is performed. If the NFS share was created in a subdirectory other than the mount point of the file system, shared directories are re-created when data is restored from HCP. As a result, an attempt to access the NFS might end in an ESTALE error. In such cases, when the restore operation is performed, the SNMP trap sends the KAQM37782-W message or the KAQM37783-W message. Refer to the message and remount the shared directories on the NFS client.

Tasks required for referencing the data of another HDI system as read-only

If referencing data of another HDI system as read-only via a linked HCP system, the system administrators of the HDI systems disclosing the data and the system administrator of the HDI system referencing the data must work together.

To share HCP data migrated from other HDI systems as read-only:

1. On the HDI system disclosing its data, create a file system, and then create a file share.

   The operations are performed by the system administrator of the HDI system that discloses its data.
2. Migrate the data in the file system disclosing its data.
3. Create a file system to reference the HCP data migrated from the HDI system disclosing the data, and then create a file share.

   If you create a file share before finishing synchronizing the HDI system disclosing its data, the data will be synchronized automatically after starting operations. To automatically synchronize data, the path of the shared directory and the path of the shared directory of the HDI system disclosing its data must match perfectly (case sensitive). Use the `arcurlget` command to check whether the target directory is synchronized.

   Set the information for the namespace to which data is migrated. Set the following settings so that they are the same as those for the file system that was configured in step 1:

   - ACL type of the file system
   - Settings related to the WORM functionality
   - Level at which namespaces are allocated (file systems or shares)

If applying the share level, allocate the information on the namespace to the share created directly under the mount point.

- Threshold at which stub processing is performed
- CIFS and NFS share information

The capacity required by a file system differs depending on the level at which namespaces are allocated. For allocation at the file system level, set the same capacity as that of the file system created in step 1. For allocation at the share level, specify a capacity equal to or greater than the total capacity occupied by the user data stored in all namespaces that are accessible from the file system.

In addition, mount the file system with both the read and write permissions.

These operations are performed by the system administrator of the HDI system referencing the shared data.

For details about how to reference data of another HDI system as read-only via a linked HCP system, see the *Administrator's Guide*.

If HCP data will no longer be shared, the system administrators of the relevant HDI systems must perform the following:

If stopping data-sharing, the system administrator of the HDI system disclosing its data must inform the system administrators of the HDI systems referencing the data regarding the stopping of sharing, and then must change the accounts used for access to the namespaces.

The system administrator of each HDI system must change the settings for file systems or file shares and delete file systems or file shares.

Performing the roaming of home-directory data among HDI systems

It is possible to enable roaming for the data in the home directory created for each end user who uses the CIFS protocol to access the data via a linked HCP system (that is, the home-directory-roaming functionality). With the home-directory-roaming functionality, an end user is able to read and write any files created in his or her normal HDI system from any HDI system at a different location.

Note: The use of the home-directory-roaming functionality requires you to link the HDI systems of system version 4.1.0-00 or later with the HCP systems of version 4.1 or later, in advance.

If it is possible to enable roaming for the home-directory data of a file system among HDI systems, such a file system is referred to as a "home-directory-roaming file system."

The following figure shows the exemplar usage of enabling roaming for home-directory data among HDI systems.

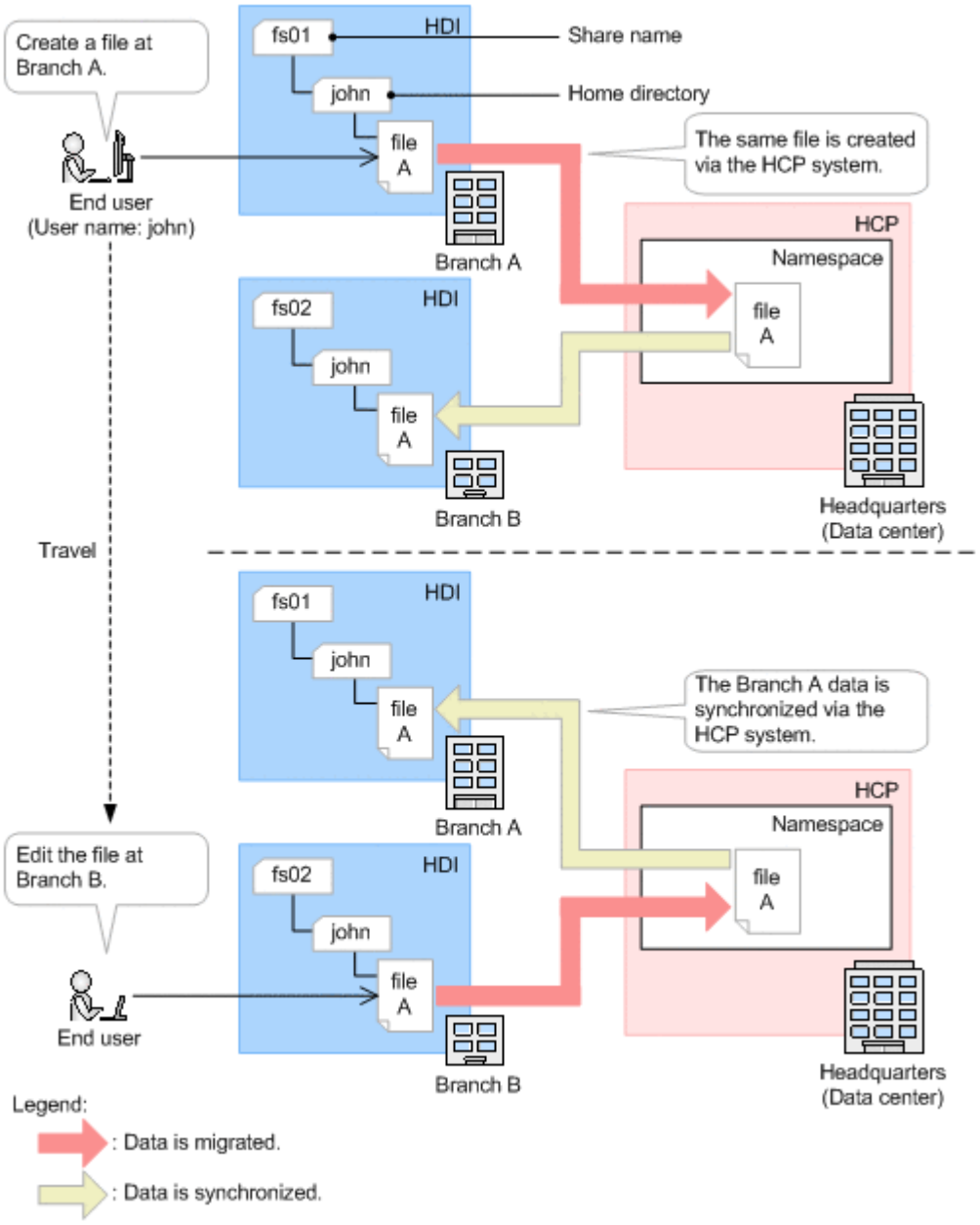


Figure 6-10 Exemplar usage of enabling roaming for home-directory data among HDI systems

Data among HDIs are automatically synchronized. After an end user edits a file, updated data is migrated to HCP, and then the updated data is used to update data in the other HDI. Upon initial installation, data is migrated every hour.

The home-directory-roaming file system must be accessed from CIFS clients.

Points to be checked before enabling roaming for home-directory data among HDI systems

This subsection describes the points to be checked before enabling roaming for home-directory data among HDI systems.

Migration-destination tenants and namespaces

Check the following points regarding HCP tenants and namespaces to be used:

- Specify the same tenant used for the migration destinations for all the linked HDI systems.
- When manually creating a namespace, you need to check, and if necessary, revise the number of days for which objects are stored until they are pruned. Ask the HCP system administrator to perform this task.
- A namespace corresponding to a home-directory-roaming file system cannot be specified as the migration destination of any file system other than the home-directory-roaming file system.
- If you use the home-directory-roaming functionality, HCP issues the message below regarding a compliance event. This message is issued during normal processing, and does not indicate a problem.

  `Privileged purge succeeded for object /management/hdr/lock/`*`user-name`*`.lock, Reason: unlock_of_homedirectory_resource.. Namespace: `*`namespace-name`*

Management of home-directory-roaming file systems

Note the following points regarding the management of home-directory-roaming file systems:

- Use the same character code in all the linked HDI systems.
- Allocate namespaces for the migration destinations at the file system level.
- You cannot make a home-directory-roaming file system to an HCP system accessible as read-only.
- The following functionality is unavailable for the home-directory-roaming file system:
  - Using the WORM functionality
  - Managing subtree quotas
  - Using the NDMP functionality
  - Importing data from other file servers
  - Setting of the cache residency policy
  - Using the read-write-content-sharing functionality
  - Using the Large File Transfer functionality
- When creating a file share in a home-directory-roaming file system, the function for automatically creating a home directory is enabled by default.

- If you back up information of a CIFS share that has been set to not use the function for automatically creating a home directory, and then the `cifsrestore` command is used to restore the information to an HDI system whose system version is not 5.3.*x*-*xx*, 5.4.*x*-*xx* or 6.*x*.*x*-*xx* (*x* represents any number), the information cannot be restored. In such a case, edit the template file of the restore script that has been output by using the `cifsrestore` command, and then run the script to restore the information of the CIFS share.
- Do not change migration policy settings related to the conditions of migrated files. When the home-directory-roaming file system is created, appropriate migration policies are set by default so that all the data in the file system is migrated to HCP.
- We recommend creating one home-directory-roaming file system for one HDI system.

  When you concurrently operate home-directory-roaming file systems, read-write-content-sharing file systems, and file systems that migrate data to HCP, you need to limit the total number of file systems to up to four.
- Increasing the number of migration tasks to be executed concurrently puts a heavier load on the system. If too many migration tasks are executing concurrently, putting a heavy load on the system, adjust the schedule so that fewer migration tasks execute concurrently.
- A maximum of 1,000 end users can use the home-directory-roaming file system.

  If the number of end users who use the home-directory-roaming file system or the number of files to be created or updated increases, migration cannot complete within one hour, and the time span that the home directory in another HDI system remains read-only is longer. Adjust the number of end users and files to ensure that migration can be completed within one hour.
- When an end user is accessing a home directory, the home directory that the same user is using in another HDI is read-only.
- If the client failed to create or update a file due to the temporary problem of the home directory being read-only, the status of the client might be improved by setting the CIFS share to use the retry function.
- If you need to stop the HDI system for routine maintenance, notify the end users in advance to stop accessing the home directory from the HDI system to be stopped, and then migrate all of the data in the home-directory-roaming file system to the HCP system. If you do not migrate the data to the HCP system, the update information is not applied to the home directory of the other HDI system. As a result, end users cannot use the most up-to-date files in the home directory of the other HDI system.

  In order to stop access to the home-directory-roaming file system, stop the CIFS service in the **Access Protocol Configuration** dialog box. Then use the **Migration Tasks** dialog box to migrate all files to HCP. When the migration is complete, use the **Check for Errors** dialog box to confirm that no migration-related error occurred. If an error occurred, keep executing the migration tasks until no error occurs.

- If communication with HDI systems is impossible due to a failure in the network or HCP system, you might not be able to access the home-directory. Retry access to the home-directory after recovering from the failure.

Authentication and accounts of CIFS clients

Check the following points regarding the authentication and accounts of CIFS clients:

- For client authentication, use Active Directory authentication. Use user mapping to assign user IDs or group IDs. The same user ID or group ID must be assigned to the account in all the HDI systems.
- Some names cannot be used as user account names. They are the same as the user names that cannot be used when using the automatic home directory creation functionality. For details about the user names that cannot be used when using the automatic home directory creation functionality, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.
- Data in the home directory becomes inaccessible if you change the user name of an account. If you need to change a user name, you must create a new account.

Information to be sent to CIFS administrators

The system administrator must inform CIFS administrators of the following points:

- Do not create any files or directories other than the home directory directly under the shared directory.
- Access only the home directories of the users or groups for which you are assigned as the CIFS administrator. Data inconsistency may occur across HDIs if you access home directories of other users and update the data.
- Do not change the access privileges for home directories.
- Do not rename or delete the home directory. To delete all the data, select and delete the files and subdirectories in the home directory.

Notification to end users

The system administrator must inform the end user who uses the home-directory-roaming file system of the following:

- Assign a network drive to the share of the home-directory-roaming file system, and then start access. If you assign only a host name and then access HDI, the end user may be unable to manipulate the home directory.
- Use a user account that is common among the HDI systems. Make sure that user accounts are not shared by end users.
- To prevent data from failing to update on other HDI systems, log off from the client machine after finishing a task.

- When you access a file or directory at your location, any file or directory that has been changed at other HDI systems will be updated. As a result, accessing a file or directory at your location might take a long time. The time required to access a file or directory varies depending on the number of files or directories that have been updated at other HDI systems.
- Sometimes the home directory temporarily becomes read-only. If you are unable to save a file, temporarily save the file to the client computer. Wait a while, and then update the file in the home directory. If you still cannot update the file, contact the system administrator.
- The home directory might temporarily be empty or contain outdated files or directories. In addition, the client might fail to update files. If such a problem occurs, save any files that should have been updated on the client computer temporarily, log off, wait for about ten minutes, and then retry access.

  The file in the home directory might have been updated. Compare this file with the temporarily saved file before updating it.
- If updated content is not being applied to the file in the home directory, the updated file might be stored in the `.conflict` directory. Check the `.conflict` directory to verify that it does not include any updated file. Data in the `.conflict` directory is automatically deleted when the period to hold the data expires. If the `.conflict` directory is created, check whether there are any necessary files as soon as possible.
- To access the `.conflict` directory, set up the Explorer menu so that all files and folders are displayed.
- If you want to use files in the `.conflict` directory, you must copy the files and place them in a location in the home directory other than the `.conflict` directory before using them. Do not copy the directory when copying the files you want to use. If you copy the directory, access privileges of the files may not be assigned as intended.
- When changing the access privileges of the home directory, you must not assign any access privilege that allow other users to update data.

Tasks required for enabling roaming for home-directory data among HDI systems

HDI administrators at various locations must work with each other to enable roaming for home-directory data among HDI systems.

Use either of the following methods:

- Create a home directory automatically on page 6-49
- Create a home directory manually on page 6-49

Tip: For details on using the roaming service for home directory data migrated from another file server or created by a CIFS administrator among HDI systems, see Appendix G, Performing the Roaming of Migrated Home-directory Data among HDI Systems on page G-1.

Create a home directory automatically

1. 1. On the HDI system at each location, create a home-directory-roaming file system, and then set the system to use the function for automatically creating a home directory to create a file share.

   When a file share is created by using the GUI, the function for automatically creating a home directory is enabled by default.

   Make sure that the following settings are identical across all the linked HDIs:

   - Timestamps of nodes
   - Settings for client authentication
   - Settings for file systems (such as ACL types, the period to hold the data for past versions, and functions to be used)
   - Namespace for the migration destinations

   If an HDI system administrator creates a namespace when creating a file system by using the GUI, the administrator must inform the system administrators of other HDI systems of the namespace name.

   Use the information provided by the HCP administrator if the HCP administrator creates the namespace where data can be accessed from all the HDIs.
2. Tell the end user to assign a network drive to the share for the home-directory-roaming file system, and then start access.

Create a home directory manually

Note: When manually creating a home directory, all the related locations must use HDI with the system version 5.3.*x*-*xx*, 5.4.*x*-*xx* or 6.*x*.*x*-*xx* (*x* represents any number).

1. Create a home-directory-roaming file system, and then set the system to not use the function for automatically creating a home directory to create a file share.

   When a file share is created by using the GUI, the function for automatically creating a home directory is enabled by default. Use the `cifsedit` command to disable the function.
2. Ask a CIFS administrator to manually create a home directory for each end user directly under the mount point of the file system created in step 1.
3. Tell the end user to assign a network drive to the share created in step 1 before access the share.
4. Confirm that the migration task for the file system created by using the GUI in step 1 completed successfully.

   Do not create a home directory for the same end user on another HDI until the migration completes.
5. The HDI system administrator in step 1 asks the other HDI system administrator to create a home-directory-roaming file system.

   At this time, provide the following information:

- Timestamps of nodes
- Settings for client authentication
- Settings for file systems (such as ACL types, the period to hold the data for past versions, and functions to be used)
- Namespace for the migration destinations

If a namespace was created when a file system was created by using the GUI, the administrator must be informed of the namespace name that was automatically created.

In addition, if the HCP administrator creates a namespace where data can be accessed from all the HDI systems, inform them of the information provided by the HCP administrator.

6. Create a home-directory-roaming file system on the other HDI system, and then set the system to not use the function for automatically creating a home directory to create a file share.

   When a file share is created by using the GUI, the function for automatically creating a home directory is enabled by default. Use the `cifsedit` command to disable the function.

   Make sure that the settings listed in step 5 are identical across all the linked HDI systems.

7. Inform the end user of the following:

   - Assign a network drive to the share created in step 6 before accessing the share.
   - Log in the system by using the home directory created in step 2.

Sharing data among HDI systems using the read-write-content-sharing functionality

With the read-write-content-sharing functionality, HDI systems at different locations can share data via linked HCP systems. This allows any end user who uses an HDI system to read and write any files created in other HDI systems.

Note: The use of the read-write-content-sharing functionality requires you to link an HDI system of version 5.1.3-00 or later with an HCP system of version 6.1 or later.

If it is possible to share the data of a file system among HDI systems, such a file system is referred to as an "read-write-content-sharing file system".

A read-write-content-sharing file system is suitable for such applications where one user updates the files that will be referenced from different locations (reference sharing) and for such applications where multiple users update files in turn as per a rule (work flow). In contrast, this file system is not suitable for any applications emphasizing system performance (such as video streaming) or any applications where data shall be synchronized immediately after it is updated. To avoid losing any update information due to a conflict of operations regarding the same file, the end user must download

the files to his or her client machine, edit them in the machine, and upload the updated ones to a read-write-content-sharing file system.

The following figure shows the exemplar usage of sharing data among HDI systems using the read-write-content-sharing functionality.

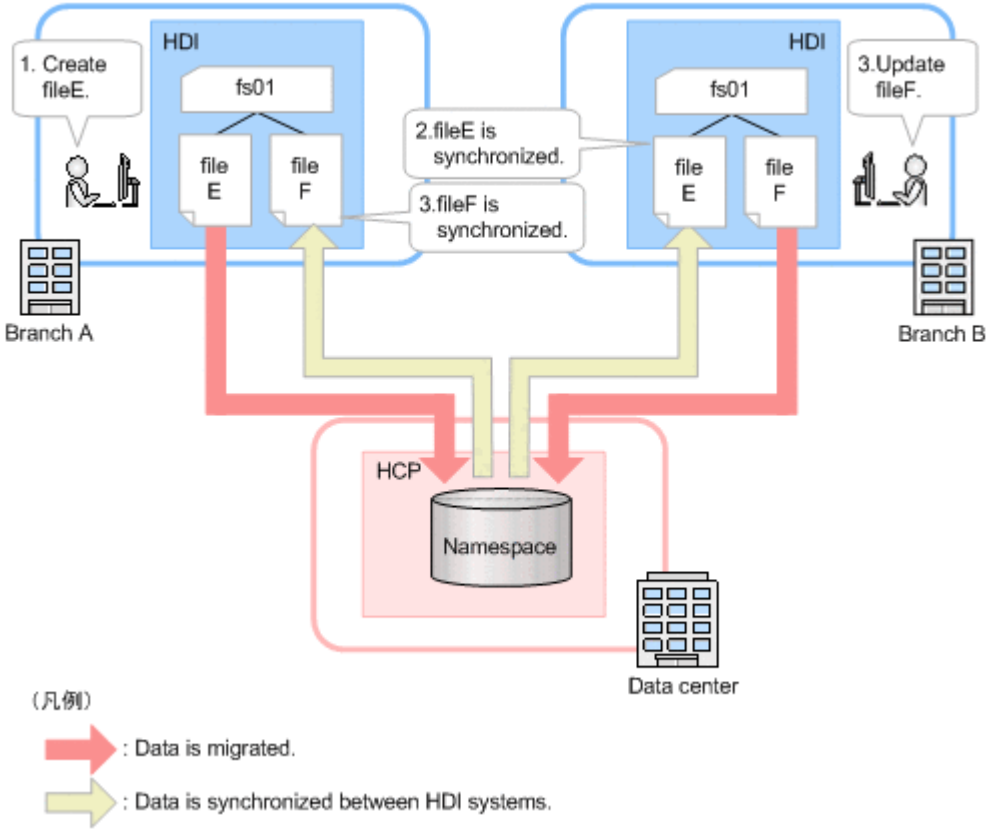


Figure 6-11 Sharing data among HDI systems using the read-write-content-sharing functionality

The following events will cause any information updated in a certain location to be applied to an HCP system:

- When an end user handles (creates, renames, or deletes) any contents of a directory, the update information of the directory is applied to the HCP system. If a directory is handled from multiple locations at the same time, the operations are applied to the HCP system one-by-one.
- The data of updated files and directories are migrated to the HCP system every 10 minutes.

In addition, the following events will cause any information updated by one location to be applied to another location after the information is applied to the HCP system. It takes approximately 30 minutes at maximum to apply the information on any file updated in one location to a file system in another location.

- When an end user handles (creates, renames, or deletes) the contents of a directory, any directory information updated at different locations is applied to the file system at his or her location.

- When an end user references any file or directory updated at a different location, the update information of the referenced file or directory is applied to the file system at the location of the end user.
- At the time that the updated data of files and directories is migrated to the HCP system every 10 minutes, the information of files and directories updated at different locations is applied to the file system of the location of the end user.

If update information of one location is applied to an HCP system before update information of another location is applied to the HCP system, when the update information of the former is applied to the latter, the files in conflict of the latter will be saved in either of the directories described below. Use the `arcconfedit` command to specify the save destination directory. The system administrator must notify the end user about which directory will be used as a storage location for files in conflict.

The directory in which the file in conflict was originally stored (default setting)

The length of the file path must be no more than 187 characters. If a file whose path length exceeds the maximum is in conflict, to prevent the file from becoming unavailable for viewing, the file will be stored in the `.conflict_longpath` directory just below the mount point of the file system, not in the directory in which the file in conflict was originally stored. Ask, as needed, the CIFS administrator or the `root` user (NFS client) to whom anonymous mapping is not applied, to copy the files that have been moved to the `.conflict_longpath` directory to a directory that the end user can access.

The `.conflict` directory just below the mount point of the file system

For NFS clients, the length of the file path must be no more than 1,024 bytes. For CIFS clients, the length must be no more than 190 characters. If a file whose path length exceeds the maximum is in conflict, the files stored in the `.conflict` directory can no longer be opened or copied to a directory other than the `.conflict` directory.

The data in the `.conflict` and `.conflict_longpath` directories are automatically deleted when the retention period expires (the default setting is four days). You can change the retention period by using the `arcconfedit` command.

Points to be checked before sharing data among HDI systems using the read-write-content-sharing functionality

This subsection describes the points to be checked for sharing data among HDI systems using the read-write-content-sharing functionality.

Tenants and namespaces at the migration destination

Check the following points regarding the tenants and namespaces of the HCP system in use:

- Specify the same tenant and namespace as the migration destination in all the linked HDI systems.

Character strings are case sensitive. If you specify a different character case for corresponding character strings, the updated file and directory information is not correctly applied to the HDI systems in different sites.

Up to 100 HDI systems can be linked.

- When you create a read-write-content-sharing file system via the GUI, the namespace for storing the setting information of the read-write-content-sharing functionality is automatically created (`rwcs-system`). When you use the read-write-content-sharing functionality, the namespace is required for each tenant.
- A namespace corresponding to a read-write-content-sharing file system cannot be specified as the migration destination of any file system other than the read-write-content-sharing file system.

Management of read-write-content-sharing file systems

Note the following points regarding the management of read-write-content-sharing file systems:

- Use the same character code in all the linked HDI systems.
- Allocate the namespaces of the migration destination at the file system level.
- No read-write-content-sharing file system can be mounted in read-only mode.
- A read-write-content-sharing file system creates a share for the mount point, while the file system does not support the configuration of a share created in any subdirectory other than the mount point.
- The following functions are not available in any read-write-content-sharing file system:
  - Using the WORM functionality
  - Management of the Quota and subtree Quota
  - Using the NDMP functionality
  - Importing data from other file servers
  - Setting of the cache residency policy
  - Using the home-directory-roaming functionality
  - Using the Large File Transfer functionality
- Set up the read-write-content-sharing file system to prohibit hard link creation. If hard links are created, there is a risk of data inconsistency between HDI systems. In addition, deleting created hard links might become difficult.
- To avoid the risk of operation without the application of different locations, set up CIFS share not to use a read-only client cache.
- A proper task is automatically established when a read-write-content-sharing file system is created. Do not change any migration policy setting.
- We recommend creating one read-write-content-sharing file system for one HDI system.

In addition, when you concurrently operate the read-write-content-sharing file systems, the home-directory-roaming file systems, and the file systems that migrate data to the HCP system, you need to limit the total number of file systems to up to four.

- Increasing the number of migration tasks to be executed concurrently puts a heavier load on the system. If too many migration tasks are executing concurrently, putting a heavy load on the system, adjust the schedule so that fewer migration tasks execute concurrently.
- Make sure that no more than 12,000 client connections using the read-write-content-sharing file systems in all the linked HDI systems exist.
- If the number of end users that use the read-write-content-sharing file system increases, or the number of files to be created or updated increases, migration might not finish within 10 minutes, and it might take a long time for the update information of a certain location to be applied to another location. Therefore, adjust the number of end users and number of files so that migration finishes within 10 minutes.
- If communication with any HDI system is impossible due to failure in the network or HCP system, no file system can be operated. In such a case, all access from end users is blocked as an I/O error. Restart the file system after recovery from such failures.
- If you stop the HDI systems for routine maintenance, after asking the end users in advance to stop accessing to share, shut down the processing node. As you click **Shutdown Node** in the **File Servers** tab of the **Processing Nodes** subwindow, the number of days of retention until pruning, which is assigned to the namespace, is displayed. Do not use the **Cluster Management** dialog box to stop nodes, as the number of days of retention until pruning is not displayed. If the planned HDI shutdown period exceeds the number of days of retention until pruning, the resource group must be restarted to restore data from the HCP system. This is to prevent any error caused by a directory operation or migration when restarting operation. For details about how to recover a read-write-content-sharing file system, see the *Troubleshooting Guide*.
- When you recover from an HDI OS failure or turn the power on again after a shutdown of HDI power, the resynchronization process will be performed for all files and directories in the shares for recovering consistency with the HCP system (excluding the files and directories in the `.conflict` and `.conflict_longpath` directory). At this time, any updated files not migrated to the HCP system are stored in the `.conflict` directory, if any. All the files in shares become stub files, degrading access performance temporarily.
- A user who performs CIFS access to a read-write-content-sharing file systems, can belong to a maximum of 700 groups, including the primary group.

Notification to end users

The system administrator must notify end users who use the read-write-content-sharing file system of the following points:

- If, before an update file is migrated to an HCP system, a conflict occurs in a directory containing the updated file due to the directory being deleted, moved, or renamed at a different location, the updated file in the directory will be deleted without being saved. Be very careful when deleting, moving, or renaming a directory, as doing so might affect the operation of other locations.
- If a directory with the same name is already created at another location, Explorer might abnormally terminate.

  If this occurs, re-create the directory by using another name because creation of the directory failed.
- Do not directly handle any file or directory in shares from your application. Instead, download and edit them on your client machine, and then apply them to the read-write-content-sharing file systems.
- It takes approximately 30 minutes at maximum to apply the update of any files or directories at another location to the files or directories at your location.
- When you access a file or directory at your location, any file or directory that has been changed at another location will be updated. As a result, accessing a file or directory at your location might take a long time. The time required to access a file or directory varies depending on the number of files or directories that have been updated at other locations.
- When you operate a directory from an NFS client, the processing might take a long time. During that time, the message "`file temporarily unavailable on the server, retrying...`" might be output to the NFS client.
- In case you encounter an I/O error in the operation of files or directories, try again after waiting a while. If you encounter the error again, contact the system administrator.
- If you change only the access right of a file or directory, the change in the access right might be canceled when it is in conflict with another update to the same file from another location.
- Any operation containing continuous processing for a large amount of files and directories, such as the copy or deletion of a directory tree, a change in the inherited access right, or the decompression of files, can take substantial time to complete, and temporarily degrade access performance for all the linked HDI systems.
- Do not store a large or frequently updated file, such as that for a database or a virtualization environment, in the read-write-content-sharing file system. This prevents data synchronization between locations and causes system degradation due to the frequent synchronization.
- Do not create any socket files on read-write-content-sharing file systems. If socket files are created, part of the data is not synchronized between distributed locations. In addition, there is a risk of data inconsistency between distributed locations.
- If a file updated by an end user is in conflict with a file updated at a different location, the file updated by the end user will be saved when the update information of the different location is applied to the location of the end user. Contact the system administrator about the details of the

save destination directory. Use the saved file to recover the file in a file share.

When the updated file is saved in the directory in which the file in conflict was originally stored

The file is saved in the following name:

name-of-the-file-in-conflict(*HDI-host-name_time-the-file-in-conflict-was-updated*(mtime)[*number*#1]).*extension-of-the-file-in-conflict*#2

#1:

This number is assigned when file names are duplicated.

#2:

For files with an extension that is sequentially assigned, the extension of the saved file will be different from that of the original file. If the extension of the saved file is different from the original file, rename the file manually.

When the file is saved in the `.conflict` directory

The save destination for each client is as follows:

For a CIFS client:

*node-name-or-IP-address**CIFS-share-name*\.conflict*date-of-the-move-to-the-.conflict-directory**path-of-the-file_date-of-the-update-of-the-file*

For an NFS client:

client-mount-point/.conflict/*date-of-the-move-to-the-.conflict-directory*/*path-of-the-file_date-of-the-update-of-the-file*

- Any data in the `.conflict` directory is automatically deleted when the retention period expires. Copy the data to any location other than the `.conflict` directory before the deletion.
- To access the `.conflict` directory, set up the Explorer menu so that all files and folders are displayed.
- In the `.conflict` directory, different data is stored for each location.
- The data in the `.conflict` directory is the data shared among all end users at your location.
- If an end user and another end user at another location handle the same directory at the same time, the operation of one of them is applied first, and then the operation of the other user is applied to the system.
- Operations from multiple locations on the same directory are under exclusive control via the HCP system. If any linked HDI system encounters an OS failure or shutdown during the operation of a directory, you cannot update the directory for up to an hour.
- When the system administrator has specified the settings so that a file in conflict with an update from a different location is stored in the directory in which the file in conflict was originally stored, be sure to restrict the path length of the file in the directory to 187 characters. If the files in conflict cannot be found in the directory, contact the system administrator.

When the system administrator has specified the settings so that a file in conflict with an update from a different location is stored in the `.conflict` directory, if the file path is too long, the file can no longer be opened or copied to locations other than the `.conflict` directory. For this reason, be sure to restrict the path length of the file to 1,024 bytes for NFS clients (or for a file name, 235 bytes) and 190 characters for CIFS clients.

- If a failure occurs on an HDI system or data is updated at another location, the files in the HDI system will be regenerated for synchronization with the latest HCP data. To view the latest data updated at another location, reopen the file. If an opened file is regenerated, an error occurs during the processing to update the file. In this case, open the file again before updating the file.
- If a resource group restarts after error recovery, restoration is automatically performed. At that time, files that have not been migrated to HCP are saved in the following format:

  For a CIFS client:

  *node-name-or-IP-address**CIFS-share-name*\.conflict\restore_*date-of-the-move-to-the-.conflict-directory**path-of-the-file*

  For an NFS client:

  client-mount-point/.conflict/restore_*date-of-the-move-to-the-.conflict-directory*/*path-of-the-file*

Tasks required for sharing data among HDI systems using the read-write-content-sharing functionality

To share data among HDI systems using the read-write-content-sharing functionality, the system administrators of the locations must create a read-write-content-sharing file system and create a file share so that data is migrated to the same tenants and namespaces.

Specify the following setting items so that all the HDI systems have the same setting:

- Timestamps of nodes
- Settings for client authentication
- Settings regarding file systems and file shares (including the ACL type, retention period of past versions, and functionality in use)
- Settings regarding the migration-destination tenants and namespaces

The migration-destination namespaces are automatically created when you specify HCP namespace information on the GUI. The system administrator who created the migration-destination namespace must inform other HDI system administrators in advance of the namespace. If the HCP administrator created the namespaces, specify the information notified by the HCP administrator.

Note: If the same file is updated from multiple HDI systems before synchronizing data among the HDI system, a conflict is caused during the next synchronization.
You can change the storage directory for files in conflict or the retention period for files stored in the `.conflict` or `.conflict_longpath` directories by using the `arcconfedit` command. Make sure to use the same settings for all the linked HDI systems.

Recovering HDI systems by restoring HCP data

If an HDI system is linked with an HCP system, a batch operation can be performed to restore the system settings information and user data if a problem occurs on an OS disk, the cluster management LU, or a user LU in the HDI system. Confirm that all files are subject to migration and the system settings information file is periodically saved to an HCP system. The system settings information file is saved with the name `sysbk_`*ID-automatically-assigned-to-HDI-system*`.1` or `sysbk_`*ID-automatically-assigned-to-HDI-system*`.2` in the HCP namespace used for storing system settings information (`system-backup-data`).

Note that you cannot restore the information below because the information below is not saved to HCP systems. Record the settings information as necessary.

- The configuration information for the file system that was not mounted when saving the information, including:
  - The minimum and maximum retention periods
  - The autocommit settings
  - Whether to issue warning messages regarding file system capacity shortages
  - Whether to enable the automatic failover functionality in the event of a file system becoming blocked
  - Whether to record file creation dates and times
- Settings information of the initial mode that is used when executing migration tasks
- User data that has not been migrated to an HCP system
- The configuration information for 64-bit inodes

Restored file systems are set to disallow creation of hard links.

In addition, you need to back up the following information to storage media that is external to the system every time the following information is updated:

Storage system configuration information

If the storage system being used is in the Hitachi AMS2000 series or the HUS100 series, use Hitachi Storage Navigator Modular 2 to download the following settings information:

- Configuration information file for parity groups and logical units
- Configuration information file for port information
- Configuration information file for system parameters

For details on how to use Hitachi Storage Navigator Modular 2, see the Hitachi Storage Navigator Modular 2 manuals.

File system information

On the node on which the resource group containing the target file system is running, execute the `fslist` command with the `-t` and `-w` options specified, and make a record of the displayed file system settings information.

CIFS and NFS share information

Use the `cifsbackup` and `nfsbackup` commands to back up CIFS and NFS share information. If both CIFS shares and NFS shares have been set up in a file system, you need to execute both the `cifsbackup` and `nfsbackup` commands.

Correspondence with namespaces

Record the relationship between namespaces and file systems or file shares. If a namespace is created automatically after you use the GUI to set the namespace information of an HCP system, the namespace is given a name automatically in the format given below.

For namespaces allocated to the file system:

file-system-name–ID-automatically-assigned-to-HDI-system

For namespaces allocated to the share:

file-system-name–ID-automatically-assigned-to-HDI-system–string-specified-by-user-when-namespace-was-allocated

7

Installing Hitachi File Services Manager and Setting Up Its Environment

This chapter describes how a system administrator can install Hitachi File Services Manager and set up the environment on the management server when running an HDI system in a cluster configuration.

Installing and uninstalling Hitachi File Services Manager

The following sections describe how to install and uninstall Hitachi File Services Manager.

Before installation:

- See Prerequisites for installing Hitachi File Services Manager on page 7-12.
- If the management server is running in a cluster configuration, see Installing and uninstalling Hitachi File Services Manager (if the management server is running in a cluster configuration) on page 7-16.

Performing a new installation of Hitachi File Services Manager

This section describes how to perform a new installation of Hitachi File Services Manager.

To perform a new installation of Hitachi File Services Manager:

1. Insert the installation media for Hitachi File Services Manager.

   If you want to copy the contents of the installation media, you must copy them to a local disk of the management server. You cannot perform an installation by using data on the network drive.
2. Use Explorer to view the contents of the installation media, and then execute `HFSMinst.exe`.

   The license agreement dialog box appears.

   If a Hitachi Command Suite product has already been installed in the root of a disk drive, the installation process will be interrupted. To prevent this, uninstall the Hitachi Command Suite product or re-install the Hitachi Command Suite product in a directory other than the root of a disk drive, and then install Hitachi File Services Manager.
3. Read the terms, and then click the **Yes** button.

   The **Welcome to the Installation of Hitachi File Services Manager (New Installation)** dialog box appears.

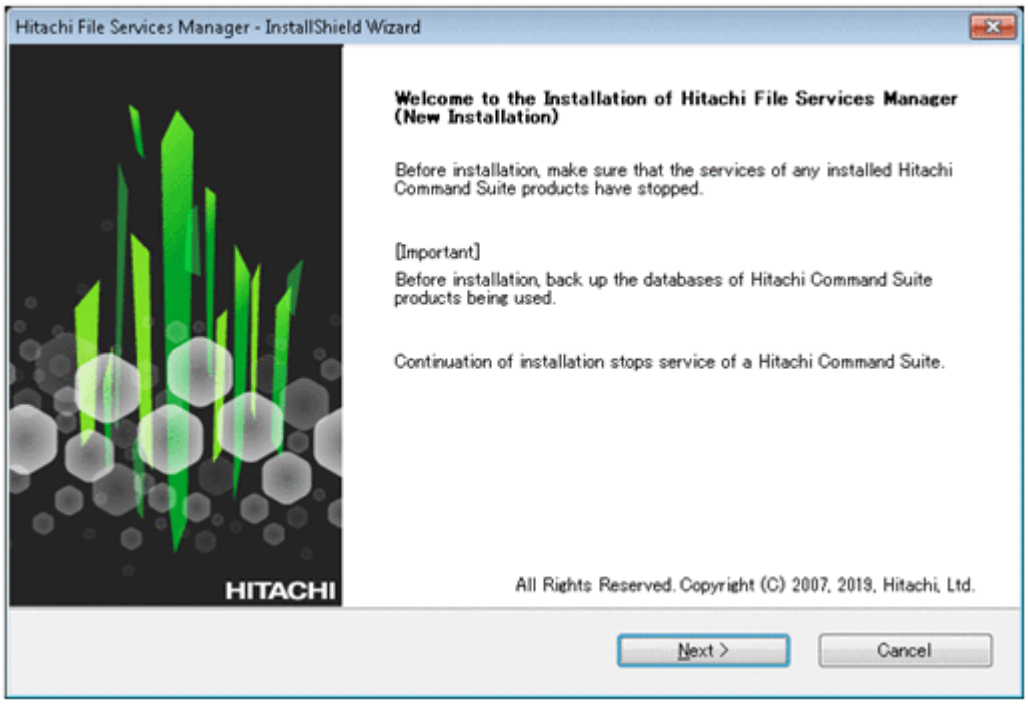


Figure 7-1 Welcome to the Installation of Hitachi File Services Manager (New Installation) dialog box

Note:

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

4. Check the information displayed in the dialog box, and then click the **Next** button.

   The operation to be performed after you click the **Next** button depends on whether Hitachi Command Suite products have been installed on the computer on which you are installing Hitachi File Services Manager.

   If Hitachi Command Suite products have been installed:

   The **Confirmation of the Setup Status of the Hitachi Command Suite Common Component Database** dialog box appears.

   This dialog box indicates how the installed Hitachi Command Suite products have been configured. After checking the configuration, click the **Next** button to display the **Setup of the Installation Folder** dialog box.

   If Hitachi Command Suite products have not been installed:

   The **Setup of the Installation Folder** dialog box appears.

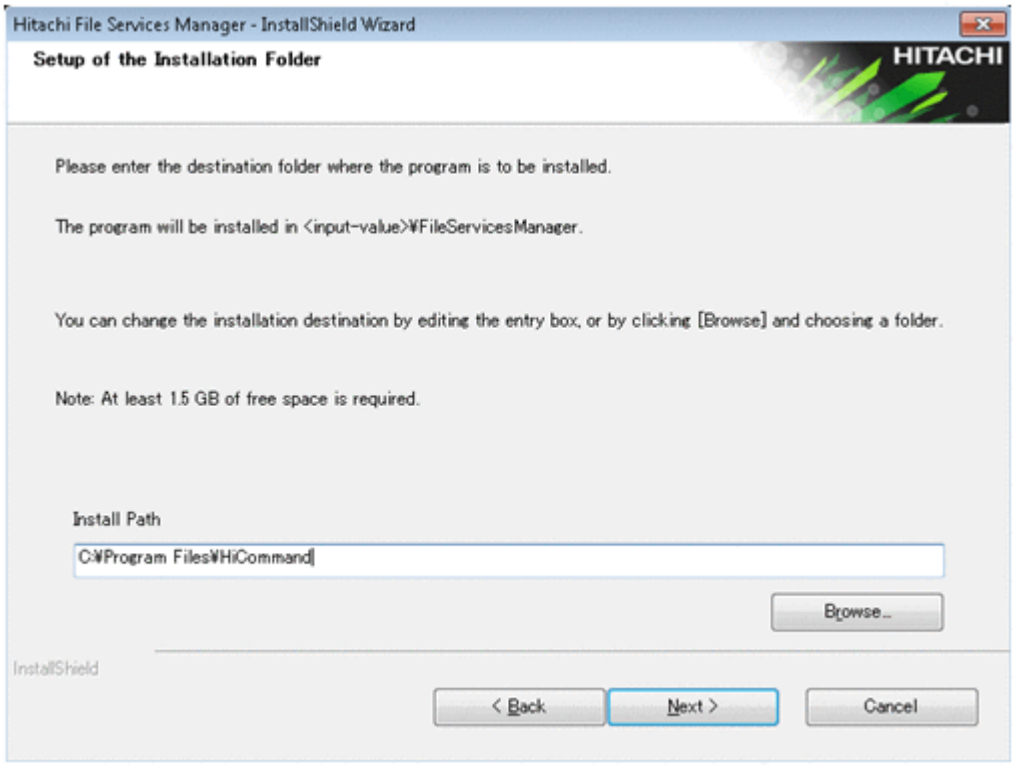


Figure 7-2 Setup of the Installation Folder dialog box

Specify the installation destination based on the following rules:

- You cannot specify the root of a disk drive (for example, `C:\` or `D:\`) as the installation destination. A folder name must be specified.
- Folders on the network drive or removable media cannot be specified. You must specify a folder on a local disk of the management server.
- Specify an absolute path, using no more than 64 bytes.
- For the path, you can use alphanumeric characters, left parentheses (`(`), right parentheses (`)`), periods (`.`), underscores (`_`), and space characters. However, you cannot specify a period (`.`) at the beginning or end of the path. Also, you cannot specify a space character at the beginning or end of the path, nor can you specify consecutive space characters.
- You can use backslashes (`\`) as path delimiters. However, the path cannot end with a backslash.
- Do not specify a symbolic link or junction.

The following shows the installation folders of Hitachi File Services Manager and Hitachi Command Suite Common Component when the installation destination is specified.

The installation destination for Hitachi File Services Manager:

absolute-path-specified-as-the-installation-destination`\FileServicesManager\`

The installation destination for Hitachi Command Suite Common Component:

absolute-path-specified-as-the-installation-destination\Base64\

If any Hitachi Command Suite product has already been installed on the computer on which you are installing Hitachi File Services Manager, the installer will overwrite the existing version of Hitachi Command Suite Common Component instead of installing it in the specified folder.

5. Specify the installation destination, and then click the **Next** button.

The **Specify the Storage Destination for Database Files of Hitachi File Services Manager** dialog box appears.

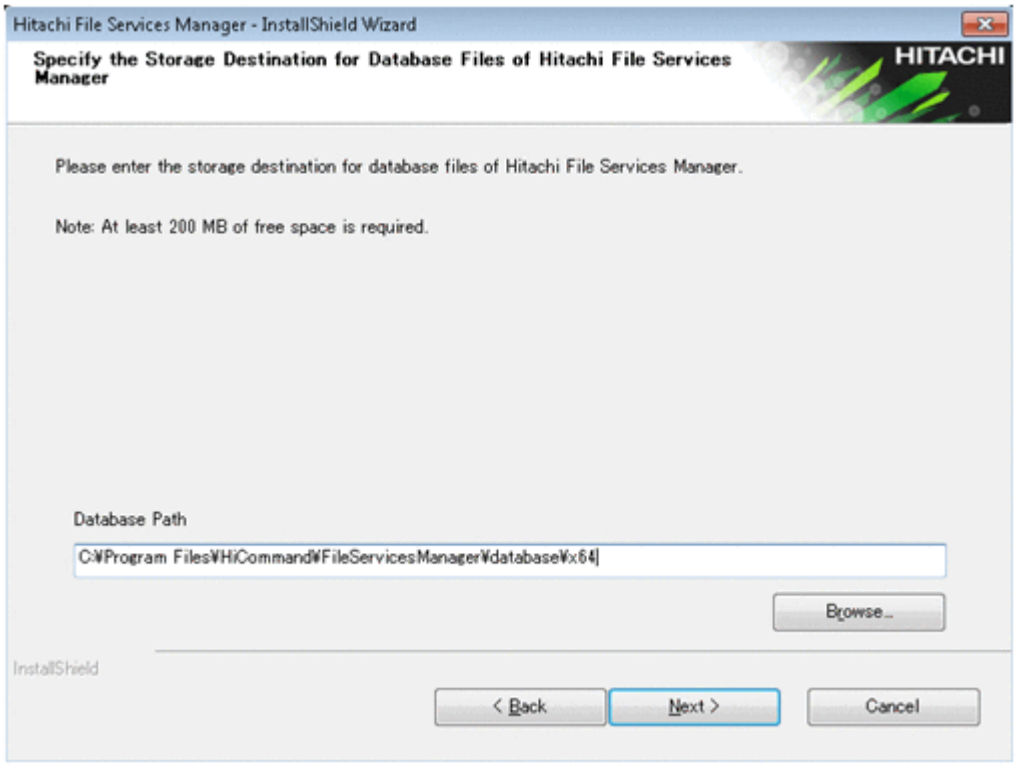


Figure 7-3 Specify the Storage Destination for Database Files of Hitachi File Services Manager dialog box

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

- Specify an absolute path, using no more than 90 bytes.
- For the path, you can use alphanumeric characters, left parentheses ((), right parentheses ()), periods (.), underscores (_), and space characters. However, you cannot specify a period (.) at the beginning or end of the path. Also, you cannot specify a space character at the beginning or end of the path, nor can you specify consecutive space characters.
- You can use backslashes (\) as path delimiters. However, the path cannot end with a backslash.

6. Specify the folder for storing database files, and then click the **Next** button.

   The operation you perform after clicking the **Next** button differs depending on whether Windows Firewall is installed.

   If Windows Firewall is installed:

   The **Registration into the Windows Firewall Exceptions List** dialog box appears. Check the information displayed in the dialog box, and then click the **Next** button. The **Confirmation Before Installation** dialog box appears.

   If Windows Firewall is not installed:

   The **Confirmation Before Installation** dialog box appears.

7. Make sure that the specified information is correct, and then click the **Install** button.

   Installation starts and a series of dialog boxes indicating the processing status appear. If the installation is successful, the **Installation Complete** dialog box appears.

   Notes:

   - Clicking the **Install** button automatically imports the SSL certificate into the following keystore file:

     Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\jdk\jre\lib\security\jssecacerts

     The default password is `changeit`. After installation, execute the following command on the management server to change the password:

     ```
     Hitachi-Command-Suite-Common-Component-installation-folder\bin
     \hcmds64keytool -storepasswd -keystore Hitachi-Command-Suite-Common-
     Component-installation-folder\uCPSB\jdk\jre\lib\security\jssecacerts -
     storepass current-changeit-password -new new-password
     ```

   - If the password for the management server keystore file (`jssecacerts`) has been set, an error dialog box appears before the **Installation Complete** dialog box is displayed. Check the information displayed in the dialog box, and then click the **OK** button. After the installation is complete, import the SSL certificate to the management server. For details on how to import the SSL certificate to the management server, see Importing the required SSL certificate for communication between the node and management server on page 7-99.

8. Click the **Finish** button to complete the installation.

   If the management server is in a non-cluster configuration, the Hitachi Command Suite Common Component services start and Hitachi File Services Manager is ready for operation.

   If the management server is in a cluster configuration, continue the setup required to run the management server in a cluster configuration. For details on how to install Hitachi File Services Manager on a management server in a cluster configuration, see Installing and uninstalling Hitachi

File Services Manager (if the management server is running in a cluster configuration) on page 7-16.

Performing an upgrade or overwrite installation of Hitachi File Services Manager

This section describes how to perform an upgrade or overwrite installation of Hitachi File Services Manager on the management server on which Hitachi File Services Manager has already been installed.

On the management server on which Hitachi File Services Manager has been installed, you can update the version of Hitachi File Services Manager by installing a newer version as an upgrade installation. If you update the OS version of the node on which Hitachi File Services Manager has been installed, always update Hitachi File Services Manager to the latest version by performing an upgrade installation.

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

Note:

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

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

1. Insert the installation media for Hitachi File Services Manager.

   If you want to copy the contents of the installation media, you must copy them to a local disk of the management server. You cannot perform an installation by using data on the network drive.
2. Use Explorer to view the contents of the installation media, and then execute `HFSMinst.exe`.

   The license agreement dialog box appears.
3. Read the terms, and then click the **Yes** button.

   The **Welcome to the Installation of Hitachi File Services Manager (Upgrade)** dialog box or the **Welcome to the Installation of Hitachi File Services Manager (Overwrite)** dialog box appears. The following shows an example of the dialog box displayed when an overwrite installation is performed.

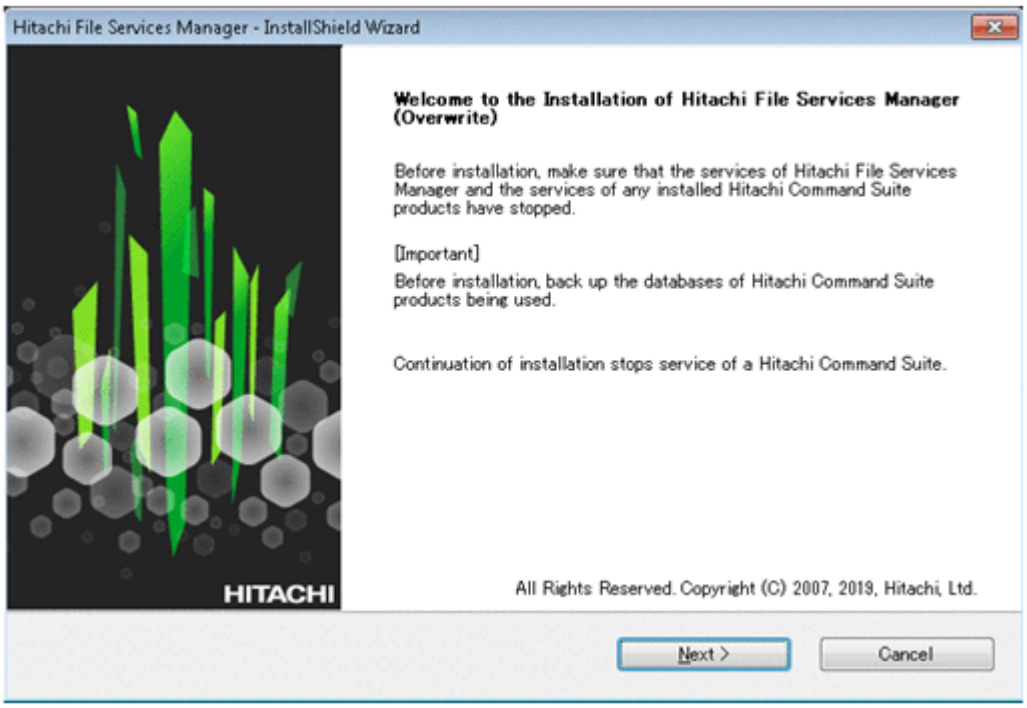


Figure 7-4 Welcome to the Installation of Hitachi File Services Manager (Overwrite) dialog box

Note:

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

4. Check the information displayed in the dialog box, and then click the **Next** button.

   The **Confirmation of the Setup Status of the Hitachi Command Suite Common Component Database** dialog box appears.

   This dialog box indicates how the installed Hitachi Command Suite products have been configured.

5. Check the configuration, and then click the **Next** button.

   The **Confirmation Before Installation** dialog box is displayed.

   If the management server does not contain the Hitachi File Services Manager database, the **Specify the Storage Destination for Database Files of Hitachi File Services Manager** dialog box appears before the **Confirmation Before Installation** dialog box. If this dialog box appears, specify the database file storage folder, and then click the **Next** button to continue installation.

   The following figure shows the **Specify the Storage Destination for Database Files of Hitachi File Services Manager** dialog box.

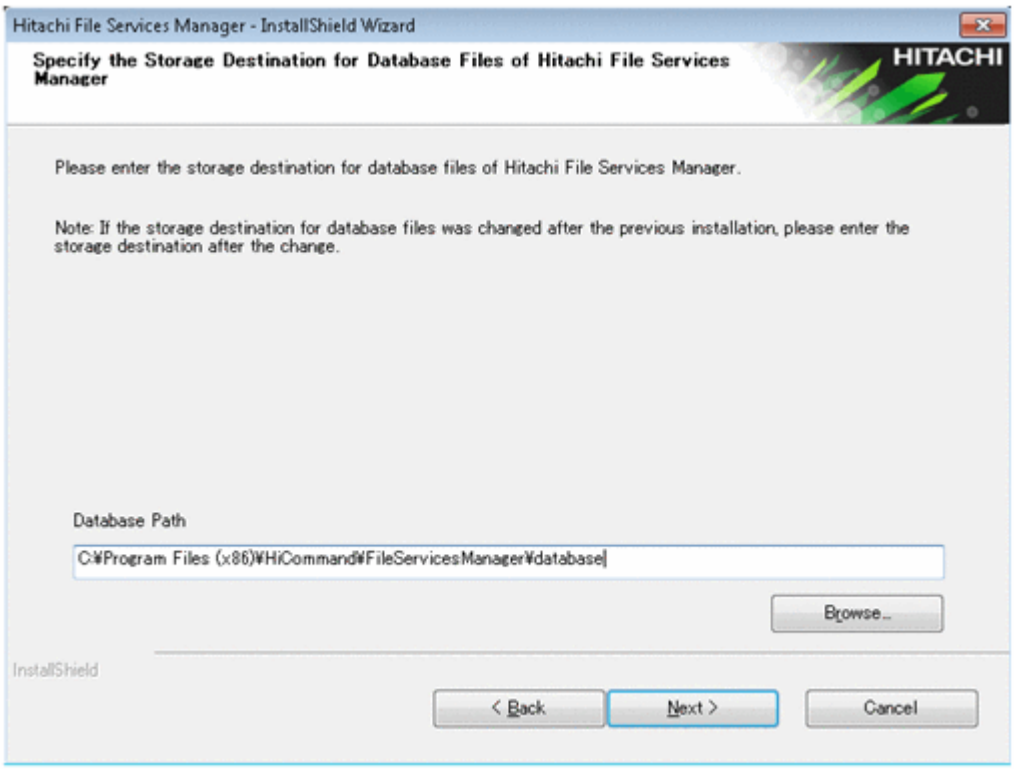


Figure 7-5 Specify the Storage Destination for Database Files of Hitachi File Services Manager dialog box (for an installation other than a new installation)

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

- Specify an absolute path, using no more than 90 bytes.
- For the path, you can use alphanumeric characters, left parentheses (( ), right parentheses ( )), periods (.), underscores (_), and space characters. However, you cannot specify a period (.) at the beginning or end of the path. Also, you cannot specify a space character at the beginning or end of the path, nor can you specify consecutive space characters.
- You can use backslashes (\ ) as path delimiters. However, the path cannot end with a backslash.

6. Make sure that the specified information is correct, and then click the **Install** button.

   Installation starts and a series of dialog boxes indicating the processing status appear. If the installation is successful, the **Installation Complete** dialog box appears.

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

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

Note:

If the password for the management server keystore file (`jssecacerts`) has been set, an error dialog box appears before the **Installation Complete** dialog box is displayed. Check the information displayed in the dialog box, and then click the **OK** button. After the installation is complete, import the SSL certificate to the management server. For details on how to import the SSL certificate to the management server, see Importing the required SSL certificate for communication between the node and management server on page 7-99.

7. Click the **Finish** button to complete the installation.

   If the management server is in a non-cluster configuration, the Hitachi Command Suite Common Component services start and Hitachi File Services Manager is ready for operation.

   If the management server is in a cluster configuration, continue the setup required to run the management server in a cluster configuration. For details on how to install Hitachi File Services Manager on a management server in a cluster configuration, see Installing and uninstalling Hitachi File Services Manager (if the management server is running in a cluster configuration) on page 7-16.

Uninstalling Hitachi File Services Manager

This section describes how to uninstall Hitachi File Services Manager.

Removing Hitachi File Services Manager prerequisites

The following describes the tasks that you need to carry out before uninstalling Hitachi File Services Manager.

- Log on to Windows as an Administrator or a member of the Administrators group.
- Stop Hitachi File Services Manager and Hitachi Command Suite product services.
- Back up Hitachi File Services Manager and the Hitachi Command Suite product databases.
- If a security monitoring program has been installed, either stop it or change its settings so that it does not hamper uninstallation of Hitachi File Services Manager.
- If an antivirus program has been installed, stop the program, and then uninstall Hitachi File Services Manager.

  You might not be able to uninstall Hitachi File Services Manager while an antivirus program is running. If an uninstallation attempt fails, take action according to the message displayed in the error dialog box.
- If a process monitoring program is installed, stop it or change its settings so that the services and processes of Hitachi File Services Manager and Hitachi Command Suite Common Component are not monitored.

If a process monitoring program starts or stops the services or processes of Hitachi File Services Manager and Hitachi Command Suite Common Component during uninstallation of Hitachi File Services Manager, the uninstallation might fail.

- Close all windows used for operating Windows services.

Performing an uninstallation

To uninstall Hitachi File Services Manager:

1. Open the **Uninstallation of Hitachi File Services Manager** dialog box.
   You can use one of the following methods to open this dialog box:
   - Choose **Start**, **Programs**, **Hitachi Command Suite**, **File Services Manager**, and then **Uninstall - HFSM**.
   - Select **Uninstall - HFSM** from the application list in the Start screen.
   - From the Windows **Programs and Features**, select **Hitachi File Services Manager** and then click the **Uninstall**.

   The **Uninstallation of Hitachi File Services Manager** dialog box appears.

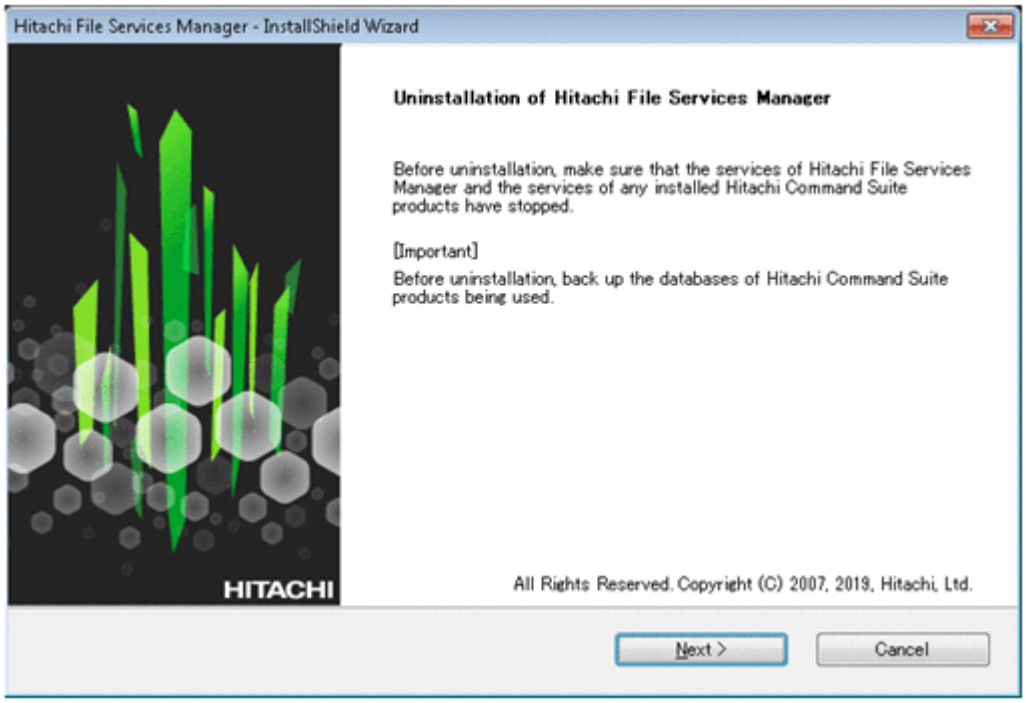


Figure 7-6 Uninstallation of Hitachi File Services Manager dialog box

2. Check the information displayed in the dialog box, and then click the **Next** button.
   The **Confirmation of the Setup Status of the Hitachi Command Suite Common Component Database** dialog box is displayed.
   This dialog box indicates whether the Hitachi Command Suite products have been installed on the management server in a non-cluster

configuration, or on the executing or standby node of the management server in a cluster configuration.

3. Check the setup status, and then click the **Next** button.

   The **Confirmation Before Uninstallation** dialog box appears.

4. Make sure that Hitachi File Services Manager version and installation destination displayed in the dialog box are correct, and then click the **Uninstall** button.

   Uninstallation starts and a series of dialog boxes indicating the processing status appear. If the uninstallation is successful, the **Uninstallation Complete** dialog box appears.

5. Click the **Finish** button to complete the uninstallation of Hitachi File Services Manager.

Prerequisites for installing Hitachi File Services Manager

Check the following before installing Hitachi File Services Manager.

Other products installed on the computer on which you will install Hitachi File Services Manager:

Make sure that the versions of Hitachi Command Suite products are 4.0 or later. Also make sure that a large configuration does not include Tuning Manager.

The environment of the computer on which you will install Hitachi File Services Manager:

- Make sure that the computer meets the requirements for Hitachi File Services Manager.

  For details on the requirements, see Requirements for a management server on page 3-5.

- If you are performing a new installation of Hitachi File Services Manager, make sure that the target disk drive has sufficient free space for installing the software.

  The following table lists the components to be installed and the amount of free space required to install each component.

Table 7-1 Components to be installed and free space required for installation

Component	Required free space
Hitachi File Services Manager	At least 4 GB
Hitachi File Services Manager database files	At least 200 MB

  The Hitachi File Services Manager and Hitachi File Services Manager database files can be installed on separate disk drives.

- To perform a version upgrade installation, you need sufficient disk space as specified in the management server requirements (minimum: 7 GB, recommended: at least 8 GB). If you perform

upgrade installation with minimum capacity of disk space, the time that installation takes become longer.

- Make sure that the port numbers listed in Table 7-2 Ports used by Hitachi File Services Manager and Hitachi Command Suite Common Component on page 7-13 are different from those used by other programs installed on the same management server.

  If a product other than Hitachi File Services Manager or a Hitachi Command Suite product is using one of these port numbers, change the settings for the applicable product. For details about how to change port numbers in Hitachi File Services Manager, see Changing the port numbers used by Hitachi Command Suite Common Component on page 7-90.

Table 7-2 Ports used by Hitachi File Services Manager and Hitachi Command Suite Common Component

Port number	Description
22015/tcp#	Used for accessing the HBase 64 Storage Mgmt Web Service when communicating with management clients (GUI). This port number can be changed.
22016/tcp	Used for accessing the HBase 64 Storage Mgmt Web Service when performing SSL communication with management clients (GUI). This port number can be changed.
22017/tcp to 22030/tcp 22033/tcp 22034/tcp 22130/tcp to 22133/tcp	Reserved by Hitachi File Services Manager and Hitachi Command Suite Common Component.
22031/tcp	Used internally for Hitachi Command Suite Common Component communication (single sign-on). This port number can be changed.
22032/tcp	Used internally for Hitachi Command Suite Common Component communication (HiRDB). This port number can be changed.
22035/tcp 22037/tcp 22038/tcp	Used internally for Hitachi Command Suite Common Component communication (communication with the Web server). This port number can be changed.
22036/tcp	Used internally for Hitachi Command Suite Common Component communication (naming service). This port number can be changed.

#:

This port is also used when SSL is enabled. To interrupt non-SSL communication from outside the network to the management server, you need to edit the `user_httpsd.conf` file.

- Execute the `services.msc` command from a command prompt to check that **Manual** or **Automatic** is set for **Startup Type** of the Application Experience service.

  If a value other than the above is set, change the setting to **Automatic** or **Manual**. If the setting is **Disabled**, the installation might fail.

  Note that, if the service does not exist, you do not need to specify this setting.

Tasks that you need to carry out before installing or upgrading Hitachi File Services Manager:

- Log on to Windows as an Administrator or a member of the Administrators group.
- Stop the services of all Hitachi Command Suite products# that are running on the computer on which you are installing Hitachi File Services Manager.

  If you install Hitachi File Services Manager without stopping the services, the services of Hitachi Command Suite Common Component and other Hitachi Command Suite products will be stopped during the installation. If the installer cannot stop the services, the installation will be canceled.

  #:

  Executing the `hcmds64srv /stop` command stops all of the Hitachi Command Suite product services, except the Hitachi Tuning Manager - Agent for SAN Switch services when Hitachi Tuning Manager - Agent for SAN Switch is installed. In this case, note that you have to stop the Hitachi Tuning Manager - Agent for SAN Switch services before stopping the Hitachi Tuning Manager services. For details on how to stop the Hitachi Tuning Manager - Agent for SAN Switch services, see the manual for Hitachi Tuning Manager - Agent for SAN Switch.
- If Hitachi NAS Manager is installed, uninstall it, and then install Hitachi File Services Manager.
- If Hitachi File Services Manager or Hitachi Command Suite products have been installed, back up their databases.
- If any Hitachi Command Suite product has been installed, make sure that `HiRDB/EmbeddedEdition _HD1` is running.

  The Hitachi Command Suite products require that this service always be running. In the Windows Services window, check the list of services to make sure that it is running. If it has stopped, start it.
- If a security monitoring program has been installed, either stop it or change its settings so that it does not hamper installation of Hitachi File Services Manager.
- If an antivirus program has been installed, stop the program, and then install Hitachi File Services Manager.

You might not be able to install Hitachi File Services Manager while an antivirus program is running. If an installation attempt fails, take action according to the message displayed in the error dialog box.

- If a process monitoring program is installed, stop it or change its settings so that the services and processes of Hitachi File Services Manager and Hitachi Command Suite Common Component are not monitored.

  If a process monitoring program starts or stops the services or processes of Hitachi File Services Manager and Hitachi Command Suite Common Component during installation of Hitachi File Services Manager, the installation might fail.

- Adjust the time on the computer on which Hitachi File Services Manager is to be installed.

  Do not adjust the time on the management server after Hitachi File Services Manager has been installed. If you change the time while Hitachi File Services Manager and Hitachi Command Suite Common Component are running, Hitachi File Services Manager might not be able to operate correctly. For details on how to adjust the time on the management server after Hitachi File Services Manager has been installed, see Adjusting the management server time on page 7-125.

- Close all windows used for operating Windows services.

- When the OS of the computer on which you will install Hitachi File Services Manager is a version of Windows that includes the Data Execution Prevention (DEP) function, if DEP is enabled, insert the installation media for Hitachi File Services Manager and disable DEP for the file `HFSMinst.exe`.

Notes on using Hitachi File Services Manager by logging in from the Device Manager GUI

When linking with Device Manager, Hitachi File Services Manager can be used by logging in from the Device Manager GUI. Required settings vary depending on the installation destination of Hitachi File Services Manager and Device Manager. Note the following when using Hitachi File Services Manager by logging in from the Device Manager GUI:

If both Hitachi File Services Manager and Device Manager are installed on the same management server:

- Start Device Manager after Hitachi File Services Manager has been installed. For details on how to start Device Manager, see the applicable Device Manager manual. If you install Hitachi File Services Manager on the management server on which Device Manager version 8.0 or later has already been installed, specify settings so that Hitachi File Services Manager connects to Device Manager to manage user accounts. For details on the procedure, see Connecting to Device Manager to manage user accounts on page 7-83.

- If Device Manager cannot be started after installation of Hitachi File Services Manager, there might be a port conflict with other products. Change the port numbers used by Device Manager, and then start Device Manager. For details on how to change the port numbers used by Device Manager, see the applicable Device Manager manual.

- For the user account used for authentication by Device Manager, set the Admin (application management) permission for Hitachi File Services Manager.
- If you uninstall Device Manager version 8.0 or later, you must also uninstall Hitachi File Services Manager.

If Hitachi File Services Manager and Device Manager are installed on separate computers:

- Specify settings so that Hitachi File Services Manager connects to Device Manager to manage user accounts. For details on the procedure, see Connecting to Device Manager to manage user accounts on page 7-83.
- For the user account used for authentication by Device Manager, set the Admin (application management) permission for Hitachi File Services Manager.

Installing and uninstalling Hitachi File Services Manager (if the management server is running in a cluster configuration)

This section describes how to install and uninstall Hitachi File Services Manager if the management server is running in a cluster configuration.

Before you install Hitachi File Services Manager on a management server in a cluster configuration, make sure that the following conditions are satisfied:

- The computer on which Hitachi File Services Manager is to be installed satisfies the requirements of the management server (Table 3-2 Requirements for a management server on page 3-5).
- Software required for cluster configurations has been installed on the computer on which Hitachi File Services Manager is to be installed (Management server cluster configuration on page 3-7).
- The same version of Hitachi File Services Manager is to be installed on the executing node and on the standby node.

Performing a new installation of Hitachi File Services Manager (if the management server is running in a cluster configuration)

This section describes how to perform a new installation of Hitachi File Services Manager on a management server in a cluster configuration.

Changing the management server to a cluster configuration

If the cluster management IP address and shared disk are not set up in Failover Cluster Management of Microsoft Failover Cluster, perform the following:

1. From the Windows **Start** menu, choose **Settings**, **Control Panel**, **Administrative Tools**, and then **Failover Cluster Management** to display Failover Cluster Management.
2. In the **Resource type** drop-down list, select **IP address**, and then register the cluster management IP address for the group.
3. In the **Resource type** drop-down list, select **Network Name**, and then register the logical host name for the group.
4. In the **Resource type** drop-down list, select **Physical Disk**, and then register the shared disk for the group.
5. In Failover Cluster Management, place the group online.

Installations in cluster environments prerequisites

Before you perform a new installation of Hitachi File Services Manager on a management server in a cluster configuration, check the following:

- For the executing and standby nodes of the management server and for the cluster management IP address, make sure that the IP address can be resolved from the host name.
- Make sure that Hitachi File Services Manager will not be accessed while you are configuring a cluster.
- Perform installation on the executing node of the management server before performing installation on the standby node.

Performing a new installation on the executing node of the management server

To perform a new installation of Hitachi File Services Manager on the executing node and configure the cluster:

1. Perform a new installation of Hitachi File Services Manager on the executing node.

   For details on how to perform a new installation of Hitachi File Services Manager, see Performing a new installation of Hitachi File Services Manager on page 7-2. When installing Hitachi File Services Manager, use the default storage locations for the databases used by Hitachi Command Suite Common Component and Hitachi File Services Manager.
2. Use a text editor to create a cluster-configuration file.

   Specify the following items in the cluster-configuration file:

   - `mode`

     Specify `online`.
   - `virtualhost`

     Specify the logical host name.
   - `onlinehost`

     Specify the host name of the executing node.
   - `standbyhost`

     Specify the host name of the standby node.

An IP address cannot be specified for `virtualhost`, `onlinehost`, or `standbyhost`.

The following shows an example of the cluster-configuration file:

```
mode = online
virtualhost = hicommand_cluster
onlinehost = hicommand_1
standbyhost = hicommand_2
```

3. Save the cluster-configuration file as `cluster.conf` in the following folder:

   Hitachi-Command-Suite-Common-Component-installation-folder`\conf\`

4. Stop the services of Tuning Manager that connects to Device Manager on the management server.

   This step is necessary if Tuning Manager and Device Manager have been installed on different computers. Stop the services on the computer on which Tuning Manager has been installed. For details on how to stop the services of Tuning Manager, see the relevant manuals for the installed version of Tuning Manager.

5. Make sure that you are ready to stop Hitachi File Services Manager and Hitachi Command Suite Common Component.

   Hitachi File Services Manager and Hitachi Command Suite Common Component automatically stop when the command in the next step is executed.

6. Execute the following command to back up the database.

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64backups /dir backup-target-folder /auto
   ```

   In *backup-target-folder*, specify the absolute path of a folder on a local disk. If you specify an existing folder, make sure that the folder is empty.

   In the path you specify, you can use alphanumeric characters, spaces, exclamation marks (`!`), hash marks (`#`), left parentheses (`(`), right parentheses (`)`), plus signs (`+`), hyphens (`-`), periods (`.`), equal signs (`=`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), carets (`^`), underscores (`_`), left curly brackets (`{`), right curly brackets (`}`), and tildes (`~`). In addition to these characters, you can use forward slashes (`/`), colons (`:`), and backslashes (`\`) as path delimiters.

   When you execute the `hcmds64backups` command, a folder named `database` will be created in the folder for storing backup files (*backup-target-folder*), and the database backup file will be stored with the name `backup.hdb`.

   If Tuning Manager and Device Manager have been installed on different computers, the services of Tuning Manager will not automatically start or stop even if the `/auto` option is specified.

7. Execute the following command to migrate the database to the shared disk:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbclustersetup /createcluster /databasepath database-re-creation-
destination-folder /exportpath data-storage-destination-folder /auto
```

Specify the command arguments based on the following rules:

- For *database-re-creation-destination-folder*, specify an absolute path that does not exceed 63 bytes. For *data-storage-destination-folder*, specify an absolute path that does not exceed 63 bytes.
- For *database-re-creation-destination-folder*, specify a location on the shared disk.
- For *data-storage-destination-folder*, specify a location on the shared disk.
- If you specify an existing folder as *data-storage-destination-folder*, make sure that the folder is empty.
- For *database-re-creation-destination-folder* and *data-storage-destination-folder*, the following characters can be used: alphanumeric characters, left parentheses (`(`), right parentheses (`)`), periods (`.`), underscores (_), and spaces. However, you cannot specify a period (`.`) at the beginning or end of the path. Also, you cannot specify a space character at the beginning or end of the path, nor can you specify consecutive space characters.
- For *database-re-creation-destination-folder* and *data-storage-destination-folder*, backslashes (`\`) can be used as path delimiters. However, the path cannot end with a backslash.

The space required for *database-re-creation-destination-folder* can be calculated as follows:

required-space = 2.1 GB + *database-capacity-for-other-Hitachi-Command-Suite-products*

If the `hcmds64dbclustersetup` command execution fails because there is not enough space for *database-re-creation-destination-folder*, increase the space for the folder, and then re-execute the command.

Do not disconnect the shared disk from the executing node until the command execution terminates normally.

If the command execution terminated abnormally and then you restart the server, the connection target of the shared disk might be changed to the standby node.

When this command is executed, the port number used by HiRDB is reset to the default (`22032`).

If Tuning Manager and Device Manager have been installed on different computers, the services of Tuning Manager will not automatically start or stop even if the `/auto` option is specified.

8. If HiRDB uses a port number other than the default (`22032`) when performing operations, change the port number to the desired value.

   For details about how to change the port number used by HiRDB, see Changing the port numbers used by Hitachi Command Suite Common Component on page 7-90.

9. If Hitachi File Services Manager and Hitachi Command Suite Common Component are running, execute the following command to stop them:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
stop
```

10. In **Control Panel**, start the **Services** administrative tool, and then open the properties dialog box of each resource listed below. In the dialog box, change the **Startup Type** setting from **Automatic** to **Manual**.
    - **HiRDB/ClusterService _HD1**
    - **HBase 64 Storage Mgmt SSO Service**
    - **HBase 64 Storage Mgmt Web SSO Service**
    - **HBase 64 Storage Mgmt Web Service**
    - **HFSM Web Service**
11. In Failover Cluster Management, add the following resources.
    - **HiRDB/ClusterService _HD1**
    - **HBase 64 Storage Mgmt SSO Service**
    - **HBase 64 Storage Mgmt Web SSO Service**
    - **HBase 64 Storage Mgmt Web Service**
    - **HFSM Web Service**

    In Failover Cluster Management, choose **New** and then **Resource**. In each dialog box, specify the settings shown in the following tables, and then click **Finish**.

Table 7-3 HiRDB/ClusterService _HD1 property settings

Tab name	Setting
General	**Startup parameters** or **Startup type**: Specify nothing. If a value is specified, delete the value.
Dependencies	Register the shared disk and client access point.
Advanced Policies	**Possible Owners**: Verify that the active and standby nodes are added.
Policies	Specify nothing.
Registry Replication	Specify nothing.

Table 7-4 HBase 64 Storage Mgmt SSO Service property settings

Tab name	Setting
General	**Startup parameters** or **Startup type**: Specify nothing. If a value is specified, delete the value.
Dependencies	Register HiRDB/ClusterService _HD1.
Advanced Policies	**Possible Owners**: Verify that the active and standby nodes are added.

Tab name	Setting
Policies	Specify nothing.
Registry Replication	Specify nothing.

Table 7-5 HBase 64 Storage Mgmt Web SSO Service property settings

Tab name	Setting
General	**Startup parameters** or **Startup type**: Specify nothing. If a value is specified, delete the value.
Dependencies	Register HBase 64 Storage Mgmt Web Service.
Advanced Policies	**Possible Owners**: Verify that the active and standby nodes are added.
Policies	Specify nothing.
Registry Replication	Specify nothing.

Table 7-6 HBase 64 Storage Mgmt Web Service property settings

Tab name	Setting
General	**Startup parameters** or **Startup type**: Specify nothing. If a value is specified, delete the value.
Dependencies	Register HBase 64 Storage Mgmt SSO Service.
Advanced Policies	**Possible Owners**: Verify that the active and standby nodes are added.
Policies	Specify nothing.
Registry Replication	Specify nothing.

Table 7-7 HFSM Web Service property settings

Tab name	Setting
General	**Startup parameters** or **Startup type**: Specify nothing. If a value is specified, delete the value.
Dependencies	Register HBase 64 Storage Mgmt Web SSO Service.
Advanced Policies	**Possible Owners**: Verify that the active and standby nodes are added.
Policies	Specify nothing.
Registry Replication	Specify nothing.

Performing a new installation on the standby node of the management server

To perform a new installation of Hitachi File Services Manager on the standby node and configure the cluster:

1. Perform a new installation of Hitachi File Services Manager on the standby node.

   For details on how to perform a new installation of Hitachi File Services Manager, see Performing a new installation of Hitachi File Services Manager on page 7-2. When installing Hitachi File Services Manager, follow the rules below:

   - Specify the same installation folder as that for the execution node.
   - Use the default storage locations for the databases used by Hitachi Command Suite Common Component and Hitachi File Services Manager.

2. Use a text editor to create a cluster-configuration file.

   Specify the following items in the cluster-configuration file:

   - `mode`

     Specify `standby`.
   - `virtualhost`

     Specify the logical host name.
   - `onlinehost`

     Specify the host name of the executing node.
   - `standbyhost`

     Specify the host name of the standby node.

   An IP address cannot be specified for `virtualhost`, `onlinehost`, or `standbyhost`.

   The following shows an example of the cluster-configuration file:

   ```
   mode = standby
   virtualhost = hicommand_cluster
   onlinehost = hicommand_1
   standbyhost = hicommand_2
   ```

3. Save the cluster-configuration file as `cluster.conf` in the following folder.

   Hitachi-Command-Suite-Common-Component-installation-folder`\conf\`

4. Stop the services of Tuning Manager that connects to Device Manager on the management server.

   This step is necessary if Tuning Manager and Device Manager have been installed on different computers. Stop the services on the computer on which Tuning Manager has been installed. For details on how to stop the services of Tuning Manager, see the relevant manuals for the installed version of Tuning Manager.

5. Make sure that you are ready to stop Hitachi File Services Manager and Hitachi Command Suite Common Component.

Hitachi File Services Manager and Hitachi Command Suite Common Component automatically stop when the command in the next step is executed.

6. Execute the following command to specify that the database on the shared disk be used:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbclustersetup /createcluster /databasepath database-re-creation-
destination-folder /exportpath data-storage-destination-folder /auto
```

Specify the command arguments based on the following rules:

- For *database-re-creation-destination-folder*, specify the same folder as the executing node.
- For *data-storage-destination-folder,* specify an absolute path that does not exceed 63 bytes.
- For *data-storage-destination-folder*, specify a location on the local disk.
- If you specify an existing folder as *data-storage-destination-folder*, make sure that the folder is empty.
- For *data-storage-destination-folder*, the following characters can be used: alphanumeric characters, left parentheses (`(`), right parentheses (`)`), periods (`.`), underscores (`_`), and spaces. However, you cannot specify a period (`.`) at the beginning or end of the path. Also, you cannot specify a space character at the beginning or end of the path, nor can you specify consecutive space characters.
- For *data-storage-destination-folder*, backslashes (`\`) can be used as path delimiters. However, the path cannot end with a backslash.

Do not disconnect the shared disk from the executing node until the `hcmds64dbclustersetup` command execution terminates normally.

If the command execution terminated abnormally, do not restart the server.

When this command is executed, the port number used by HiRDB is reset to the default (`22032`).

If Tuning Manager and Device Manager have been installed on different computers, the services of Tuning Manager will not automatically start or stop even if the `/auto` option is specified.

7. If HiRDB uses a port number other than the default (`22032`) when performing operations, change the port number to the desired value.

For details about how to change the port number used by HiRDB, see Changing the port numbers used by Hitachi Command Suite Common Component on page 7-90.

8. If Hitachi File Services Manager and Hitachi Command Suite Common Component are running, execute the following command to stop them:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
stop
```

9. In **Control Panel**, start the **Services** administrative tool, and then open the properties dialog box of each resource listed below. In the dialog box, change the **Startup Type** setting from **Automatic** to **Manual**.
    - **HiRDB/ClusterService _HD1**
    - **HBase 64 Storage Mgmt SSO Service**
    - **HBase 64 Storage Mgmt Web SSO Service**
    - **HBase 64 Storage Mgmt Web Service**
    - **HFSM Web Service**
10. In Failover Cluster Management, place the group online.

Performing an upgrade or overwrite installation of Hitachi File Services Manager (if the management server is running in a cluster configuration)

This section describes how to perform an upgrade or overwrite installation of Hitachi File Services Manager if the management server is running in a cluster configuration.

Perform installation on the executing node of the management server before performing installation on the standby node.

Upgrade or overwrite installation on the executing node of the management server

To perform an upgrade or overwrite installation of Hitachi File Services Manager on the executing node and set up Hitachi File Services Manager for a cluster system:

1. From the Windows **Start** menu, choose **Settings**, **Control Panel**, **Administrative Tools**, and then **Failover Cluster Management** to display Failover Cluster Management.
2. To perform an upgrade or overwrite installation from v6.1.2 or earlier, take the following resources offline in Failover Cluster Management:
    - **HBase Storage Mgmt Common Service**
    - **HBase Storage Mgmt Web Service**

    To perform an upgrade or overwrite installation from v6.2.0 or later, take the following resources offline in Failover Cluster Management:
    - **HBase 64 Storage Mgmt SSO Service**
    - **HBase 64 Storage Mgmt Web SSO Service**
    - **HBase 64 Storage Mgmt Web Service**
    - **HFSM Web Service**
3. Stop Hitachi File Services Manager and Hitachi Command Suite Common Component.

    For details about how to stop the services, see the manual corresponding to the version of Hitachi File Services Manager you are using.

4. To perform an upgrade or overwrite installation from v6.1.2 or earlier, take the following resources offline in Failover Cluster Management:
   - **HiRDB/ClusterService _HD0**

   To perform an upgrade or overwrite installation from v6.2.0 or later, take the following resources offline in Failover Cluster Management:
   - **HiRDB/ClusterService _HD1**
5. In Failover Cluster Management, delete the following service offline. (This step is necessary only when you are performing an upgrade installation from v6.1.2 or earlier.)
   - **HBase Storage Mgmt Common Service**
   - **HBase Storage Mgmt Web Service**
   - **HiRDB/ClusterService _HD0**
6. Prevent the resources from restarting. In Failover Cluster Management, open the properties dialog box of each resource listed below. In the dialog box, choose the **Policies** tab, select **If resource fails, do not restart**, and then click the **OK** button. (This step is necessary only when you are performing an upgrade or overwrite installation from v6.2.0 or later.)
   - **HBase 64 Storage Mgmt Web Service**
   - **HiRDB/ClusterService _HD1**
   - **HFSM Web Service**
7. Start HiRDB.

   For details about how to start HiRDB, see the manual corresponding to the version of Hitachi File Services Manager you are using.
8. Back up the database.

   For details about how to back up the database, see the manual corresponding to the version of Hitachi File Services Manager you are using.
9. Upgrading from v6.1.2 or earlier, copy the cluster configuration file (`cluster.conf`) to a folder other than the installation folder.

   This operation is necessary if Hitachi File Services Manager v6.1.2 or earlier was installed in the default installation folder (`C:\Program Files(x86)\HiCommand`).

   The cluster configuration file is located in the following folder:
   Hitachi-Command-Suite-Common-Component-installation-folder`\conf`
10. On the executing node, perform an upgrade or overwrite installation of Hitachi File Services Manager.

    For details about the procedure, see Performing an upgrade or overwrite installation of Hitachi File Services Manager on page 7-7.
11. Upgrading from v6.1.2 or earlier, move or copy the cluster configuration file.

    This operation is necessary if Hitachi File Services Manager v6.1.2 or earlier was installed in the default installation folder (`C:\Program Files(x86)\HiCommand`).

Move or copy the cluster configuration file (`cluster.conf`) that you saved in advance to the following folder:

Hitachi-Command-Suite-Common-Component-installation-folder`\Base64\conf`

12. Transfer the database to the shared disk. (This step is necessary only when you are performing an upgrade installation from v6.1.2 or earlier.)

    For details about how to transfer the database to the shared disk, see steps 7 and 8 in Performing a new installation on the executing node of the management server on page 7-17.

Caution: Upgrading from v6.1.2 or earlier, specify the different folder as a database-re-creation-destination-folder from that of before upgrade.

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

    For details about how to stop the services, see step 9 in Performing a new installation on the executing node of the management server on page 7-17

14. In **Control Panel**, start the **Services** administrative tool, and then open the properties dialog box of each resource listed below. In the dialog box, change the **Startup Type** setting from **Automatic** to **Manual**.

    - **HBase 64 Storage Mgmt SSO Service**
    - **HBase 64 Storage Mgmt Web SSO Service**
    - **HBase 64 Storage Mgmt Web Service**
    - **HFSM Web Service**

15. In Failover Cluster Management, add the resources. (This step is necessary only when you are performing an upgrade installation from v6.1.2 or earlier.)

    For details, see steps 11 in Performing a new installation on the executing node of the management server on page 7-17.

16. In Failover Cluster Management, switch the group in which Hitachi File Services Manager resources are registered to the standby node.

    To switch to the standby node, right-click the group in which the resources used by Hitachi File Services Manager are registered, and then select **Move Group**.

Upgrade or overwrite installation on the standby node of the management server

To perform an upgrade or overwrite installation of Hitachi File Services Manager on the standby node and set up Hitachi File Services Manager for a cluster system:

1. Stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

   For details about how to stop the services, see the manual corresponding to the version of Hitachi File Services Manager you are using.

2. Upgrading from v6.1.2 or earlier, copy the cluster configuration file (`cluster.conf`) to a folder other than the installation folder.

   This operation is necessary if Hitachi File Services Manager v6.1.2 or earlier was installed in the default installation folder (`C:\Program Files(x86)\HiCommand`).

   The cluster configuration file is located in the following folder:

   Hitachi-Command-Suite-Common-Component-installation-folder`\conf`

3. On the standby node, perform an upgrade or overwrite installation of Hitachi File Services Manager.

   For details about the procedure, see Performing an upgrade or overwrite installation of Hitachi File Services Manager on page 7-7.

4. Upgrading from v6.1.2 or earlier, move or copy the cluster configuration file.

   This operation is necessary if Hitachi File Services Manager v6.1.2 or earlier was installed in the default installation folder (`C:\Program Files(x86)\HiCommand`).

   Move or copy the cluster configuration file (`cluster.conf`) that you saved in advance to the following folder:

   Hitachi-Command-Suite-Common-Component-installation-folder `\Base64\conf`

5. Transfer the database to the shared disk. (This step is necessary only when you are performing an upgrade installation from v6.1.2 or earlier.)

   For details about how to transfer the database to the shared disk, see steps 6 and 7 in Performing a new installation on the standby node of the management server on page 7-22.

6. Execute the following command to stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
   stop
   ```

7. In **Control Panel**, start the **Services** administrative tool, and then open the properties dialog box of each resource listed below. In the dialog box, change the **Startup Type** setting from **Automatic** to **Manual**. (This step is necessary only when you are performing an upgrade installation from v6.1.2 or earlier.)

   - **HiRDB/ClusterService _HD1**
   - **HBase 64 Storage Mgmt SSO Service**
   - **HBase 64 Storage Mgmt Web SSO Service**
   - **HBase 64 Storage Mgmt Web Service**
   - **HFSM Web Service**

8. In Failover Cluster Management, switch the group in which Hitachi File Services Manager resources are registered to the executing node.

   To switch to the executing node, right-click the group in which the resources used by Hitachi File Services Manager are registered, and then select **Move Group**.

9. In Failover Cluster Management, right-click the following resource name and select **Properties**.
   - **HBase 64 Storage Mgmt Web Service**
   - **HiRDB/ClusterService _HD1**
   - **HFSM Web Service**
10. On the **Policies** tab, select the following items:
   - **If resource fails, attempt restart on current node**.
   - **If restart is unsuccessful, failover all resources in this Role** (or **If restart is unsuccessful, failover all resources in this service or application**).
11. In Failover Cluster Management, place online the group in which the resources for Hitachi File Services Manager have been registered.

Performing a new installation, upgrade installation, or overwrite installation of Hitachi File Services Manager (when Hitachi Command Suite products are running in a cluster configuration)

This section describes how to install Hitachi File Services Manager when Hitachi Command Suite products are running in the cluster configuration.

Note that, if a Hitachi Command Suite product of a version from 8.1.2 to 8.5.1 is installed in an environment where Hitachi File Services Manager is running in a cluster configuration, the Hitachi File Services Manager settings that were set in Microsoft Failover Cluster will be lost. (For details about these settings, see Table 7-7 HFSM Web Service property settings on page 7-21.) In this case, specify the settings shown in Table 7-7 HFSM Web Service property settings on page 7-21 again.

1. In a browser, enter the cluster management IP address and bring the shared disk online.
2. Use Failover Cluster Management to take offline the services and resources of all Hitachi Command Suite products other than HiRDB/ClusterService _HD1 and HiRDB/ClusterService _HD0, which will be taken offline in step 5.

   If you are performing an upgrade installation or overwrite installation of Hitachi File Services Manager, take the services and resources of Hitachi File Services Manager offline as well.
3. In Failover Cluster Management, open the properties dialog box for each of the services and resources of the Hitachi Command Suite products. Then, select **Policies**, **If resource fails, do not restart**, and then click the **OK** button.

   If you are performing an upgrade installation or overwrite installation of Hitachi File Services Manager, configure the same settings for each of the services and resources of Hitachi File Services Manager as well.
4. Stop Hitachi File Services Manager and Hitachi Command Suite Common Component on the active node.

For details about how to stop the services, see the manual corresponding to the version of Hitachi File Services Manager you are using.

5. Use Failover Cluster Management to take the following resources offline:
   - **HiRDB/ClusterService _HD1**
   - **HiRDB/ClusterService _HD0** (only when you are performing an upgrade installation from v6.1.2 or earlier.)
6. In Failover Cluster Management, delete the resources that are not being used by another application. (This step is necessary only when you are performing an upgrade installation from v6.1.2 or earlier.)
   - **HBase Storage Mgmt Common Service**
   - **HBase Storage Mgmt Web Service**
   - **HiRDB/ClusterService _HD0**
7. Start HiRDB, and back up the database on the active node.

   For details about how to start HiRDB and back up the database, see the manual corresponding to the version of Hitachi File Services Manager you are using.
8. Confirm that the active node can access the shared disk, and then install Hitachi File Services Manager on the active node.

   If you are performing a new installation, see Performing a new installation of Hitachi File Services Manager (if the management server is running in a cluster configuration) on page 7-16. Note that, in this case, you must specify a directory on the shared disk as the location to store the database. If you are performing an overwrite or upgrade installation, see Performing an upgrade or overwrite installation of Hitachi File Services Manager (if the management server is running in a cluster configuration) on page 7-24.
9. Stop the services of Hitachi Command Suite products and of Hitachi File Services Manager on the active node.

   For details on how to stop services, see the manual for each product.
10. In **Control Panel**, start the **Services** administrative tool, and then open the properties dialog box of each resource listed below. In the dialog box, change the **Startup Type** setting from **Automatic** to **Manual**.
    - **HBase 64 Storage Mgmt Common Service**
    - **HBase 64 Storage Mgmt SSO Service**
    - **HBase 64 Storage Mgmt Web Service**
    - **HBase 64 Storage Mgmt Web SSO Service**
    - **HFSM Web Service**
    - The services of currently used Hitachi Command Suite products#

      #: For details, see the documentation for Hitachi Command Suite products you are using.
11. In Failover Cluster Management, right-click each of the services of Hitachi Command Suite products and of Hitachi File Services Manager, and then change the node to the standby node.

12. Stop the services of Hitachi Command Suite products and of Hitachi File Services Manager on the standby node.

    For details on how to stop services, see the manual for each product.

13. Confirm that the standby node can access the shared disk, and then install Hitachi File Services Manager on the standby node.

    If you are performing a new installation, see Performing a new installation of Hitachi File Services Manager (if the management server is running in a cluster configuration) on page 7-16. Note that, in this case, you must specify the same directory on the shared disk that you specified in step 8. If you are performing an overwrite or upgrade installation, see Performing an upgrade or overwrite installation of Hitachi File Services Manager (if the management server is running in a cluster configuration) on page 7-24.

14. Stop the services of Hitachi Command Suite products and of Hitachi File Services Manager on the standby node.

    For details on how to stop services, see the manual for each product.

15. In **Control Panel**, start the **Services** administrative tool, and then open the properties dialog box of each resource listed below. In the dialog box, change the **Startup Type** setting from **Automatic** to **Manual**.

    - **HBase 64 Storage Mgmt Common Service**
    - **HBase 64 Storage Mgmt SSO Service**
    - **HBase 64 Storage Mgmt Web Service**
    - **HBase 64 Storage Mgmt Web SSO Service**
    - **HFSM Web Service**
    - The services of currently used Hitachi Command Suite products#

      #: For details, see the documentation for Hitachi Command Suite products you are using.

16. Add the HFSM Web Service as a resource of Failover Cluster Management, and then specify the settings shown in Table 7-7 HFSM Web Service property settings on page 7-21. (Note: Perform this step only if you are performing a new installation or an upgrade from version 6.1.2 or earlier.)

17. Right-click each of the resources for which the services of Hitachi Command Suite products and of Hitachi File Services Manager were added. Then, select **Properties**.

18. On the **Policies** tab, select the following items:

    - **If resource fails, attempt restart on current node**.
    - **If restart is unsuccessful, failover all resources in this Role** (or **If restart is unsuccessful, failover all resources in this service or application**).

19. If necessary, move the resources to the node that will be used.

20. In Failover Cluster Management, put the following resources online: resources for which the services of Hitachi Command Suite products and of Hitachi File Services Manager were added.

Uninstalling Hitachi File Services Manager (if the management server is running in a cluster configuration)

This section describes how to uninstall Hitachi File Services Manager if the management server is running in a cluster configuration. Perform the following operations on both the executing and standby nodes.

If the resource is not online on the executing node, place it online, and then perform uninstallation.

To uninstall Hitachi File Services Manager if the management server is running in a cluster configuration:

1. From the Windows **Start** menu, choose **Settings**, **Control Panel**, **Administrative Tools**, and then **Failover Cluster Management** to display Failover Cluster Management.
2. In Failover Cluster Management, switch the group in which the resources for Hitachi File Services Manager have been registered to the executing node.

   To switch to the executing node, right-click the group in which the resources used by Hitachi File Services Manager are registered, and then select **Move Group**.
3. In Failover Cluster Management, place the following resources offline.
   - **HBase 64 Storage Mgmt SSO Service**
   - **HBase 64 Storage Mgmt Web SSO Service**
   - **HBase 64 Storage Mgmt Web Service**
   - **HFSM Web Service**
4. On the executing node, execute the following command to stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
   stop
   ```
5. In Failover Cluster Management, place **HiRDB/ClusterService _HD1** offline.
6. From among the following resources, delete the resources that are not being used by another application:
   - **HiRDB/ClusterService _HD1**
   - **HBase 64 Storage Mgmt SSO Service**
   - **HBase 64 Storage Mgmt Web SSO Service**
   - **HBase 64 Storage Mgmt Web Service**
   - **HFSM Web Service**
7. In Failover Cluster Management, perform the following operation on the resources that you did not delete in step 6.

   Open the properties dialog box of each resource. In the dialog box, choose the **Policies** tab, select **If resource fails, do not restart**, and then click the **OK** button.

8. On the executing node, uninstall Hitachi File Services Manager.

   For details on how to uninstall Hitachi File Services Manager, see Uninstalling Hitachi File Services Manager on page 7-10.

9. In Failover Cluster Management, switch the group in which the resources for Hitachi File Services Manager have been registered to the standby node.

   To switch to the standby node, right-click the group in which the resources used by Hitachi File Services Manager are registered, and then select **Move Group**.

10. On the standby node, execute the following command to stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
stop
```

11. On the standby node, uninstall Hitachi File Services Manager.

    For details on how to uninstall Hitachi File Services Manager, see Uninstalling Hitachi File Services Manager on page 7-10.

12. From among the following resources, place offline and then delete the resources that are not being used by another application.

    - Shared disk
    - Logical IP address of the cluster

13. If the group in which Hitachi File Services Manager resources have been registered is no longer necessary, delete it.
14. In Failover Cluster Management, right-click the resources that were set to **If resource fails, do not restart** in step 7, and select **Properties**.
15. On the **Policies** tab, select the following items:

    - **If resource fails, attempt restart on current node**.
    - **If restart is unsuccessful, failover all resources in this Role** (or **If restart is unsuccessful, failover all resources in this service or application**).

16. In Failover Cluster Management, place online the resource that was in step 15.

Starting and stopping Hitachi File Services Manager

The system administrator can start or stop Hitachi File Services Manager by starting or stopping Hitachi Command Suite Common Component.

The following sections describe how to start and stop Hitachi File Services Manager, and how to check whether Hitachi File Services Manager is running.

List of resident processes

The following table lists the resident processes of Hitachi File Services Manager and Hitachi Command Suite Common Component.

Table 7-8 Resident processes of Hitachi File Services Manager and Hitachi Command Suite Common Component

Process	Description
hcmdssvctl.exe	Process of the Hitachi Command Suite servlet service
cjstartsv.exe	Process of the Hitachi File Services Manager J2EE service
hntr2mon.exe#1	Process for collecting Hitachi Command Suite common trace information
hntr2srv.exe#1	Process of the Hitachi Command Suite common trace service
httpsd.exe rotatelogs.exe	Process of the Hitachi Command Suite common Web service This process might be started redundantly.
pdservice.exe#2	Process of the HiRDB process server control

#1:

If a 64-bit OS is configured in the management server, 32-bit and 64-bit processes are resident.

#2:

This process must always be running. Do not stop it manually or register it as a cluster resource.

Starting Hitachi File Services Manager

You can use either of the following methods to start Hitachi File Services Manager:

- Using the Windows menu
- Using a command

The following explains how to start Hitachi File Services Manager. If the HDI system is being operated and managed by logging in from the Device Manager GUI, you must start Device Manager and Hitachi Command Suite Common Component. For details on how to start these programs, see the Device Manager documentation.

Tip: From version 05-70 onward, if you start Hitachi Command Suite Common Component, services of Hitachi Command Suite products such as Device Manager are also started at the same time.

Using the Windows menu

To use the Windows menu to start Hitachi File Services Manager:

1. Log on to Windows as an Administrator or a member of the Administrators group.
2. Start Hitachi File Services Manager by using either of the following methods:

- Choose **Start**, **Programs**, **Hitachi Command Suite**, **File Services Manager**, and then **Start - HFSM**.
- Select **Start - HFSM** from the application list in the Start screen.

The progress of the processing is displayed in a command prompt window.

3. When the processing is complete, press any key to close the command prompt window.

Using a command

To use a command to start Hitachi File Services Manager:

1. Execute the following command to start Hitachi File Services Manager:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
start
```

Stopping Hitachi File Services Manager

You can use either of the following methods to stop Hitachi File Services Manager:

- Using the Windows menu
- Using a command

The following explains how to stop Hitachi File Services Manager. If the HDI system is being operated and managed by logging in from the Device Manager GUI, you must stop Device Manager and Hitachi Command Suite Common Component. For details on how to stop these programs, see the Device Manager documentation.

Tip: From version 05-70 onward, if you stop Hitachi Command Suite Common Component, services of Hitachi Command Suite products such as Device Manager are also stopped at the same time.

Using the Windows menu

To use the Windows menu to stop Hitachi File Services Manager:

1. Log on to Windows as an Administrator or a member of the Administrators group.
2. Stop Hitachi File Services Manager by using one of the following methods:
   - Choose **Start**, **Programs**, **Hitachi Command Suite**, **File Services Manager**, and then **Stop - HFSM**.
   - Select **Stop - HFSM** from the application list in the Start screen.

   The progress of the processing is displayed in a command prompt window.
3. When the processing is complete, press any key to close the command prompt window.

Using a command

To use a command to stop Hitachi File Services Manager:

1. Execute the following command to stop Hitachi File Services Manager:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
stop
```

Checking whether Hitachi File Services Manager is running

You can use either of the following methods to whether Hitachi File Services Manager is running:

- Using the Windows menu
- Using a command

The following explains how to check whether Hitachi File Services Manager is running. If the HDI system is being operated and managed by logging in from the Device Manager GUI, you must check the operating status of Device Manager and Hitachi Command Suite Common Component. For details on how to check these programs, see the Device Manager documentation.

Using the Windows menu

To use the Windows menu to check whether Hitachi File Services Manager is running:

1. Log on to Windows as an Administrator or a member of the Administrators group.
2. Check whether Hitachi File Services Manager is running by using one of the following methods:
   - Choose **Start**, **Programs**, **Hitachi Command Suite**, **File Services Manager**, and then **Status - HFSM**.
   - Select **Status - HFSM** from the application list in the Start screen.

   Messages indicating whether Hitachi File Services Manager is running are displayed in a command prompt window. If Hitachi File Services Manager and Hitachi Command Suite Common Component are running normally, the following messages are displayed:

```
KAPM06440-I The HiRDB service has already started.
KAPM05007-I Already started service. service-name=HBase 64 Storage Mgmt
Web Service
KAPM05007-I Already started service. service-name=HBase 64 Storage Mgmt
Web SSO Service
KAPM05007-I Already started service. service-name=HBase 64 Storage Mgmt
SSO Service
KAPM05007-I Already started service. service-name=HFSM Web Service
```

3. After confirming that Hitachi File Services Manager is running, press any key to close the command prompt window.

Using a command

To use a command to check whether Hitachi File Services Manager is running:

1. Execute the following command to check whether Hitachi File Services Manager is running:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
status
```

If Hitachi File Services Manager and Hitachi Command Suite Common Component have started normally, the following messages are displayed:

```
KAPM06440-I The HiRDB service has already started.
KAPM05007-I Already started service. service-name=HBase 64 Storage Mgmt
Web Service
KAPM05007-I Already started service. service-name=HBase 64 Storage Mgmt
Web SSO Service
KAPM05007-I Already started service. service-name=HBase 64 Storage Mgmt
SSO Service
KAPM05007-I Already started service. service-name=HFSM Web Service
```

Managing the system administrator account

The system administrator can manage the system administrator account by editing the configuration files. In addition, if Hitachi File Services Manager is used by logging in from the Device Manager GUI, the server that manages Hitachi File Services Manager user accounts can be changed if necessary.

If the management server is being used in a cluster configuration, the settings must be same on both the executing node and standby node.

Before authenticating the system administrator account by using an external authentication server

Hitachi File Services Manager can authenticate users by linking to an external authentication server. If you register the user IDs that are registered on the external authentication server into Hitachi File Services Manager, you can use those user IDs to log in to Hitachi File Services Manager. This saves you from having to managing login passwords and controlling accounts in Hitachi File Services Manager.

In addition, if you use both an external authentication server and an external authorization server, you can control users' access permissions for Hitachi File Services Manager by using the external authorization server. When an external authorization server is also linked to, you do not need to manage accounts and set permissions for individual users in Hitachi File Services Manager because Hitachi File Services Manager manage users by using the *authorization groups* external authorization server.

Requirements for an external authentication server and an external authorization server depend on whether only an external authentication server is linked to or an external authorization server is also linked to. Environment settings for the LDAP server on page 3-17, Environment

settings for the KDC server on page 3-28 and Environment settings for the RADIUS server on page 3-29 describe requirements for each case.

Notes:

If command line control characters are included in the arguments of commands that will be executed when specifying the settings to link to an external authentication server, escape the characters correctly according to the specifications of the command line.

Also, you need to pay attention to backslashes (\) included in the arguments because they are treated specially in the command line.

If the following characters are included in an argument, enclose the argument in double quotation marks (") or use a caret (^) to escape each character:

Spaces `& | ^ < > ( )`

A backslash might be treated as an escape character depending on the character that follows it. Therefore, if a backslash and any of the above characters are included in an argument, use a caret to escape each character rather than enclose the argument in double quotation marks.

Also, if there is a backslash at the end of an argument, escape it by using another backslash.

For example, if a shared secret to be registered by the `hcmds64radiussecret` command is `secret01\`, escape it as follows:

```
hcmds64radiussecret /set secret01\\ /name ServerName
```

Setting the security related to the system administrator account

You can set conditions for the minimum number and combination of characters that must be specified for the passwords of system administrator accounts. Setting conditions can help reduce the risk of third parties being able to guess the system administrator passwords.

Also, you can specify the settings so that accounts are automatically locked when a set number of login attempts fail. Automatically locking an account when multiple login attempts fail can help reduce the risk of the GUI being accessed inappropriately.

Notes:

Automatic account locking and the password complexity checking are functions of Hitachi Command Suite Common Component. These functions are not supported by Hitachi File Services Manager or HiCommand products whose versions are 5.0 or earlier. For this reason, the following problems might occur when operations are performed with products of earlier versions:

- A user cannot log in even if the correct user ID and password are specified.

  The user account might be locked. Take appropriate action, such as unlocking the relevant account or registering a new user account.
- A password cannot be changed, or a user account cannot be added.

The specified password might not follow the password entry rules. Specify an appropriate password as indicated in the output message.

You can use either of the following methods to set the password conditions or to specify the settings related to automatic account locking:

- Specifying the settings in the `security.conf` file
- Specifying the settings in the GUI

This section describes how to use the `security.conf` file to set the password conditions and to specify the settings related to account locking.

Setting the password conditions

Specify the password conditions in the `security.conf` file. The `security.conf` file is stored in the following folder on the management server:

Hitachi-Command-Suite-Common-Component-installation-folder\conf\sec\

Soon after the setting value in the `security.conf` file is changed, the new value becomes valid.

The specified password conditions are applied when you add an account for a system administrator, or change the password for a system administrator. These password conditions are not applied to the passwords for existing accounts, so system administrators can log in to the GUI if their existing passwords do not satisfy the password conditions.

The following table lists the password conditions specified in the `security.conf` file.

Table 7-9 Password conditions specified in the security.conf file

Item	Description
`password.min.length`	Specifies the minimum number of characters for a password. Specify a value from 1 to 256. The default value is `4`.
`password.min.uppercase`	Specifies the minimum number of uppercase characters that must be included in a password. Specify a value from 0 to 256. If 0 is specified, uppercase characters do not have to be specified. The default value is `0`.
`password.min.lowercase`	Specifies the minimum number of lowercase characters that must be included in a password. Specify a value from 0 to 256. If 0 is specified, lowercase characters do not have to be specified. The default value is `0`.
`password.min.numeric`	Specifies the minimum number of numbers that must be included in a password. Specify a value from 0 to 256. If 0 is specified, numbers do not have to be specified.

Item	Description
	The default value is `0`.
`password.min.symbol`	Specifies the minimum number of symbols that must be included in a password. Specify a value from 0 to 256. If 0 is specified, symbols do not have to be specified. The default value is `0`.

`password.check.userID`	Specifies whether the user ID can be used as the password.
	`true`
	Specify this to prevent users from setting passwords that are the same as their user IDs.
	`false`
	Specify this to allow users to set passwords that are the same as their user IDs.
	The default value is `false`.

The following shows an example of the coding in the `security.conf` file:

```
# This is the minimum length of the password
# (minimum: 1 -256characters)
password.min.length=4

# This is the minimum number of uppercase characters included in the password
# (minimum: 0-256 characters, character type: A-Z)
password.min.uppercase=0

# This is the minimum number of lowercase characters included in the password
# (minimum: 0-256 characters, character type: a-z)
password.min.lowercase=0

# This is the minimum number of numeric characters included in the password
# (minimum: 0-256 characters, character type: 0-9)
password.min.numeric=0

# This is the minimum number of symbolic characters included in the password
# (minimum: 0-256 characters, character type: ! # $ % & ' ( ) * + - . = @ \ ^
_ |)
password.min.symbol=0

# This specifies whether the user ID can be used for the password.
# (true = cannot use the user ID, false = can use the user ID)
password.check.userID=false
```

Specifying the settings related to automatic account locking

The settings related to automatic account locking are specified in the `security.conf` file. The `security.conf` file is stored in the following folder on the management server:

Hitachi-Command-Suite-Common-Component-installation-folder\conf\sec\

Soon after the setting value in the `security.conf` file is changed, the new value becomes valid.

Notes:

- The set maximum number of login failures is applied at login authentication.

  For example, if you change the setting for the number of login failures from 5 to 2, an account will not be locked even if three login attempts in succession have already failed. The next (fourth) time the password is specified correctly, login is permitted. If login fails, the account is locked.
- If the account of a system administrator is automatically locked while that administrator is logged in, the logged-in system administrator can continue operations until logging out.

The following table lists the setting related to automatic account locking specified in the `security.conf` file.

Table 7-10 Setting related to automatic account locking specified in the security.conf file

Item	Description
`account.lock.num`	Specifies the number of login failures allowed before a user account is automatically locked. Specify a value from 0 to 10. If 0 is specified, user accounts will not be locked because of login failures. The default value is `0`.

The following shows an example of the coding in the `security.conf` file:

```
...
# This is the minimum number of login failures before an account is locked
# (minimum: 0-10 times)
account.lock.num=0
...
```

Specifying the settings related to locking the system account

The system administrator can edit the `user.conf` file in order to lock the `System` account. During the initial installation, there is no automatic and manual lock mechanism for the `System` account.

To change the settings related to locking the `System` account:

1. Edit the `user.conf` file to change the settings related to locking the `System` account.

   The `user.conf` file is located in the folder below. If this file does not exist, create it.

   Hitachi-Command-Suite-Common-Component-installation-folder\conf\
2. Stop and then restart Hitachi File Services Manager and Hitachi Command Suite Common Component.

   For details on how to do this, see Starting and stopping Hitachi File Services Manager on page 7-32.

The following table lists the setting related to locking the System account in the user.conf file:

Table 7-11 Property in the user.conf file (Settings made in the user.conf file to lock the System account)

Property	Description
account.lock.system	Specifies whether to lock the System account. true Specify this option if you want to lock the System account. If this is specified, the System account can be manually locked. false Specify this option if you do not want to lock the System account. If this is specified, the System account cannot be locked. The default value is false. If you specify a character string other than the above, the value will default to false.

The following shows an example of the coding in the user.conf file:

```
...
account.lock.system=true
...
```

Note:

If true is set in the user.conf file, the automatic and manual lock mechanism for the System account will be enabled for all installed Hitachi Command Suite products whose version is 6.1 or later. If you cannot use the System account to log in to Hitachi Storage Command Suite products version 6.0 or earlier, it is likely that the account is locked. If this is case, unlock the account from the Users subwindow.

Unlocking a system administrator account

A system administrator who has the Admin (user management) permission can unlock a system administrator account from the Users subwindow. The system administrator can also use commands to unlock an account.

To unlock a system administrator account by using commands:

1. Execute a command as follows to make sure that the Hitachi Command Suite Common Component service is running.

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
   status
   ```

2. Execute a command as follows to unlock the account.

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64unlockaccount /user user-ID-of-user-to-be-unlocked /pass password-
of-user-to-be-unlocked
```

Performing an external authentication by using an LDAP server

To authenticate the system administrator account by using an LDAP server, specify the following settings in Hitachi File Services Manager.

1. Check the data structure of the LDAP server to determine the method for linking with Hitachi File Services Manager and for authentication.
2. In the `exauth.properties` file on the management server, specify necessary information.

   Necessary settings depend on whether only an external authentication server is linked to or an external authorization server is also linked to.

   You can use either of the following methods to define the LDAP server:

   - In the `exauth.properties` file, directly specify information about the LDAP server to connect to.

     Specify information such as IP address and port number in the `exauth.properties` file for each LDAP server.
   - Use the DNS server to look up the LDAP server to connect to.

     Before using this method, you need to set up the DNS server environment on the OS of the LDAP server. In addition, you need to register the host name, port number, and domain name of the LDAP server in the SRV records of the DNS server.

   Important:

   - To use StartTLS for communication between the management server and the LDAP server, you need to directly specify information about the LDAP server to connect to in the `exauth.properties` file.
   - If you use the DNS server to look up the LDAP server to connect to, it might take longer for users to log in.
3. In the following cases, on the management server, register a user account used to search for user information on the LDAP server.

   - When the data structure is the hierarchical structure model
   - When the data structure is the flat model and an external authorization server is also linked to#

   #:

   When registering an authorization group in Hitachi File Services Manager by using the GUI (for details on the procedure, see step 5), if you want to check whether the distinguished name of the authorization group is registered on the external authorization server by using a user ID such as the `System` account registered in Hitachi File Services Manager, you need to register a user account used to search for LDAP user information on the management server.

4. On the LDAP server, register the accounts of users who will use Hitachi File Services Manager.

   User IDs and passwords must consist of characters that can be used in Hitachi File Services Manager. Specify 1 to 256 bytes of the following characters:

   `0` to `9` `A` to `Z` `a` to `z` `!` `#` `$` `%` `&` `'` `(` `)` `*` `+` `-` `.` `=` `@` `\` `^` `_` `|`

   In Hitachi File Services Manager, user IDs are not case-sensitive. The combination of character types for passwords must follow the settings in the external authentication server.

5. Register accounts and set permissions by using the GUI.

   When linking with only an external authentication server:

   - Register users.
   - Change the user authentication method.

     This operation is required if you want to change the authentication method for existing users.
   - Register users into user groups.
   - Configure both user management and the operation permissions for Hitachi File Services Manager.

   When also linking with an external authorization server:

   - Register authorization groups.
   - Configure both user management and the operation permissions for Hitachi File Services Manager.

   Reference note:

   Users who belong to nested groups of a registered authorization group can now also use Hitachi File Services Manager via the roles (permissions) set for the authorization group.

6. Use the `hcmds64checkauth` command to make sure that the external authentication server and the external authorization server can be properly connected to.

The following sections describe operations you need to perform on the management server.

Data structure model and authentication method for LDAP authentication

The LDAP server has the following two data structure models.

- Hierarchical structure model
- Flat model

You must first determine which data structure model is being used, because the information you need to set in the `exauth.properties` file and the operations you need to perform on the management server depend on the data structure.

In addition, check BaseDN, which is the entry that will be the start point for searching for LDAP user information during authentication. BaseDN must be

specified in the `exauth.properties` file. Only the user entries that are in the hierarchy below BaseDN can be authenticated. Make sure that all users you want to authenticate for Hitachi File Services Manager are in this hierarchy.

Hierarchical structure model

A data structure in which the hierarchies below BaseDN branch off and in which user entries are registered in another hierarchy. If the hierarchical structure model is used, the entries in the hierarchy below BaseDN are searched for an entry that has the same login ID and user attribute value.

The following figure shows an example of the hierarchical structure model. The user entries enclosed by the dotted line can be authenticated. In this example, BaseDN is `cn=group,dc=example,dc=com`, because the target user entries extend across two departments (`cn=sales` and `cn=development`).

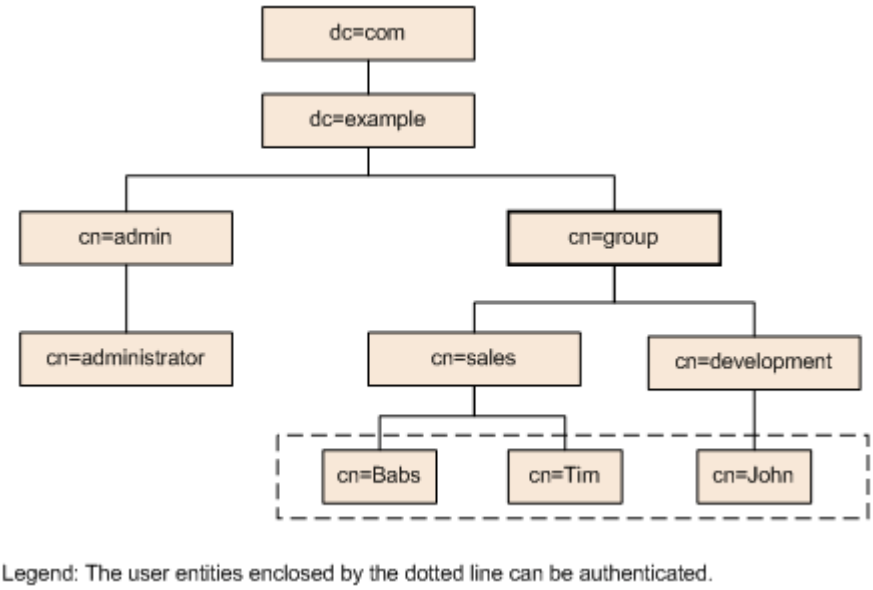


Figure 7-7 Example of the hierarchical structure model

Flat model

A data structure in which there are no branches in the hierarchy below BaseDN and in which user entries are registered in the hierarchy located just below BaseDN. If the flat model is used, the entries in the hierarchy below BaseDN are searched for an entry that has the DN that consists of a combination of the login ID and BaseDN. If such a value is found, the user is authenticated.

The following figure shows an example of the flat model. The user entities enclosed by the dotted line can be authenticated. In this example, BaseDN is `ou=people,dc=example,dc=com`, because all of the user entries are located just below `ou=people`.

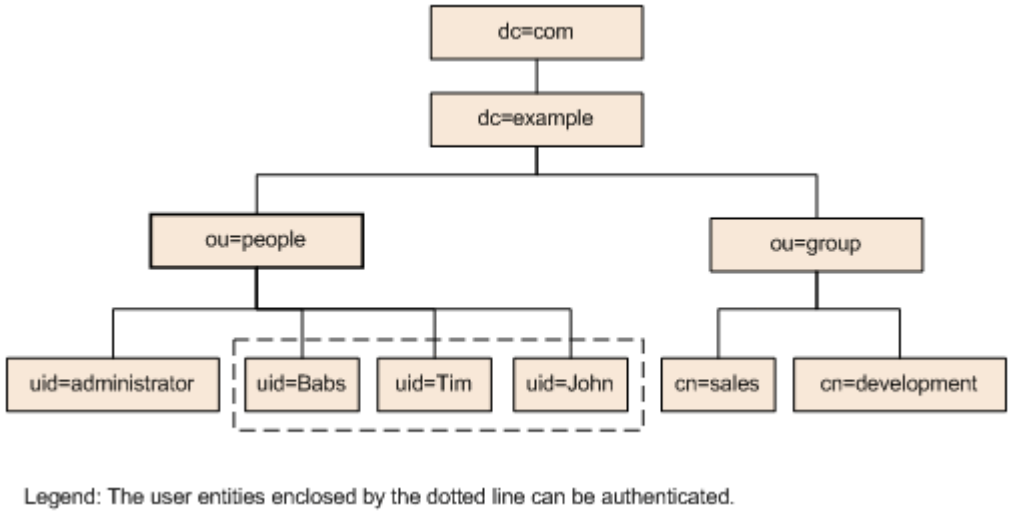


Figure 7-8 Example of the flat model

Note, however, that even if the flat model is being used, if either of the following conditions is satisfied, specify the settings by following the explanation for the hierarchical structure model:

- If a user attribute value other than the RDN attribute value is used as the user ID of Hitachi File Services Manager:

  If a user attribute value other than the RDN attribute value (for example, the Windows logon ID) of a user entry is used as the user ID of Hitachi File Services Manager, you must use the authentication method for the hierarchical structure model.
- If the RDN attribute value of a user entry includes an invalid character that cannot be used in a user ID for Hitachi File Services Manager:

  When using the authentication method for the flat model, the RDN attribute value of a user entry functions as the user ID for Hitachi File Services Manager. Therefore, if the RDN attribute value of a user entry includes an invalid character that cannot be used in a user ID of a Hitachi File Services Manager, you cannot use the authentication method for the flat model.

  Example of a valid RDN:

  `uid=John123S`

  `cn=John_Smith`

  Example of an invalid RDN:

  `uid=John:123S` (A colon is used.)

  `cn=John Smith` (A space is used between `John` and `Smith`.)

Modifying exauth.properties for LDAP authentication

This section describes the settings required for the `exauth.properties` file in order to use an LDAP server to authenticate users.

1. Specify values for the following properties in the `exauth.properties` file:

- Common properties (Table 7-12 Items to specify in the exauth.properties file when using an LDAP server for authentication (common items) on page 7-46)
- Properties for an external authentication server and an external authorization server

  Specify these property values for each LDAP server.

  The items you need to specify differ depending on whether you directly specify information about the LDAP server (Table 7-13 Items to specify in the exauth.properties file when using an LDAP server for authentication (when directly specifying information about the external authentication server) on page 7-47 and Table 7-14 Items to specify in the exauth.properties file when using an LDAP server for authentication (when an external authentication server and StartTLS are used for communication) on page 7-50) or you use the DNS server to look up the LDAP server (Table 7-15 Items to specify in the exauth.properties file when using an LDAP server for authentication (when using the DNS server to look up information about the external authentication server) on page 7-50).

The template of the `exauth.properties` file is stored in the following location:

Hitachi-Command-Suite-Common-Component-installation-folder`\sample\conf\exauth.properties`

Notes:

Do not enter a space at the beginning or end of a setting value. Also, do not enclose a setting value in double quotation marks ("). If you do, the value is ignored, and the default value is used instead.

2. Save the `exauth.properties` file in the following location:

   Hitachi-Command-Suite-Common-Component-installation-folder`\conf\exauth.properties`

   If the setting value of the `auth.ocsp.enable` or `auth.ocsp.responderURL` property is changed, the Hitachi File Services Manager must be restarted. If the setting value of any other property or attribute is changed, the change takes effect immediately.

Table 7-12 Items to specify in the exauth.properties file when using an LDAP server for authentication (common items) on page 7-46 through Table 7-15 Items to specify in the exauth.properties file when using an LDAP server for authentication (when using the DNS server to look up information about the external authentication server) on page 7-50 describe the items to specify in the `exauth.properties` file.

Table 7-12 Items to specify in the exauth.properties file when using an LDAP server for authentication (common items)

Property	Details
`auth.server.type`	Specify an external authentication server type. Specify `ldap`. Default value: `internal` (used when not linking to an external authentication server)

Property	Details
auth.server.name	Specify the server identification names of LDAP servers. You can specify any name for this property in order to identify which LDAP servers the settings such as the port number and the protocol for connecting to the LDAP server (see Table 7-13 Items to specify in the exauth.properties file when using an LDAP server for authentication (when directly specifying information about the external authentication server) on page 7-47 or Table 7-15 Items to specify in the exauth.properties file when using an LDAP server for authentication (when using the DNS server to look up information about the external authentication server) on page 7-50) are applied to. ServerName has been set as the initial value. You must specify at least one name. When specifying multiple LDAP server identification names, separate the names with commas (,). Do not register the same server identification name more than once. Specifiable values: No more than 64 bytes of the following characters: 0 to 9 A to Z a to z ! # ( ) + - . = @ [ ] ^ _ { } ~ Default value: none
auth.group.mapping	Specify whether to also link to an external authorization server. Specify true to link to an external authorization server. Specify false to not to link to an external authorization server. Default value: false

Table 7-13 Items to specify in the exauth.properties file when using an LDAP server for authentication (when directly specifying information about the external authentication server)

Attributes	Details
protocol#1	Specify the protocol for connecting to the LDAP server. This attribute is required. When communicating in plain text format, specify ldap. When using StartTLS communication, specify tls. Before specifying tls, make sure that one of the following encryption methods can be used on the LDAP server. • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA Specifiable values: ldap or tls Default value: none
host#2	Specify the host name or IP address of the LDAP server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets ([]). This attribute is required.

Attributes	Details
	Default value: none
port	Specify the port number of the LDAP server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP server. Specifiable values: 1 to 65535 Default value: 389
timeout	Specify the amount of time to wait before timing out when connecting to the LDAP server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
attr	Specify the attribute (Attribute Type) to use as the user ID during authentication. • For the hierarchical structure model Specify the name of the attribute containing the unique value to be used for identifying the user. The value stored in this attribute will be used as the user ID for Hitachi File Services Manager.#3 For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of Hitachi File Services Manager, specify the attribute name sAMAccountName in which the Windows logon ID has been defined. • For the flat model Specify the RDN attribute name of the user entry. For example, if the user's DN is uid=John,ou=People,dc=example,dc=com, specify the uid that is the attribute name of the RDN uid=John. sAMAccountName has been set as the initial value. This attribute is required. Default value: none
basedn	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP server. The user entries that are located in the hierarchy below this DN will be checked during authentication. If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP server without change. • For the hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries to be searched. For example, for Figure 7-7 Example of the hierarchical structure model on page 7-44, specify cn=group,dc=example,dc=com. • For the flat model Specify the DN of the hierarchy just above the user entries to be searched. For example, for Figure 7-8 Example of the flat model on page 7-45, specify ou=people,dc=example,dc=com.

Attributes	Details
	This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (\) to escape each character. Spaces `# + ; , < = > \` Default value: none
`retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
`domain.name`	Specify the name of a domain managed by the LDAP server. This item is required when an external authorization server is also linked to. Default value: none
`dns_lookup`	Specify `false`. Default value: `false`

Note:

To specify the attributes, use the following syntax:

`auth.ldap.`*auth.server.name-property-value*`.`*attribute*`=`*value*

#1:

When communicating by using StartTLS as the protocol for connecting to the LDAP server, you need to specify the security settings of Common Component. For details about specifying security settings in order to communicate by using StartTLS, see Setting the security for Hitachi Command Suite Common Component (communication with an LDAP server) on page 7-85.

#2:

When using StartTLS as the protocol for connecting to the LDAP server, in the `host` attribute specify the same host name as the value of CN in the LDAP server certificate. You cannot use an IP address.

#3:

The specified attribute must not include characters that cannot be used in a user ID of the Hitachi File Services Manager.

Table 7-14 Items to specify in the exauth.properties file when using an LDAP server for authentication (when an external authentication server and StartTLS are used for communication)

Property	Details
`auth.ocsp.enable`	Specify whether or not to verify the validity of an LDAP server's electronic signature certificate by using an OCSP responder or a CRL when the LDAP server and StartTLS are used for communication. If you want to verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`
`auth.ocsp.responderURL`	Specify the URL of an OCSP responder if you want to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: None

Table 7-15 Items to specify in the exauth.properties file when using an LDAP server for authentication (when using the DNS server to look up information about the external authentication server)

Attributes	Details
`protocol`	Specify the protocol for connecting to the LDAP server. This attribute is required. Specifiable values: `ldap` Default value: none
`port`	Specify the port number of the LDAP server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP server. Specifiable values: 1 to 65535 Default value: 389
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
`attr`	Specify the attribute (Attribute Type) to use as the user ID during authentication. • For the hierarchical structure model Specify the name of the attribute containing the unique value to be used for identifying the user. The value stored in this attribute will be used as the user ID for Hitachi File Services Manager.# For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of a Hitachi File

Attributes	Details
	Services Manager, specify the attribute name `sAMAccountName` in which the Windows logon ID has been defined. • For the flat model Specify the RDN attribute name of the user entry. For example, if the user's DN is `uid=John,ou=People,dc=example,dc=com`, specify the `uid` that is the attribute name of the RDN `uid=John`. `sAMAccountName` has been set as the initial value. This attribute is required. Default value: none
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP server. The user entries that are located in the hierarchy below this DN will be checked during authentication. If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP server without change. • For the hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries to be searched. For example, for Figure 7-7 Example of the hierarchical structure model on page 7-44, specify `cn=group,dc=example,dc=com`. • For the flat model Specify the DN of the hierarchy just above the user entries to be searched. For example, for Figure 7-8 Example of the flat model on page 7-45, specify `ou=people,dc=example,dc=com`. This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (`\`) to escape each character. Spaces `# + ; , < = > \` Default value: none
`retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
`domain.name`	Specify the domain name managed by the LDAP server. Default value: none
`dns_lookup`	Specify `true`.

Attributes	Details
	However, if the following attribute values are already set, the LDAP server will be connected to by using the user-specified values instead of by using the DNS server to look up the information. • `auth.ldap.`*auth.server.name-property-value*`.host` • `auth.ldap.`*auth.server.name-property-value*`.port` Default value: `false`

Note:

To specify the attributes, use the following syntax:

`auth.ldap.`*auth.server.name-property-value*`.`*attribute*`=`*value*

#:

The specified attribute must not include invalid characters that cannot be used in a user ID of the Hitachi File Services Manager.

The following examples show how to specify the properties:

- When directly specifying information about an LDAP server (when linking to only an external authentication server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.dns_lookup=false
```

- When Using the DNS server to look up an LDAP server (when linking to only an external authentication server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- When directly specifying about the LDAP server (when also linking to an authorization server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
```

```
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=false
```

- When using the DNS server to look up the LDAP server (when also linking to an authorization server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

Setting LDAP user information (LDAP authentication)

By using the `hcmds64ldapuser` command, you can register, on the management server, a user account used to search for LDAP user information. After registering a user account, you can use this command to delete such an account or check LDAP servers for which user accounts used to search for LDAP user information have been registered on the management server.

This step is necessary in the following cases:

- When the data structure is the hierarchical model
- When the data structure is the flat model and an external authorization server is also linked to#

#:

When registering an authorization group in Hitachi File Services Manager by using the GUI, if you want to check whether the distinguished name of the authorization group is registered on the external authorization server by using a user ID such as the `System` account registered in Hitachi File Services Manager, you need to register a user account used to search for LDAP user information on the management server.

In cases other than above, this step is not necessary, because LDAP user information is not searched during authentication and authorization. If a user account used to search for LDAP user information has been already registered, delete it.

Registering an account to search for LDAP user information (LDAP authentication)

Use the `hcmds64ldapuser` command to register a user account used to search for LDAP user information.

For a user account used to search for LDAP user information, register a user account that satisfies the following conditions:

- The user account is already registered in the LDAP server.
- The user account can bind to the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file
- The user account can search the attributes for all entries below the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file
- The user account can reference the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file
- The user account can reference the authorization groups that are under the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file (when an external authorization server is also linked to)
- The user account can search the attributes of the authorization groups that are under the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file and search the attributes of nested groups of the authorization groups (when an external authorization server is also linked to)

The format of the `hcmds64ldapuser` command is as follows:

`Hitachi-Command-Suite-Common-Component-installation-folder``\bin \hcmds64ldapuser /set /dn `*`DN-of-user-account-used-to-search-for-LDAP-user-info`*` [/pass `*`password-of-user-account-used-to-search-for-LDAP-user-info`*`] /name `*`server-identification-name`*

- *DN-of-user-account-used-to-search-for-LDAP-user-info*

  Specify a DN by following the rules defined in RFC4514. For example, if the following characters are included in a DN, you need to use a backslash (\) to escape each character.

  Spaces `# + , ; < = > \`
- *password-of-user-account-used-to-search-for-LDAP-user-info*

  This is case-sensitive and must exactly match the password registered in the LDAP server. If you execute the command without specifying the `pass` option, you will be prompted to enter a password (in the interactive mode, the entered character string is displayed by using replacement characters).
- *server-identification-name*

  Specify the server identification name that was specified for the `auth.server.name` property in the `exauth.properties` file.

Note:

In the LDAP server, you can use double quotation marks (") for the DN and password. In the management server, however, you need to register a user account whose DN and password do not include double quotation marks.

The following describes an example of execution using the data structure shown in Figure 7-7 Example of the hierarchical structure model on page 7-44. In this data structure, the DN of the entry used as the start point for searching is specified as `cn=group,dc=example,dc=com`. If a user searching the attribute values of all users (`Babs`, `Tim`, and `John`) below the DN has the `administrator` privilege, specify the `dn` option as the DN of `administrator` (`cn=administrator,cn=admin,dc=example,dc=com`). The following is an example of executing the command. The password of `administrator` is `administrator_pass`:

```
hcmds64ldapuser /set /dn
"cn=administrator,cn=admin,dc=example,dc=com" /pass
administrator_pass /name ServerName
```

Important:

- If you are using Active Directory, you can use the `dsquery` command provided by Active Directory to check the DN of a user. The following example shows how to use the `dsquery` command to check the DN of the user `administrator`, and also shows the execution results:

  ```
  dsquery user -name administrator
  "CN=administrator,CN=admin,DC=example,DC=com"
  ```

- If the DN includes commas such as `cn=administrator,cn=admin,dc=example,com`, specify as follows:

  ```
  hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example
  \,com" /pass administrator_pass /name ServerName
  ```

Deleting the account that searches for LDAP user information (LDAP authentication)

To delete a user account used to search for LDAP user information, execute the following command.

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64ldapuser /delete /name server-identification-name
```

Checking which LDAP servers have accounts that search for LDAP user information (LDAP authentication)

To check the names of LDAP servers for which a user account used to search for LDAP user information has been registered on the management server, execute the following command.

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64ldapuser /list
```

Checking the connection status of external authentication and authorization servers (LDAP authentication)

By using the `hcmds64checkauth` command, you can make sure that the external authentication server and the external authorization server can properly be connected to.

Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64checkauth [/user *user-ID* /pass *password*] [/summary]

- *user-ID* and *password* must match those of the user account that has been registered in the LDAP server. *user-ID* must be the same value as the one specified for the attribute `auth.ldap.`*auth.server.name-property-value*`.attr` in the `exauth.properties` file. However, you cannot specify a user account whose *user-ID* or *password* begins with a forward slash (`/`).

  If you execute the command without specifying the `user` option or the `pass` option, you will be prompted to enter a user ID and password (in the interactive mode, the entered character string is displayed by using replacement characters).
- If you execute the command with the `summary` option specified, the confirmation message is displayed in summary format.

If you execute the `hcmds64checkauth` command, the settings in the `exauth.properties` file, and the connection status of the external authentication server and the external authorization server are checked in the four phases described below. Check results are displayed for each phase.

Phase 1

The command verifies that common properties (Table 7-12 Items to specify in the exauth.properties file when using an LDAP server for authentication (common items) on page 7-46) have been correctly specified in the `exauth.properties` file.

Phase 2

The command verifies that the properties for the external authentication server and the external authorization server (Table 7-13 Items to specify in the exauth.properties file when using an LDAP server for authentication (when directly specifying information about the external authentication server) on page 7-47 to Table 7-15 Items to specify in the exauth.properties file when using an LDAP server for authentication (when using the DNS server to look up information about the external authentication server) on page 7-50) have been correctly specified in the `exauth.properties` file.

Phase 3

The command verifies that the external authentication server can be connected to.

Phase 4

If an external authorization server is also linked to, the command verifies that the external authorization server can be connected to and authorization groups can be searched.

When a phase finishes normally, the following message is displayed:

```
KAPM15004-I The result of the configuration check of Phase X was normal.
```

Note: X is the phase number.

- Example of executing the `hcmds64checkauth` command when the hierarchical structure model is used:
  The following example shows how to execute the `hcmds64checkauth` command, using the user account `John` shown in Figure 7-7 Example of the hierarchical structure model on page 7-44.
  This example assumes that `sAMAccountName` has been specified in `auth.ldap.`*`auth.server.name-property-value`*`.attr` in the `exauth.properties` file. If the `sAMAccountName` attribute value of `John` is `John_Smith`, specify `John_Smith` in *user-ID*. If the password of `John` to be used on the LDAP server is `John_pass`, specify `John_pass` in *password*.
  ```
  hcmds64checkauth /user John_Smith /pass John_pass
  ```
- Example of executing the `hcmds64checkauth` command when the flat model is used:
  The following example shows how to execute the `hcmds64checkauth` command, using the user account `John` shown in Figure 7-8 Example of the flat model on page 7-45.
  This example assumes that `uid` has been specified in `auth.ldap.`*`auth.server.name-property-value`*`.attr` in the `exauth.properties` file. As the RDN of `John` is given by `uid=John`, specify the RDN attribute value `John` in *user-ID*. If the password of `John` to be used on the LDAP server is `John_pass`, specify `John_pass` in *password*.
  ```
  hcmds64checkauth /user John /pass John_pass
  ```

Performing an external authentication by using a RADIUS server

To authenticate the system administrator account by using a RADIUS server, specify the following settings in Hitachi File Services Manager.

1. In the `exauth.properties` file on the management server, specify necessary information.
   Necessary settings depend on whether only an external authentication server is linked to or an external authorization server is also linked to.
   You can use either of the following methods to define the LDAP server to be used as an external authorization server:
   - In the `exauth.properties` file, directly specify information about the LDAP server to connect to.
     Specify information such as IP address and port number in the `exauth.properties` file for each LDAP server.
   - Use the DNS server to look up the LDAP server to connect to.
     Before using this method, you need to set up the DNS server environment on the OS of the LDAP server. In addition, you need to

register the host name, port number, and domain name of the LDAP server in the SRV records of the DNS server.

Important:

– To use StartTLS for communication between the management server and the LDAP server, you need to directly specify information about the LDAP server to connect to in the `exauth.properties` file.

– When using the DNS server to look up the LDAP server to connect to, it might take longer for users to log in.

2. When also linking to an external authorization server, on the management server, register a user account used to search for user information on the LDAP server.
3. On the RADIUS server, register the accounts of users who will use Hitachi File Services Manager.

   User IDs and passwords must consist of characters that can be used in Hitachi File Services Manager. Specify 1 to 256 bytes of the following characters:

   `0` to `9` `A` to `Z` `a` to `z` `! # $ % & ' ( ) * + - . = @ \ ^ _ |`

   In Hitachi File Services Manager, user IDs are not case-sensitive. The combination of character types for passwords must follow the settings in the external authentication server.
4. Specify a shared secret on the management server for communicating with the RADIUS server.
5. Register accounts and set permissions by using the GUI.

   When linking with only an external authentication server:

   - Register users.
   - Change the user authentication method.

     This operation is required if you want to change the authentication method for existing users.
   - Register users into user groups.
   - Configure both user management and the operation permissions for Hitachi File Services Manager.

   When also linking with an external authorization server:

   - Register authorization groups.
   - Configure both user management and the operation permissions for Hitachi File Services Manager.

   Reference note:

   Users who belong to nested groups of a registered authorization group can now also use Hitachi File Services Manager via the roles (permissions) set for the authorization group.
6. Use the `hcmds64checkauth` command to make sure that the external authentication server and the external authorization server can be properly connected to.

The following sections describe operations you need to perform on the management server.

Modifying exauth.properties for RADIUS authentication

This section describes the settings required for the `exauth.properties` file in order to use a RADIUS server to authenticate users.

1. Specify values for the following properties in the `exauth.properties` file:
   - Common properties (Table 7-16 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common items) on page 7-60)
   - Properties for an external authentication server (Table 7-17 Items to specify in the exauth.properties file when using a RADIUS server for authentication (settings for the external authentication server) on page 7-60)

     Specify these property values for each RADIUS server.
   - Properties for an external authorization server

     These properties need to be set when an external authorization server is also linked to. Specify information about the LDAP server for each domain.

     The items you need to specify differ depending on whether you directly specify information about the LDAP server (Table 7-18 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common settings for the external authorization server) on page 7-62 to Table 7-20 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when an external authorization server and StartTLS are used for communication) on page 7-64) or you use the DNS server to look up the LDAP server (Table 7-18 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common settings for the external authorization server) on page 7-62 and Table 7-21 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when using the DNS server to look up information about the external authorization server) on page 7-65).

   The template of the `exauth.properties` file is stored in the following location:

   Hitachi-Command-Suite-Common-Component-installation-folder`\sample\conf\exauth.properties`

   Note:

   Do not enter a space at the beginning or end of a setting value. Also, do not enclose a setting value in double quotation marks (`"`). If you do, the value is ignored, and the default value is used instead.
2. Save the `exauth.properties` file in the following location:

   Hitachi-Command-Suite-Common-Component-installation-folder`\conf\exauth.properties`

   If the setting value of the `auth.ocsp.enable` or `auth.ocsp.responderURL` property is changed, the Hitachi File Services

Manager must be restarted. If the setting value of any other property or attribute is changed, the change takes effect immediately.

Table 7-16 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common items) on page 7-60 through Table 7-21 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when using the DNS server to look up information about the external authorization server) on page 7-65 list and describe the properties to specify in the `exauth.properties` file.

Table 7-16 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common items)

Property names	Details
`auth.server.type`	Specify an external authentication server type. Specify `radius`. Default value: `internal` (used when not linking to an external authentication server)
`auth.server.name`	Specify the server identification names of RADIUS servers. You can specify any name for this property in order to identify which RADIUS servers the settings such as the port number and the protocol for connecting to the RADIUS server (see Table 7-17 Items to specify in the exauth.properties file when using a RADIUS server for authentication (settings for the external authentication server) on page 7-60) are applied to. `ServerName` has been set as the initial value. You must specify at least one name. When specifying multiple RADIUS server identification names, separate the names with commas (,). Do not register the same server identification name more than once. Specifiable values: No more than 64 bytes of the following characters: `0` to `9` `A` to `Z` `a` to `z` `!` `#` `(` `)` `+` `-` `.` `=` `@` `[` `]` `^` `_` `{` `}` `~` Default value: none
`auth.group.mapping`	Specify whether to also link to an external authorization server. Specify `true` to link to an external authorization server. Specify `false` to not to link to an external authorization server. Default value: `false`

Table 7-17 Items to specify in the exauth.properties file when using a RADIUS server for authentication (settings for the external authentication server)

Attributes	Details
`protocol`	Specify the protocol for RADIUS server authentication. This attribute is required. Specifiable values: `PAP` or `CHAP` Default value: none
`host`#1	Specify the host name or IP address of the RADIUS server. If you specify the host name, make sure

Attributes	Details
	beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets ([]). This attribute is required. Default value: none
port	Specify the port number for RADIUS server authentication. Make sure beforehand that the port you specify is set as the listen port number on the RADIUS server. Specifiable values: 1 to 65535 Default value: 1812
timeout	Specify the amount of time to wait before timing out when connecting to the RADIUS server. Specifiable values: 1 to 65535 (seconds) Default value: 1
retry.times	Specify the number of retries to attempt when an attempt to connect to the RADIUS server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 3
attr.NAS-Identifier#2	Specify the host name of the HDI management server. The RADIUS server uses this attribute value to identify the management server. The host name of the management server has been set as the initial value. Specifiable values: Specify no more than 253 bytes of the following characters: 0 to 9 A to Z a to z ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ Default value: none
attr.NAS-IP-Address#2	Specify the IPv4 address of the HDI management server. The RADIUS server uses this attribute value to identify the management server. If the format of the address is invalid, this property is disabled. Default value: none
attr.NAS-IPv6-Address#2	Specify the IPv6 address of the HDI management server. The RADIUS server uses this attribute value to identify the management server. Enclose the IPv6 address in square brackets ([]). If the format of the address is invalid, this property is disabled. Default value: none

Note:

To specify the attributes, use the following syntax:

auth.radius.*auth.server.name-property-value*.*attribute*=*value*

#1:

When linking to an external authorization server that is running on the same computer and using StartTLS as the protocol for connecting to the LDAP server, in the `host` attribute specify the same host name as the value of CN in the LDAP server certificate. You cannot use an IP address.

#2:

You must specify exactly one of the following: `attr.NAS-Identifier`, `attr.NAS-IP-Address`, or `attr.NAS-IPv6-Address`.

Table 7-18 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common settings for the external authorization server)

Attributes	Details
`domain.name`	Specify the name of a domain managed by the LDAP server. This item is required when an external authorization server is also linked to. Default value: none
`dns_lookup`	Specify whether to use the DNS server to look up the information about the LDAP server. If you want to directly specify information about the LDAP server in the `exauth.properties` file, specify `false`. If you want to use the DNS server to look up the information, specify `true`. However, if the following attribute values are already set, the LDAP server will be connected to by using the user-specified values instead of by using the DNS server to look up the information. • `auth.group.`*domain-name*`.host` • `auth.group.`*domain-name*`.port` Default value: `false`

Note:

To specify the attributes, use the following syntax:

`auth.radius.`*auth.server.name-property-value*`.`*attribute*`=`*value*

Table 7-19 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when directly specifying information about the external authorization server)

Attributes	Details
`protocol`[#1]	Specify the protocol for connecting to the LDAP server. When communicating in plain text format, specify `ldap`. When using StartTLS communication, specify `tls`. Before specifying `tls`, make sure that one of the following encryption methods can be used on the LDAP server. • TLS_RSA_WITH_AES_256_CBC_SHA

Attributes	Details
	• TLS_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA Specifiable values: `ldap` or `tls` Default value: `ldap`
`host`#2	If the external authentication server and the external authorization server are running on different computers, specify the host name or IP address of the LDAP server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets (`[]`). If you omit this attribute, the external authentication server and the external authorization server are assumed to be running on the same computer. Default value: none
`port`	Specify the port number of the LDAP server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP server. Specifiable values: 1 to 65535 Default value: 389
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP server. The user entries that are located in the hierarchy below this DN will be checked during authorization. Specify the DN of the hierarchy that includes all of the user entries to be searched. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (`\`) to escape each character. Spaces `# + ; , < = > \` If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP server without change. If you omit this attribute, the value specified in the `defaultNamingContext` property of Active Directory is assumed as the BaseDN. Default value: none
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
`retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP server fails. Specifiable values: 1 to 60 (seconds) Default value: 1

Attributes	Details
`retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20

Note:

To specify the attributes, use the following syntax:

`auth.group.`*domain-name*`.`*attribute*`=`*value*

For *domain-name*, specify the value specified for `auth.radius.`*auth.server.name-property-value*`.domain.name`.

#1:

When communicating by using StartTLS as the protocol for connecting to the LDAP server, you need to specify the security settings of Common Component. For details about specifying security settings in order to communicate by using StartTLS, see Setting the security for Hitachi Command Suite Common Component (communication with an LDAP server) on page 7-85.

#2:

When the external authentication server and the external authorization server are running on different computers and when using StartTLS as the protocol for connecting to the LDAP server, in the `host` attribute specify the same host name as the value of CN in the LDAP server certificate. You cannot use an IP address.

Table 7-20 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when an external authorization server and StartTLS are used for communication)

Property	Details
`auth.ocsp.enable`	Specify whether or not to verify the validity of an LDAP server's electronic signature certificate by using an OCSP responder or a CRL when the LDAP server and StartTLS are used for communication. If you want to verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`
`auth.ocsp.responderURL`	Specify the URL of an OCSP responder if you want to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: None

Table 7-21 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when using the DNS server to look up information about the external authorization server)

Attributes	Details
`protocol`	Specify the protocol for connecting to the LDAP server. Specifiable values: `ldap` Default value: `ldap`
`port`	Specify the port number of the LDAP server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP server. Specifiable values: 1 to 65535 Default value: 389
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP server. The user entries that are located in the hierarchy below this DN will be checked during authorization. Specify the DN of the hierarchy that includes all of the user entries to be searched. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (`\`) to escape each character. Spaces `# + ; , < = > \` If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP server without change. If you omit this attribute, the value specified in the `defaultNamingContext` property of Active Directory is assumed as the BaseDN. Default value: none
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
`retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20

Note:

To specify the attributes, use the following syntax:

`auth.group.`*domain-name*`.`*attribute*`=`*value*

For *domain-name*, specify the value specified for `auth.radius.`*auth.server.name-property-value*`.domain.name`.

The following examples show how to specify the properties:

- When linking to only an external authentication server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=false
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
```

- When directly specifying information about an external authorization server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=false
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.host=ldap.example.com
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using the DNS server to look up an external authorization server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=true
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

Setting LDAP user information (RADIUS authentication)

When using an LDAP server as an external authorization server, by using the `hcmds64ldapuser` command, you can register, on the management server, a user account used to search for LDAP user information. After registering a user account, you can use this command to delete such an account or check LDAP servers for which user accounts used to search for LDAP user information have been registered on the management server.

Registering an account to search for LDAP user information (RADIUS authentication)

Use the `hcmds64ldapuser` command to register a user account used to search for LDAP user information.

For a user account used to search for LDAP user information, register a user account that satisfies the following conditions:

- The user account is already registered in the LDAP server.
- The user account can bind to the DN specified for `auth.group.`*domain-name*`.basedn` in the `exauth.properties` file
- The user account can search the attributes for all entries below the DN specified for `auth.group.`*domain-name*`.basedn` in the `exauth.properties` file
- The user account can reference the DN specified for `auth.group.`*domain-name*`.basedn` in the `exauth.properties` file
- The user account can reference the authorization groups that are under the DN specified for `auth.group.`*domain-name*`.basedn` in the `exauth.properties` file.
- The user account can search the attributes of the authorization groups that are under the DN specified for `auth.group.`*domain-name*`.basedn` in the `exauth.properties` file and search the attributes of nested groups of the authorization groups

The format of the `hcmds64ldapuser` command is as follows:

Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64ldapuser /set /dn *DN-of-user-account-used-to-search-for-LDAP-user-info* [/pass *password-of-user-account-used-to-search-for-LDAP-user-info*] /name *domain-name*

- *DN-of-user-account-used-to-search-for-LDAP-user-info*

  Specify a DN by following the rules defined in RFC4514. For example, if the following characters are included in a DN, you need to use a backslash (\) to escape each character.

  Spaces # + , ; < = > \
- *password-of-user-account-used-to-search-for-LDAP-user-info*

  This is case-sensitive and must exactly match the password registered in the LDAP server. If you execute the command without specifying the `pass` option, you will be prompted to enter a password (in the interactive

mode, the entered character string is displayed by using replacement characters).

- *domain-name*
  Specify the domain name specified for `auth.radius.`*auth.server.name-property-value*`.domain.name` in the `exauth.properties` file.

Note:
In the LDAP server, you can use double quotation marks (") for the DN and password. In the management server, however, you need to register a user account whose DN and password do not include double quotation marks.

Important:

- You can use the `dsquery` command provided by Active Directory to check the DN of a user. The following example shows how to use the `dsquery` command to check the DN of the user `administrator`, and also shows the execution results:
  ```
  dsquery user -name administrator
  "CN=administrator,CN=admin,DC=example,DC=com"
  ```
- If the DN includes commas such as `cn=administrator,cn=admin,dc=example,com`, specify as follows:
  ```
  hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example
  \,com" /pass administrator_pass /name ServerName
  ```

Deleting the account that searches for LDAP user information (RADIUS authentication)

To delete a user account used to search for LDAP user information, execute the following command.

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64ldapuser /delete /name domain-name
```

Checking which LDAP servers have accounts that search for LDAP user information (RADIUS authentication)

To check the names of LDAP servers for which a user account used to search for LDAP user information has been registered on the management server, execute the following command:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64ldapuser /list
```

Setting a shared secret (RADIUS authentication)

By using the `hcmds64radiussecret` command, you can specify a shared secret on the management server to communicate with the RADIUS server. After specifying a shared secret, you can use this command to delete a shared secret or to list the server identification names of external authentication servers in which a shared secret has been registered.

Specifying a shared secret (RADIUS authentication)

To specify a shared secret by using the `hcmds64radiussecret` command, execute the following command.

Hitachi-Command-Suite-Common-Component-installation-folder\bin \hcmds64radiussecret [/set *shared-secret*] /name *RADIUS-server-indication-name*

- If you execute the command without specifying the `set` option, you will be prompted to enter a shared secret key (in the interactive mode, the entered character string is displayed by using replacement characters).
- *RADIUS-server-indication-name* must match a server indication name specified for the `auth.server.name` property in the `exauth.properties` file.

The following example shows how to execute the `hcmds64radiussecret` command when the shared secret is `secret01` and the server identification name of the RADIUS server is `ServerName`.

```
hcmds64radiussecret /set secret01 /name ServerName
```

Deleting a shared secret (RADIUS authentication)

To delete a shared secret, execute the following command.

Hitachi-Command-Suite-Common-Component-installation-folder\bin \hcmds64radiussecret /delete /name *RADIUS-server-indication-name*

Listing the IDs of RADIUS servers that have shared secrets (RADIUS authentication)

To list the server identification names of RADIUS servers in which a shared secret has been registered, execute the following command:

Hitachi-Command-Suite-Common-Component-installation-folder\bin \hcmds64radiussecret /list

Checking the connection status of external authentication and authorization servers (RADIUS authentication)

By using the `hcmds64checkauth` command, you can make sure that the external authentication server and the external authorization server can be properly connected to.

Hitachi-Command-Suite-Common-Component-installation-folder\bin \hcmds64checkauth [/user *user-ID* /pass *password*] [/summary]

- *user-ID* and *password* must match those of the user account that has been registered in the RADIUS server. However, you cannot specify a user account whose *user-ID* or *password* begins with a forward slash (`/`).

  If you execute the command without specifying the `user` option or the `pass` option, you will be prompted to enter a user ID and password (in the interactive mode, the entered character string is displayed by using replacement characters).
- If you execute the command with the `summary` option specified, the confirmation message is displayed in summary format.

If you execute the `hcmds64checkauth` command, the settings in the `exauth.properties` file, and the connection status of the external authentication server and the external authorization server are checked in the four phases described below. Check results are displayed for each phase.

Phase 1

The command verifies that common properties (Table 7-16 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common items) on page 7-60) have been correctly specified in the `exauth.properties` file.

Phase 2

The command verifies that the properties for the external authentication server (Table 7-17 Items to specify in the exauth.properties file when using a RADIUS server for authentication (settings for the external authentication server) on page 7-60) and properties for the external authorization server (Table 7-18 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common settings for the external authorization server) on page 7-62 through Table 7-21 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when using the DNS server to look up information about the external authorization server) on page 7-65) have been correctly specified in the `exauth.properties` file.

Phase 3

The command verifies that the external authentication server can be connected to.

Phase 4

If an external authorization server is also linked to, the command verifies that the external authorization server can be connected to and authorization groups can be searched.

When a phase finishes normally, the following message is displayed:

```
KAPM15004-I The result of the configuration check of Phase X was normal.
```

Note: X is the phase number.

Performing an external authentication by using a KDC server

To authenticate the system administrator account by using a KDC server, specify the following settings in Hitachi File Services Manager.

1. In the `exauth.properties` file on the management server, specify necessary information.

   Necessary settings depend on whether only an external authentication server is linked to or an external authorization server is also linked to.

   You can use either of the following methods to define the KDC server to be used as an external authorization server:

   - In the `exauth.properties` file, directly specify information about the KDC server to connect to.

Specify information about the KDC server, such as the IP address and port number, in the `exauth.properties` file for each realm.

- Use the DNS server to look up the KDC server to connect to.

  Specify information about the DNS server that manages KDC servers in the `exauth.properties` file.

  In addition, before using this method, you need to register the host name, port number, and realm name of the KDC server in the SRV records of the DNS server.

Important:

– To use StartTLS for communication between the management server and the LDAP server, you need to directly specify information about the KDC server to connect to in the `exauth.properties` file.

– When using the DNS server to look up the KDC server to connect to, it might take longer for users to log in.

2. When also linking to an external authorization server, on the management server, register a user account used to search for user information on the LDAP server.
3. On the KDC server, register the accounts of users who will use Hitachi File Services Manager.

   User IDs and passwords must consist of characters that can be used in Hitachi File Services Manager. Specify 1 to 256 bytes of the following characters:

   `0` to `9` `A` to `Z` `a` to `z` `!` `#` `$` `%` `&` `'` `(` `)` `*` `+` `-` `.` `=` `@` `\` `^` `_` `|`

   In Hitachi File Services Manager, user IDs are not case-sensitive. The combination of character types for passwords must follow the settings in the external authentication server.
4. Register accounts and set permissions by using the GUI.

   When linking with only an external authentication server:

   - Register users.
   - Change the user authentication method.

     This operation is required if you want to change the authentication method for existing users.
   - Register users into user groups.
   - Configure both user management and the operation permissions for Hitachi File Services Manager.

   When also linking with an external authorization server:

   - Register authorization groups.
   - Configure both user management and the operation permissions for Hitachi File Services Manager.

   Reference note:

   Users who belong to nested groups of a registered authorization group can now also use Hitachi File Services Manager via the roles (permissions) set for the authorization group.

5. Use the `hcmds64checkauth` command to make sure that the external authentication server and the external authorization server can be properly connected to.

The following sections describe operations you need to perform on the management server.

Modifying exauth.properties for Kerberos authentication

This section describes the settings required for the `exauth.properties` file in order to use a KDC server to authenticate users.

1. Specify values for the necessary properties in the `exauth.properties` file:

   - Common properties (Table 7-22 Items to specify in the exauth.properties file when using a KDC server for authentication (common items) on page 7-73)
   - Properties for an external authentication server

     Specify these property values for each KDC server.

     The items you need to specify differ depending on whether you directly specify information about the KDC server (Table 7-23 Items to specify in the exauth.properties file when using a KDC server for authentication (when directly specifying information about the external authentication server) on page 7-73) or you use the DNS server to look up the KDC server (Table 7-24 Items to specify in the exauth.properties file when using a KDC server for authentication (when using the DNS server to look up information about the external authentication server) on page 7-75).
   - Properties for an external authorization server (Table 7-25 Items to specify in the exauth.properties file when using a KDC server for authentication (settings for the external authorization server) on page 7-76 and Table 7-26 Items to specify in the exauth.properties file when using a KDC server for authentication (when an external authorization server and StartTLS are used for communication) on page 7-77)

     These properties need to be set if you directly specify information about the KDC server and an external authorization server is also linked. Specify the properties for each realm.

   The template of the `exauth.properties` file is stored in the following location:

   Hitachi-Command-Suite-Common-Component-installation-folder\sample\conf\exauth.properties

   Note:

   Do not enter a space at the beginning or end of a setting value. Also, do not enclose a setting value in double quotation marks ("). If you do, the value is ignored, and the default value is used instead.

2. Save the `exauth.properties` file in the following location:

   Hitachi-Command-Suite-Common-Component-installation-folder\conf\exauth.properties

If the setting value of the `auth.ocsp.enable` or `auth.ocsp.responderURL` property is changed, the Hitachi File Services Manager must be restarted. If the setting value of any other property or attribute is changed, the change takes effect immediately.

Table 7-22 Items to specify in the exauth.properties file when using a KDC server for authentication (common items) on page 7-73 through Table 7-26 Items to specify in the exauth.properties file when using a KDC server for authentication (when an external authorization server and StartTLS are used for communication) on page 7-77 list and describe the properties to specify in the `exauth.properties` file.

Table 7-22 Items to specify in the exauth.properties file when using a KDC server for authentication (common items)

Property names	Details
`auth.server.type`	Specify an external authentication server type. Specify `kerberos`. Default value: `internal` (used when not linking to an external authentication server)
`auth.group.mapping`	Specify whether to also link to an external authorization server. Specify `true` to link to an external authorization server. Specify `false` to not to link to an external authorization server. Default value: `false`

Table 7-23 Items to specify in the exauth.properties file when using a KDC server for authentication (when directly specifying information about the external authentication server)

Attributes	Details
`default_realm`	Specify the default realm name. If you specify a user ID but not a realm name in the login window of the GUI, the user is authenticated as a user who belongs to the realm specified for this attribute. This attribute is required. Default value: none
`dns_lookup_kdc`	Specify `false`. Default value: `false`
`default_tkt_enctypes`	Specify the encryption type used for Kerberos authentication. This property is enabled only if the management server OS is Windows. You can use the following encryption types: • aes128-cts • rc4-hmac • des3-cbc-sha1 • des-cbc-md5

Attributes	Details
	• des-cbc-crc If you want to specify multiple encryption types, use a comma to separate the encryption types. Among the specified encryption types, an encryption type that is supported by both the management server OS and a KDC server will be used. Default value: None (DES-CBC-MD5 is used for authentication.)
`clockskew`	Specify the acceptable range of difference between the management server time and KDC server time. If the difference exceeds this value, an authentication error occurs. Specifiable values: 0 to 300 (seconds) Default value: 300
`timeout`	Specify the amount of time to wait before timing out when connecting to the KDC server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 3
`realm_name`	Specify the realm identification names. You can specify any name for this attribute in order to identify which realms the property attribute settings are applied to. You must specify at least one name. When specifying multiple realm identification names, separate the names with commas (,). Do not register the same realm identification name more than once. Default value: none
value-specified-for-realm_name`.realm`	Specify the name of the realm set in the KDC server. This attribute is required. Default value: none
value-specified-for-realm_name`.kdc`	Specify the information about the KDC server in the following format: *host-name-or-IP-address*`[:`*port-number*`]` This attribute is required. *host-name-or-IP-address* If you specify the host name, make sure beforehand that the name can be resolved to an IP address. If you specify the IP address, use an IPv4 address. In an IPv6 environment, you must specify the host name. Note that you cannot specify the loopback address (`localhost` or `127.0.0.1`). *port-number*

Attributes	Details
	Make sure beforehand that the port you specify is set as the listen port number on the KDC server. If you do not specify a port number or the specified port number cannot be used in a KDC server, 88 is assumed. When specifying multiple KDC servers, separate them with commas as follows: *host-name-or-IP-address*[:*port-number*] ,*host-name-or-IP-address*[:*port-number*],...

Note:

To specify the attributes, use the following syntax:

`auth.kerberos.`*attribute*=*value*

Table 7-24 Items to specify in the exauth.properties file when using a KDC server for authentication (when using the DNS server to look up information about the external authentication server)

Attributes	Details
`default_realm`	Specify the default realm name. If you specify a user ID but not a realm name in the login window of the GUI, the user is authenticated as a user who belongs to the realm specified for this attribute. This attribute is required. Default value: none
`dns_lookup_kdc`	Specify `true`. This attribute is required. However, if all the following attributes values are already set, the KDC server will not be looked up by using the DNS server. • `realm_name` • *value-specified-for-realm_name*`.realm` • *value-specified-for-realm_name*`.kdc`
`default_tkt_enctypes`	Specify the encryption type used for Kerberos authentication. This property is enabled only if the management server OS is Windows. You can use the following encryption types: • aes128-cts • rc4-hmac • des3-cbc-sha1 • des-cbc-md5 • des-cbc-crc If you want to specify multiple encryption types, use a comma to separate the encryption types. Among the specified encryption types, an encryption type that is supported by both the management server OS and a KDC server will be used.

Attributes	Details
	Default value: None (DES-CBC-MD5 is used for authentication.)
clockskew	Specify the acceptable range of difference between the management server time and KDC server time. If the difference exceeds this value, an authentication error occurs. Specifiable values: 0 to 300 (seconds) Default value: 300
timeout	Specify the amount of time to wait before timing out when connecting to the KDC server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 3

Note:

To specify the attributes, use the following syntax:

auth.kerberos.*attribute*=*value*

Table 7-25 Items to specify in the exauth.properties file when using a KDC server for authentication (settings for the external authorization server)

Attributes	Details
protocol#	Specify the protocol for connecting to the LDAP server. When communicating in plain text format, specify ldap. When using StartTLS communication, specify tls. StartTLS communication can be used only when directly specifying information about the KDC server. Before specifying tls, make sure that one of the following encryption methods can be used on the LDAP server. • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA Specifiable values: ldap or tls Default value: ldap
port	Specify the port number of the LDAP server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP server. Specifiable values: 1 to 65535 Default value: 389
basedn	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP server. The user entries that are located in the hierarchy below this DN will be checked during authorization. Specify the DN of the hierarchy that includes all of the user entries to be searched.

Attributes	Details
	Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (\) to escape each character. Spaces # + ; , < = > \ If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP server without change. If you omit this attribute, the value specified in the defaultNamingContext property of Active Directory is assumed as the BaseDN. Default value: none
timeout	Specify the amount of time to wait before timing out when connecting to the LDAP server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
retry.interval	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
retry.times	Specify the number of retries to attempt when an attempt to connect to the LDAP server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20

Note:

To specify the attributes, use the following syntax:

auth.group.*realm-name*.*attribute*=*value*

For *realm-name*, specify the value specified for auth.kerberos.*realm_name-property-value*.realm.

#:

When communicating by using StartTLS as the protocol for connecting to the LDAP server, you need to specify the security settings of Common Component. For details about specifying security settings in order to communicate by using StartTLS, see Setting the security for Hitachi Command Suite Common Component (communication with an LDAP server) on page 7-85.

Table 7-26 Items to specify in the exauth.properties file when using a KDC server for authentication (when an external authorization server and StartTLS are used for communication)

Property	Details
auth.ocsp.enable	Specify whether or not to verify the validity of an LDAP server's electronic signature certificate by using an OCSP responder or

Property	Details
	a CRL when the LDAP server and StartTLS are used for communication. If you want to verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`
`auth.ocsp.responderURL`	Specify the URL of an OCSP responder if you want to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: None

The following examples show how to specify the properties:

- When directly specifying information about a KDC server (when not linking to an external authorization server):

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
```

- When using the DNS server to look up a KDC server (when not linking to an external authorization server):

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- When directly specifying information about a KDC server (when also linking to an external authorization server):

```
auth.server.type=kerberos
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using the DNS server to look up a KDC server (when also linking to an external authorization server):

```
auth.server.type=kerberos
auth.group.mapping=true
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

Setting LDAP user information (Kerberos authentication)

When using an LDAP server as an external authorization server, by using the `hcmds64ldapuser` command, you can register, on the management server, a user account used to search for LDAP user information. After registering a user account, you can use this command to delete such an account or check LDAP servers for which user accounts used to search for LDAP user information have been registered on the management server.

Registering an account to search for LDAP user information (Kerberos authentication)

Use the `hcmds64ldapuser` command to register a user account used to search for LDAP user information.

For a user account used to search for LDAP user information, register a user account that satisfies the following conditions:

- The user account is already registered in the LDAP server.
- The user account can bind to the DN specified for `auth.group.`*realm-name*`.basedn` in the `exauth.properties` file
- The user account can search the attributes for all entries below the DN specified for `auth.group.`*realm-name*`.basedn` in the `exauth.properties` file
- The user account can reference the DN specified for `auth.group.`*realm-name*`.basedn` in the `exauth.properties` file
- The user account can reference the authorization groups that are under the DN specified for `auth.group.`*realm-name*`.basedn` in the `exauth.properties` file
- The user account can search the attributes of the authorization groups that are under the DN specified for `auth.group.`*realm-name*`.basedn` in the `exauth.properties` file and search the attributes of nested groups of the authorization groups

The format of the `hcmds64ldapuser` command is as follows:

Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64ldapuser /set /dn *DN-of-user-account-used-to-search-for-LDAP-user-info* [/pass *password-of-user-account-used-to-search-for-LDAP-user-info*] /name *realm-name*

- *DN-of-user-account-used-to-search-for-LDAP-user-info*

Specify a DN by following the rules defined in RFC4514. For example, if the following characters are included in a DN, you need to use a backslash (\) to escape each character.

Spaces # + , ; < = > \

- *password-of-user-account-used-to-search-for-LDAP-user-info*

  This is case-sensitive and must exactly match the password registered in the LDAP server. If you execute the command without specifying the pass option, you will be prompted to enter a password (in the interactive mode, the entered character string is displayed by using replacement characters).

- *realm-name*

  If you directly specify information about a KDC server in the exauth.properties file, specify the value specified for auth.kerberos.default_realm or auth.kerberos.*auth.kerberos.realm_name-property-value*.realm.

  If you specify the settings in the exauth.properties file to use the DNS server to look up information about a KDC server, specify the realm name registered in the DNS server.

Note:

In the LDAP server, you can use double quotation marks (") for the DN and password. In the management server, however, you need to register a user account whose DN and password do not include double quotation marks.

Important:

- You can use the dsquery command provided by Active Directory to check the DN of a user. The following example shows how to use the dsquery command to check the DN of the user administrator, and also shows the execution results:

  ```
  dsquery user -name administrator
  "CN=administrator,CN=admin,DC=example,DC=com"
  ```

- If the DN includes commas such as cn=administrator,cn=admin,dc=example,com, specify as follows:

  ```
  hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example
  \,com" /pass administrator_pass /name ServerName
  ```

Deleting the account that searches for LDAP user information (Kerberos authentication)

To delete a user account used to search for LDAP user information, execute the following command.

Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64ldapuser /delete /name *realm-name*

Checking which LDAP servers have accounts that search for LDAP user information (Kerberos authentication)

To check the names of LDAP servers for which a user account used to search for LDAP user information has been registered on the management server, execute the following command.

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64ldapuser /list
```

Checking the connection status of external authentication and authorization servers (Kerberos authentication)

By using the `hcmds64checkauth` command, you can make sure that the external authentication server and the external authorization server can be properly connected to. If you have specified multiple realm names in the `exauth.properties` file, perform this operation for each realm.

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64checkauth [/user user-ID /pass password] [/summary]
```

- The user account to be specified for *user-ID* and *password* depends on whether only an external authentication server is linked or an external authorization server is also linked to.

  When linking to only an external authentication server:

  Specify a user account that is registered in Hitachi File Services Manager and whose authentication method has been set to Kerberos authentication.

  When also linking to an external authorization server:

  Specify a user account that is not registered in Hitachi File Services Manager.

  If you specify a user who belongs to a realm different from the realm name specified for `default_realm` in the `exauth.properties` file, specify a character string that contains the realm name for *user-ID*. If you specify a user who belongs to the realm specified for `default_realm` in the `exauth.properties` file, you can omit the realm name. In addition, note that you cannot specify a user account whose *user-ID* or *password* begins with a forward slash (`/`).

  If you execute the command without specifying the `user` option or the `pass` option, you will be prompted to enter a user ID and password (in the interactive mode, the entered character string is displayed by using replacement characters).
- If you execute the command with the `summary` option specified, the confirmation message is displayed in summary format.

If you execute the `hcmds64checkauth` command, the settings in the `exauth.properties` file, and the connection status of the external authentication server and the external authorization server are checked in the four phases described below. Check results are displayed for each phase.

Phase 1

The command verifies that common properties (Table 7-22 Items to specify in the exauth.properties file when using a KDC server for authentication (common items) on page 7-73) have been correctly specified in the `exauth.properties` file.

Phase 2

The command verifies that the properties for the external authentication server (Table 7-23 Items to specify in the exauth.properties file when using a KDC server for authentication (when directly specifying information about the external authentication server) on page 7-73 and Table 7-24 Items to specify in the exauth.properties file when using a KDC server for authentication (when using the DNS server to look up information about the external authentication server) on page 7-75) and properties for the external authorization server (Table 7-25 Items to specify in the exauth.properties file when using a KDC server for authentication (settings for the external authorization server) on page 7-76 and Table 7-26 Items to specify in the exauth.properties file when using a KDC server for authentication (when an external authorization server and StartTLS are used for communication) on page 7-77) have been correctly specified in the `exauth.properties` file.

Phase 3

The command verifies that the external authentication server can be connected to.

Phase 4

If an external authorization server is also linked to, the command verifies that the external authorization server can be connected to and authorization groups can be searched.

When a phase finishes normally, the following message is displayed:

```
KAPM15004-I The result of the configuration check of Phase X was normal.
```

Note: X is the phase number.

Encryption types for Kerberos authentication

In Hitachi File Services Manager, the encryption types listed below can be used for Kerberos authentication. Configure the KDC server so that one of the following encryption types can be used.

- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC
- DES3-CBC-SHA1
- DES-CBC-CRC
- DES-CBC-MD5

Note that, if the OS of the external authentication server is Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 and the environment meets both of the following conditions, user authentication might not work properly:

- The domain functional level on the external authentication server is set to **Windows Server 2003** or **Windows 2000**.
- The OS of the management server supports AES128-CTS encryption.

For example, even if the domain functional level of Active Directory is set to **Windows Server 2003** or **Windows 2000**, in either of the following cases, the corresponding user cannot be authenticated via Active Directory:

- A user existing before an Active Directory system was built is migrated to the Active Directory system, which has a domain functional level of **Windows Server 2003**, and then the user's password is changed.
- An Active Directory system built in Windows Server 2003 is migrated to an Active Directory system built in Windows Server 2008, Windows Server 2012 with a domain functional level of **Windows Server 2003**, and then a user's password is changed.

In this case, change the `default_tkt_enctypes` property setting in the `exauth.properties` file as follows:

```
auth.kerberos.default_tkt_enctypes=rc4-hmac
```

Connecting to Device Manager to manage user accounts

If Hitachi File Services Manager is linked with Device Manager, Hitachi File Services Manager must connect to Device Manager to manage user accounts. If you install Hitachi File Services Manager on a management server on which Device Manager version 8.0 or later has already been installed, or if you install Hitachi File Services Manager and Device Manager on different machines, specify settings so that Hitachi File Services Manager connects to Device Manager to manage user accounts.

If you install Hitachi File Services Manager on a management server on which Device Manager version 8.0 or later has already been installed

To specify settings so that Hitachi File Services Manager connects to Device Manager to manage user accounts, perform the following procedure:

1. On the management server, execute the following command to set the information required to connect to Device Manager:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64prmset /host IP-address-or-host-name-of-the-management-server /
   port Device-Manager-port-number [/sslport Device-Manager-port-number-for-
   SSL-connection]
   ```

2. Restart Hitachi File Services Manager and Device Manager.

   For details about how to start and stop Hitachi File Services Manager, see Starting and stopping Hitachi File Services Manager on page 7-32. To restart Device Manager, ask the Device Manager system administrator.

If you install Hitachi File Services Manager and Device Manager on different machines

To specify settings so that Hitachi File Services Manager connects to Device Manager to manage user accounts, perform the following procedure:

Also note that the procedure for changing the management server differs depending on the order in which Hitachi File Services Manager and Device Manager were installed.

Hitachi File Services Manager is installed after Device Manager is operational or both Hitachi File Services Manager and Device Manager are installed at the same time

1. Execute the following command on the management server on which Hitachi File Services Manager is installed to set the information required to connect the server on which Device Manager is installed:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64prmset /host Device-Manager-IP-address-or-host-name /port port-
number [/sslport SSL-port-number]
```

2. Restart Hitachi File Services Manager.

   For details about how to start and stop Hitachi File Services Manager, see Starting and stopping Hitachi File Services Manager on page 7-32.

Device Manager is installed after Hitachi File Services Manager is operational

1. Execute the following command on the management server on which Hitachi File Services Manager is installed to output the authentication data for Hitachi File Services Manager:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64authmove /export /datapath absolute-path-of-the-folder-to-which-
Hitachi-File-Services-Manager-authentication-data-is-output
```

2. Ask the Device Manager system administrator to migrate the Hitachi File Services Manager authentication data.
3. Execute the following command on the management server on which Hitachi File Services Manager is installed to set the information required to connect the server on which Device Manager is installed:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64prmset /host Device-Manager-IP-address-or-host-name /port port-
number [/sslport SSL-port-number]
```

4. Restart Hitachi File Services Manager and Device Manager.

   For details about how to start and stop Hitachi File Services Manager, see Starting and stopping Hitachi File Services Manager on page 7-32. To restart Device Manager, ask the Device Manager system administrator.

Setting the security for Hitachi Command Suite Common Component (communication with an LDAP server)

In Hitachi File Services Manager, when performing user authentication or authorization by linking with an LDAP server, you can encrypt network transmissions between Hitachi File Services Manager and the LDAP server by using StartTLS. To use StartTLS to protect communications between the management server and LDAP server, you need to perform the following operations:

- Obtain a certificate for the LDAP server
- Import the certificate into the truststore file

To encrypt network transmissions between Hitachi File Services Manager and an LDAP server by using StartTLS, you also need to set up the `exauth.properties` file.

Note:

The `CN` (the `CN` in the `Subject` section) of the certificate for the LDAP server must be the same as the value specified for the following attribute in the `exauth.properties` file.

If the authentication method is LDAP:

`auth.ldap.`*value-specified-for-auth.server.name*`.host`

If the authentication method is RADIUS and an external authorization server is also linked to:

If the external authentication server and the external authorization server are running on the same computer:

`auth.radius.`*value-specified-for-auth.server.name*`.host`

If the external authentication server and the external authorization server are running on different computers:

`auth.group.`*domain-name*`.host`

If the authentication method is Kerberos and an external authorization server is also linked to:

`auth.kerberos.`*value-specified-for-auth.kerberos.realm_name*`.kdc`

Obtaining a certificate for an LDAP server

Obtain a server certificate for the LDAP server that communicates with the management server. For details, see the documentation for the LDAP server you use.

If you use a digitally-signed certificate issued by a certificate authority, make sure that all certificates issued by authorities between the certificate authority that issued the server certificate and the root certificate authority must form a certificate chain. To use a CRL distribution point (CDP) to verify the validity of the digitally-signed certificate, you must obtain a certificate whose AIA and CDP fields do not contain URLs that begin with `ldap`.

If you have obtained a certificate for the LDAP server from a well-known CA, the CA certificate might already be set up in the standard truststore

referenced by Common Component. Execute the command below to check this. If a registered CA certificate is used to authenticate LDAP server certificates, you do not need to set up the truststore described in Importing an LDAP server certificate to the truststore file on page 7-86.

Hitachi-Command-Suite-Common-Component-installation-folder\bin \hcmds64keytool -list -v -keystore *truststore-file-name* -storepass *password-to-access-the-truststore*

- For the `-keystore` option, specify the truststore file to be referenced.

  Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB \jdk\jre\lib\security\cacerts
- For the `-storepass` option, specify the password used to reference the truststore `cacerts`. The default is `changeit`.

Note:

Do not import and use your own certificate into the truststore `cacerts` because that truststore is updated when Common Component is upgraded.

Importing an LDAP server certificate to the truststore file

Import the certificate for the LDAP server into the truststore used by Common Component. We recommend importing the LDAP server certificate into `ldapcacerts`. The certificate can be imported to `jssecacerts`, even when the certificate is shared with other programs. If no truststore file exists, create a truststore file.

Hitachi-Command-Suite-Common-Component-installation-folder\conf\sec \ldapcacerts

Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\jdk \jre\lib\security\jssecacerts

To create a truststore file, import a certificate, and check the contents, use the `hcmds64keytool` utility.

To create a truststore file and import a certificate, execute the following command:

Hitachi-Command-Suite-Common-Component-installation-folder\bin \hcmds64keytool -import -alias *unique-name-in-the-truststore* -file *certificate-file-name* -keystore *truststore-file-name* -storepass *password-to-access-the-truststore*

- For the `-alias` option, specify the name used to identify the certificate in the truststore.
- For the `-file` option, specify the certificate file.
- For the `-keystore` option, specify the truststore file to be registered and created.
- For the `-storepass` option, specify the password used to access the truststore.

To view the contents of the truststore, execute the following command:

Hitachi-Command-Suite-Common-Component-installation-folder\bin \hcmds64keytool -list -v -keystore *truststore-file-name* -storepass *password-to-access-the-truststore*

- For the `-keystore` option, specify the truststore file to be checked.
- For the `-storepass` option, specify the password used to access the truststore.

Note that, to apply the truststore, you need to restart Hitachi File Services Manager by using the following procedure:

1. Stop Hitachi File Services Manager.
   For details on how to do this, see Stopping Hitachi File Services Manager on page 7-34.
2. Start Hitachi File Services Manager.
   For details on how to do this, see Starting Hitachi File Services Manager on page 7-33.

Notes:

- If there are multiple certificate files, import certificate files by specifying alias names not used in the truststore.
- Note the following when you use the `hcmds64keytool` utility to specify a unique name in the truststore, the truststore file name, and the password:
  - Do not use the following symbols in the file name: `: , ; * ? " < > |`
  - Specify the file name as a character string of no more than 255 bytes.
  - Do not include double quotation marks (") in the unique name in the truststore or the password.

Setting up the Hitachi File Services Manager environment

The system administrator can set up or change Hitachi File Services Manager environment by editing the configuration files.

If the management server is being used in a cluster configuration, the settings must be same on both the executing node and standby node.

This section describes how the system administrator can set up Hitachi File Services Manager environment.

Changing the log file settings

The system administrator can change settings of Hitachi File Services Manager message log, such as maximum capacity or output level, by editing the property file.

To change the log file settings:

1. Edit the property file (`user.properties`) to change the log file settings.
   The property file is located in the following folder:
   Hitachi-File-Services-Manager-installation-folder\conf\

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

   For details on how to do this, see Starting and stopping Hitachi File Services Manager on page 7-32.

The following table lists the properties related to log file settings.

Table 7-27 Properties in the user.properties file related to log file settings

Property	Description

`hnasm.common.logger.loglevel`	Specify the output level of the Hitachi File Services Manager message log.
	Specifiable value[#1]
	`-1`, `0` to `1000`
	Default value
	`20`
	If you specify an invalid value, `20` is assumed.

`hnasm.common.logger.syslog.loglevel`	Specify the output level of the Hitachi File Services Manager event log.
	Specifiable value[#1]
	`-1`, `0` to `1000`
	Default value
	`0`
	If you specify an invalid value, `0` is assumed.

`hnasm.common.logger.maxfilenumber`	Specify the maximum number of backups of the Hitachi File Services Manager message log.
	Specifiable value[#2]
	`1` to `16`
	Default value
	`10`
	If you specify an invalid value, `10` is assumed.

`hnasm.common.logger.maxfilesize`	Specify the maximum capacity of the Hitachi File Services Manager message log in bytes.
	Specifiable value[#2]
	`4096` to `2147483647`
	Default value
	`2097152`
	If you specify an invalid value, `2097152` is assumed.

#1: The meaning of the values is listed below. Note that we recommend that you use the default value.

- -1: For a message log, nothing is output. For an event log, only the Hitachi Command Suite Common Component log is output.

- 0 to 9: System information (start and stop, significant errors, etc.) is output.
- 10 to 19: System information and error information are output.
- 20 to 29: System information, error information, and execution history information are output.
- 30 to 1000: Debug information is output.

#2: We recommend that you set a value equal to or larger than the default value.

The following shows an example of the coding in the `user.properties` file:

```
hnasm.common.logger.loglevel=20
hnasm.common.logger.syslog.loglevel=0
hnasm.common.logger.maxfilenumber=10
hnasm.common.logger.maxfilesize=2097152
```

Changing the update setting of the license information

The system administrator can edit the property file to specify whether to automatically update the license information every time it is displayed in the License Settings subwindow.

To change the update setting of the license information:

1. Edit the property file (`user.properties`) to change the update setting of the license information.

   The property file is located in the following folder:

   Hitachi-File-Services-Manager-installation-folder\conf\
2. Stop and then restart Hitachi File Services Manager and Hitachi Command Suite Common Component.

   For details on how to do this, see Starting and stopping Hitachi File Services Manager on page 7-32.

The following table describes the property used to change the update setting of the license information.

Table 7-28 Properties in the user.properties file used for changing the update setting of the license information

Property	Description

`hnasm.model.refresh.screen.license`	Specifies whether to automatically update the license information every time it is displayed.
	`true`
	Specify this to enable automatic information updates.
	`false`
	Specify this to disable automatic information updates.

Property	Description
	The default setting is `true`. If the specified value is neither of the above two values, `true` will be assumed.

The following shows an example of the coding in the `user.properties` file:

```
...
hnasm.model.refresh.screen.license=true
...
```

Changing the port numbers used by Hitachi Command Suite Common Component

The system administrator can edit the configuration files to change the port numbers used by Hitachi Command Suite Common Component.

To change a port number for Hitachi Command Suite Common Component after installing Hitachi File Services Manager:

1. Stop the services of the Hitachi Command Suite products whose versions are earlier than 8.

   This step is necessary only if Hitachi Command Suite whose versions are earlier than 8 are installed. For details on how to stop the service of a Hitachi Command Suite product, see the documentation for that product.
2. Stop Hitachi File Services Manager and Hitachi Command Suite Common Component.

   For details on how to do this, see Starting and stopping Hitachi File Services Manager on page 7-32.
3. Edit the configuration files for Hitachi Command Suite Common Component to change the port number.

   The method used to change the port number depends on the port number.

Table 7-29 Port number settings files for Hitachi Command Suite Common Component

Default port number	Settings files	Location
22015/tcp	*Hitachi-Command-Suite-Common-Component-installation-folder*`\uCPSB\httpsd\conf\user_httpsd.conf`	`Listen`
22016/tcp	*Hitachi-Command-Suite-Common-Component-installation-folder*`\uCPSB\httpsd\conf\user_httpsd.conf`	• `VirtualHost` *host-name*`:`*port-number* • `Listen`[#]

Default port number	Settings files	Location
22031/tcp	*Hitachi-Command-Suite-Common-Component-installation-folder*\uCPSB\httpsd\conf\user_hsso_httpsd.conf	Listen 127.0.0.1:*port-number*
22032/tcp	*Hitachi-Command-Suite-Common-Component-installation-folder*\HDB\CONF\emb\HiRDB.ini	PDNAMEPORT
	Hitachi-Command-Suite-Common-Component-installation-folder\HDB\CONF\pdsys	pd_name_port
	Hitachi-Command-Suite-Common-Component-installation-folder\database\work\def_pdsys	pd_name_port
22035/tcp	*Hitachi-Command-Suite-Common-Component-installation-folder*\uCPSB\CC\web\redirector\workers.properties	worker.HBase64StgMgmtSSOService.port
	Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties	webserver.connector.ajp13.port
22036/tcp	*Hitachi-Command-Suite-Common-Component-installation-folder*\uCPSB\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties	ejbserver.rmi.naming.port
22037/tcp	*Hitachi-Command-Suite-Common-Component-installation-folder*\uCPSB\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties	ejbserver.http.port
22038/tcp	*Hitachi-Command-Suite-Common-Component-installation-folder*\uCPSB\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties	ejbserver.rmi.remote.listener.port

#:

Even when SSL is enabled for accessing HBase 64 Storage Mgmt Web Service, /tcp is used for internal communication. Therefore, you must not delete or comment out the `Listen 22015` line.

4. Start Hitachi File Services Manager and Hitachi Command Suite Common Component.

   For details on how to do this, see Starting and stopping Hitachi File Services Manager on page 7-32.

5. If you stopped services in step 1, start them.

This step is necessary only if Hitachi Command Suite products whose versions are earlier than 8 are installed. For details on how to start the service of a Hitachi Command Suite product, see the documentation for that product.

6. If you change the following port numbers, you need to change the URLs of the management server:

   - 22015/tcp (used for accessing HBase 64 Storage Mgmt Web Service)

     You need to change the URLs if you use non-SSL for communication between the management server and management clients.
   - 22016/tcp (used for accessing SSL HBase 64 Storage Mgmt Web Service)

     You need to change the URLs if you use SSL for communication between the management server and management clients.

   For details on how to change the URLs of the management server, see the Device Manager documentation.

   Note that you might not need to change the URLs depending on the network environment between the management server and management clients, such as an environment that has a firewall configured.

Configuring SSL

To protect communication between the management server and clients using encryption, the system administrator can set up SSL on the management server. HBase 64 Storage Mgmt Web Service uses the public key cryptosystem for encryption.

The following explains the tasks to perform when configuring SSL on the management server and how to disable the SSL setting.

Setting up SSL

When you set up SSL, you need to create a private key and a certificate. You also need to specify in the `user_httpsd.conf` file where they are stored. There are two types of certificates:

- Self-signed certificate

  A certificate signed by the user who issued the certificate. Users can create this type of certificate by themselves. We recommend that self-signed certificates be used only for testing encrypted communication.
- CA-issued certificate

  A certificate signed by the trusted CA. This type of certificate enables improved security over a self-signed certificate.

To set up SSL using a self-signed certificate:

1. On the management server, execute the `hcmds64ssltool` command to create private keys (private keys supporting RSA ciphers and elliptic curve ciphers (ECC)), a certificate signing request (CSR), and a self-signed certificate.

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64ssltool /key private-key-file /csr certificate-signing-request-
file /cert self-signed-certificate-file /certtext contents-of-a-self-
signed-certificate [/validity number-of-valid-days] [/dname DN]
```

- For the `key` option, specify the path to the location to which a private key will be output. The size of a private key is 2,048 bits (fixed). The private key for an RSA cipher is output with the specified file name. The private key for an elliptic curve cipher is output with a file name consisting of the prefix `ecc-` and the specified file name. The size of private key for an elliptic curve cipher is 384 bits.
- For the `csr` option, specify the path to the location to which the certificate signing request will be output. The certificate signing request for an RSA cipher is output with the specified file name. The certificate signing request for an elliptic curve cipher is output with a file name consisting of the prefix `ecc-` and the specified file name.
- For the `cert` option, specify the path to the location to which the self-signed certificate will be output. The self-signed certificate for an RSA cipher is output with the specified file name. The self-signed certificate for an elliptic curve cipher is output with a file name consisting of the prefix `ecc-` and the specified file name.
- For the `certtext` option, specify the path to the location to which the contents of the self-signed certificate will be output in text format. The content of the self-signed certificate for an RSA cipher is output with the specified file name. The content of the self-signed certificate for an elliptic curve cipher is output with a file name consisting of the prefix `ecc-` and the specified file name.
- For the `validity` option, specify the number of days during which the self-signed certificate is valid. If this option is omitted, the valid period is set to 3,650 days.
- For the `dname` option, specify the DN to be included in the self-signed certificate and certificate signing request. If you execute the command without specifying this option, you will be prompted to specify the DN.

  To specify the DN, combine each attribute type with the corresponding attribute value into one attribute by using an equal sign (`=`), and then specify the attributes by separating each by a comma.

  For the DN, you cannot specify a double quotation mark (`"`) or backslash (`\`). In addition, specify each attribute value as defined by RFC2253. For example, if the specified DN includes any of the following characters, escape each of them by using a backslash (`\`).

  A space at the beginning of or at the end of the DN

  A hash mark (`#`) at the beginning of the DN

  A plus sign (`+`), comma (`,`), semicolon (`;`), left angle bracket (`<`), equal sign (`=`), or right angle bracket (`>`)

  The following table lists and describes the attribute types and values specified for the DN.

Table 7-30 Attribute types and values specified for the DN

Attribute type	Full name of attribute type	Attribute value
CN	Common Name	Specify the host name of the management server (HBase 64 Storage Mgmt Web Service). This attribute is required. Specify the host name used when connecting to the management server (HBase 64 Storage Mgmt Web Service of Common Component) from the management client. You can also specify the host name in FQDN format. If the management server is running in a cluster configuration, specify the logical host name.
OU	Organizational Unit Name	Specify the name of the organizational unit.
O	Organization Name	Specify the organizational name. This attribute is required.
L	Locality Name	Specify the name of the city, town, or other locality.
ST	State or Province Name	Specify the name of the state or province.
C	Country Name	Specify the two-letter country code.

Caution: When you execute the `hcmds64ssltool` command, if a file with the same name already exists in the output location, the existing file will be overwritten. Therefore, when you recreate a private key, certificate signing request, or self-signed certificate, we recommend you to output them to a directory other than existing storage directories.

A certificate signing request and self-signed certificate are created with a private key size of 2,048 bits. The certificate signing request is created in PEM format.

Note that SHA256withRSA is the default signature algorithm for the server certificate for the RSA cipher, and SHA384withECDSA is the default signature algorithm for the server certificate for the elliptic curve cipher.

The following is an example of executing commands to create a private key, a certificate signing request, and a self-signed certificate:

- Private key file: `httpsdkey.pem`
- Certificate signing request file: `httpd.csr`
- Self-signed certificate file: `httpsd.pem`
- Contents of a self-signed certificate: `httpsdpem.txt`
- Number of valid days: 365 days
- DN

CN: `hfsm-nagpur`

OU: `Website`

O: `HITACHI`

L: `New York`

ST: `Washington`

C: `US`

```
"C:\Program Files\HiCommand\Base64\bin\hcmds64ssltool " /key C:\temp
\httpsdkey.pem /csr C:\temp\httpsd.csr /cert C:\temp\httpsd.pem /certtext
C:\temp\httpsdpem.txt /validity 365 /dname "CN=hfsm-
nagpur,OU=Website,O=HITACHI,L=New York,ST=Washington,C=US"
```

2. Copy the private key file and certificate file to an appropriate folder.

   We recommend that you copy them to the following folder:

   Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB/httpsd\conf\ssl\server

3. Edit the `user_httpsd.conf` file. Specify information such as the paths to the private key and the server certificate in each directive of the `user_httpsd.conf` file, and then delete the hash mark (#) at the beginning of the line.

   The `user_httpsd.conf` file is located in the following folder:

   Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB/httpsd\conf\

   The following is an example of the `user_httpsd.conf` file format (default).

```
ServerName host-name-of-management-server
Listen 22015                    ← Port number for non-SSL communication
Listen [::]:22015               ← Port number for non-SSL communication
#Listen 127.0.0.1:22015           (for IPv6 environment)
SSLDisable
#Listen 22016                   ← Port number for SSL communication
#Listen [::]:22016              ← Port number for SSL communication (for IPv6 environment)
#<VirtualHost *:22016>          ← Port number for SSL communication
#  ServerName host-name-of-management-server
#  SSLEnable
#  SSLProtocol TLSv12
#  SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-
SHA:ECDHE-ECDSA-AES128-SHA:AES256-SHA256:AES256-SHA:AES128-SHA256:AES128-SHA
#  SSLRequireSSL
#  SSLCertificateKeyFile "Hitachi-Command-Suite-Common-Component-installation-
folder/uCPSB/httpsd/conf/ssl/server/httpsdkey.pem"
#  SSLCertificateFile "Hitachi-Command-Suite-Common-Component-installation-
folder/uCPSB/httpsd/conf/ssl/server/httpsd.pem"
#  SSLECCCertificateKeyFile "Hitachi-Command-Suite-Common-Component-
installation-folder/uCPSB/httpsd/conf/ssl/server/ecc-httpsdkey.pem"
#  SSLECCCertificateFile "Hitachi-Command-Suite-Common-Component-installation-
folder/uCPSB/httpsd/conf/ssl/server/ecc-httpsd.pem"
#  SSLCACertificateFile "Hitachi-Command-Suite-Common-Component-installation-
folder/uCPSB/httpsd/conf/ssl/cacert/anycert.pem"
#</VirtualHost>
#HWSLogSSLVerbose On
```

- For the ServerName directives in the following locations, specify the host name that you specified for Common Name in the certificate signing request. Note that host names are case sensitive.

  - ServerName at the beginning of the user_httpsd.conf file

  - ServerName enclosed by <VirtualHost> and </VirtualHost>

- If you are using an IPv6 environment, remove the hash mark (#) at the beginning of the lines #Listen [::]:22015 and #Listen [::]:22016.

- For <VirtualHost>, usually specify an asterisk (*), although you can also specify a host name.

- For operation in advanced security mode, add the SSLProtocol and SSLRequiredCiphers directives to limit the cipher strength.

  Note that when using TLS v1.1 or TLS v1.2 for communication, also specify the protocol, encryption algorithm, and hash algorithm for the directives above. Also, edit the security settings of the browser for the machine used to access management servers such as management consoles. To edit the settings, in **Tools** in Internet Explorer, select **Internet Options**, and in the **Advanced** tab, edit the settings so that TLS 1.1 and TLS 1.2 can be used. The following shows what you can also specify for the SSLProtocol and SSLRequiredCiphers directives.

Table 7-31 Information that can also be specified for the SSLProtocol and SSLRequiredCiphers directives

Target directive	Information to be specified
SSLProtocol	Specify the protocol to be used. TLSv11 Specify this when using TLS v1.1. TLSv12 Specify this when using TLS v1.2.
SSLRequiredCiphers	Specify the encryption algorithm and hash algorithm to be used. AES256-SHA256 Specify this when using AES256 as the encryption algorithm and SHA256 as the hash algorithm. AES128-SHA256 Specify this when using AES128 as the encryption algorithm and SHA256 as the hash algorithm.

The following is an example of the specifications after the additional information was specified:

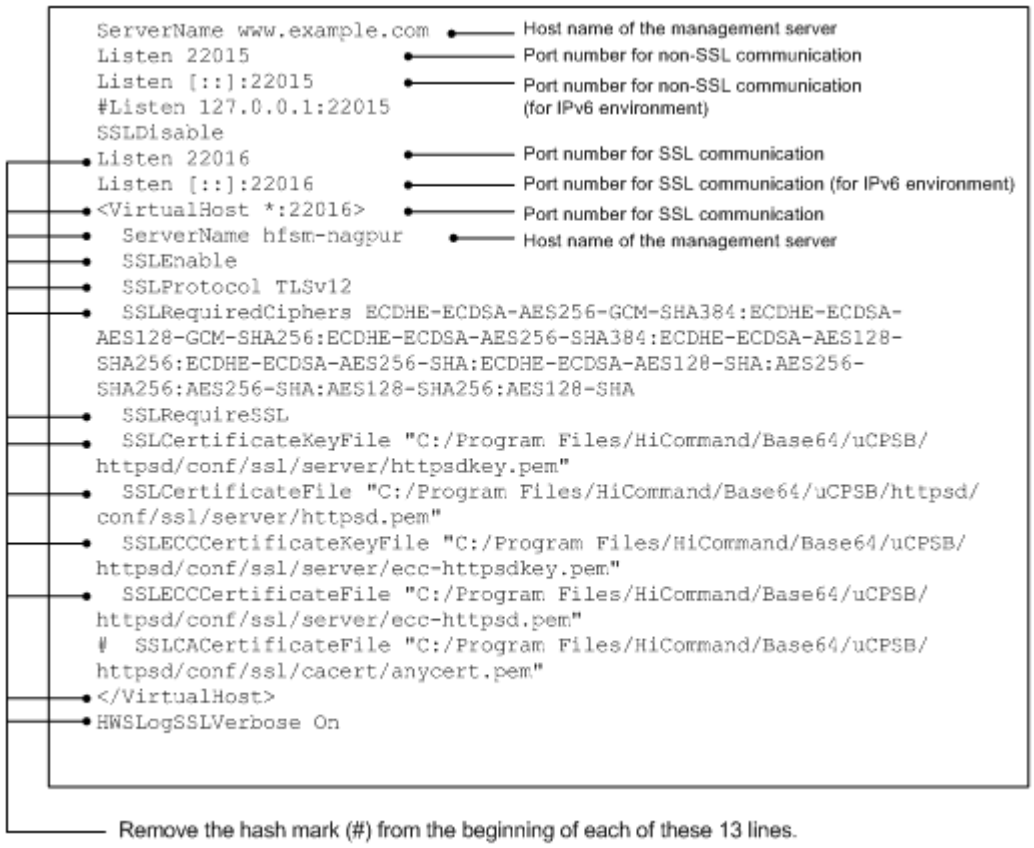
```
SSLProtocol TLSv1 TLSv11 TLSv12
SSLRequiredCiphers AES256-SHA:AES128-SHA:DES-CBC3-SHA:AES256-
SHA256:AES128-SHA256
```

- For the `SSLCertificateKeyFile` directive, specify the absolute path to the private key file for Common Component.

  Do not specify a symbolic link and junction for the path.
- For the `SSLCertificateFile` directive, specify the absolute path to the signed server certificate sent back from the certificate authority or the absolute path to the self-signed certificate file.
- For the `SSLECCCertificateKeyFile` directive, specify the absolute path to the private key file for the Common Component instance for the elliptic curve cipher. This setting is unnecessary if you use the RSA cipher only.
- For the `SSLECCCertificateFile` directive, specify the absolute path of the server certificate for the Common Component instance for the elliptic curve cipher. This setting is unnecessary if you use the RSA cipher only.
- For the `SSLCACertificateFile` directive, if you use a server certificate issued by a certificate authority, specify the absolute path to the server certificate. Multiple server certificates can be contained in one file by chaining multiple PEM format server certificates by using a text editor. Note that you must not specify a symbolic link or junction for the path.

Caution: The non-SSL port (default: 22015) is used for communication within Device Manager even if SSL is enabled. Do not delete or comment out the line `Listen 22015` (this line is for when the default port is used) because the line is the setting for the non-SSL port.

The following shows an example of specifying settings in the `user_httpsd.conf` file. The lines beginning with a hash mark (`#`) are comment lines.



4. Change the URL of the management server.

   This step is necessary if both Hitachi File Services Manager and Device Manager are installed on the same management server. For details about how to change the URL of the management server, see the applicable Device Manager manual.

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

   For details on how to do this, see Starting and stopping Hitachi File Services Manager on page 7-32.

Disabling the SSL settings

To disable SSL:

1. In the `user_httpsd.conf` file, add a hash mark (`#`) to the beginning of each SSL directive showing information such as paths to the private key and the server certificate, so that they are commented out.

   Edit the `user_httpsd.conf` file to disable SSL.

   The `user_httpsd.conf` file is located in the following folder:

   `Hitachi-Command-Suite-Common-Component-installation-folder``\uCPSB\httpsd\conf\`

   To disable SSL, see the example format of the user_httpsd.conf file (default) in Setting up SSL on page 7-92. Then, add a hash mark (#) to the beginning of each SSL directive from `Listen 22016` to

`HWSLogSSLVerbose On`, so that those directives will be treated as comment lines.

2. Change the URL of the management server.

   This step is necessary if both Hitachi File Services Manager and Device Manager are installed on the same management server. For details about how to change the URL of the management server, see the applicable Device Manager manual.

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

   For details on how to do this, see Starting and stopping Hitachi File Services Manager on page 7-32.

Acquiring a CA-issued certificate

To acquire a CA-issued certificate, you need to create and send a certificate signing request (CSR) to the CA, and then receive a signed certificate from the CA. You use the signed certificate received from CA to set SSL. For details on how to create a CSR and how to use a certificate, see Setting up SSL on page 7-92.

To acquire a CA-issued certificate:

1. Send the created certificate signing request (CSR) to a certificate authority (CA).
2. Receive the certificate from the CA.

Changing the port number assigned for SSL

The default port number assigned for SSL is `22016`.

For details on how to change the default SSL port number (22016), see Changing the port numbers used by Hitachi Command Suite Common Component on page 7-90.

Importing the required SSL certificate for communication between the node and management server

The system administrator must import the SSL certificate to the management server because communication between the management server and a node is performed using SSL.

Normally, the SSL certificate is imported automatically during installation of Hitachi File Services Manager. However, if a password has been set for the management server keystore file (`jssecacerts`), you must manually import the SSL certificate after installing Hitachi File Services Manager.

To manually import the SSL certificate to the management server:

1. Execute the following command to check whether the SSL certificate has been imported to the management server:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64keytool -list -alias hfsm2 -keystore Hitachi-Command-Suite-Common-
Component-installation-folder\uCPSB\jdk\jre\lib\security\jssecacerts
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64keytool -list -alias hfsm -keystore Hitachi-Command-Suite-Common-
Component-installation-folder\uCPSB\jdk\jre\lib\security\jssecacerts
```

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

If the specified aliases (`hfsm2` and `hfsm`) do not exist, proceed to the next step.

If information for the certificate is displayed, the certificate has already been imported. The following steps are unnecessary.

2. Execute the following command to import the SSL certificate to the management server:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64keytool -import -trustcacerts -alias hfsm2 -file Hitachi-File-
Services-Manager-installation-folder\cert\cacert3.cer -keystore Hitachi-
Command-Suite-Common-Component-installation-folder\uCPSB\jdk\jre\lib
\security\jssecacerts
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64keytool -import -trustcacerts -alias hfsm -file Hitachi-File-
Services-Manager-installation-folder\cert\cacert2.cer -keystore Hitachi-
Command-Suite-Common-Component-installation-folder\uCPSB\jdk\jre\lib
\security\jssecacerts
```

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

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

   For details on how to do this, see Starting and stopping Hitachi File Services Manager on page 7-32.

Configuring the warning banner

As one security solutions, the system administrator can enable an optional message (warning banner) to be displayed in the Login window of Hitachi File Services Manager. Issuing a warning beforehand to third parties that might attempt unauthorized accesses can help reduce the risk of problems such as data corruption or information leakage.

If you register the same message in different languages, the message can be switched automatically to suit the locale of the Web browser on the management console.

You can use one of the following methods to register a warning banner:

- Using commands
- Using the GUI

This section describes how to use commands to register and remove messages.

Creating a message file

In a message file, in addition to the text of the message, you can use HTML tags to change font attributes, or to place line breaks in desired locations.

Unicode (UTF-8) characters can be used. A message can contain no more than 1,000 characters, including HTML tags (line breaks are also counted in the number of characters). To display a character used in HTML tags, such as a left angle bracket (<), right angle bracket (>), ampersand (&), single quotation mark (') or double quotation mark ("), use the HTML escape sequence. For example, to display an ampersand (&) in a message, write & in the message file.

The following shows an example of a message:

```
<center><b>Warning Notice!</b></center>
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. <br>
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.
```

Note that when you register a message, Hitachi File Services Manager does not check or correct the HTML syntax. Therefore you must make sure that you use valid HTML syntax when you edit message files. If there is a problem with HTML syntax in a message, the message might not be displayed in the Login window correctly.

Reference note:

Sample message files in English (bannermsg.txt) and Japanese (bannermsg_ja.txt) are stored in the following folder on the management server:

Hitachi-Command-Suite-Common-Component-installation-folder\sample\resource\

These sample files are overwritten whenever Hitachi Command Suite Common Component is installed. If you want to use sample files, first copy them to another folder.

Registering a message

Use the hcmds64banner command to register the message you created. If Hitachi Command Suite products that support the warning banner function have been installed on the management server, the registered message is also displayed in the Login window of those products.

To register a message, you need to log in with an account that has Administrator permissions.

To register a message:

1. Execute the following command to register a message:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64banner /add /file file-name [/locale locale-name]
```

file-name

Specify the absolute path of the message file. The following characters can be used: alphanumeric characters, spaces, exclamation marks (!), hash marks (#), left parentheses (( ), right parentheses ( )), plus signs (+), hyphens (-), periods (.), equal signs (=), at marks (@), left square bracket ([), right square bracket (]), caret (^), underscores (_), left curly bracket ({), right curly bracket (}), and tildes (~). You can use forward slashes (/), colons (:), and backslashes (\) as path delimiters.

`/locale` *locale-name*

Specify the locale for the language used in the message. For example, specify `en` for English, or `ja` for Japanese. If a message has already been registered with the specified locale, the message will be updated.

If you want to be able to use the GUI to later edit the message, omit this option.

Deleting a message

You can use the `hcmds64banner` command to delete the registered message. To delete a message, you need to log in with an account that has Administrator permissions.

To delete a message:

1. Execute the following command to delete a message:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64banner /delete [/locale locale-name]
```

`/locale` *locale-name*

Specify the locale for the language used in the message. For example, specify `en` for English, or `ja` for Japanese.

If you omit this option, the message that was registered by executing the `hcmds64banner` command without the `/locale` option is deleted.

Acquiring and checking the Hitachi File Services Manager audit logs

By editing the environment settings file (`auditlog.conf`) of Hitachi Command Suite Common Component, the system administrator can specify for user operation information related to Hitachi File Services Manager to be output as audit logs. If the system administrator specifies this setting, Hitachi File Services Manager audit logs are output to the Windows event log files (application log files).

A severity level is specified for each audit event. You can filter audit log data to be output according to the severity levels of events.

The following table lists the categories of audit logs that can be output by Hitachi File Services Manager.

Table 7-32 Categories of audit logs that can be output by Hitachi File Services Manager

Categories	Description
`Authentication`	Events indicating whether an administrator or end user succeeded in an attempt to be authenticated.

If you specify `Authentication` in the `auditlog.conf` file, the following audit events are output as Hitachi File Services Manager audit log data.

Table 7-33 Audit events that are output as Hitachi File Services Manager audit log data

Type description	Audit event	Severity	Message ID
Administrator or end user authentication	Successful login	6	KAPM01124-I
	Successful login (to the external authentication server)	6	KAPM02450-I
	Failed login	6	KAPM01081-E
	Failed login (no permission)	6	KAPM01095-E
	Failed login (wrong user ID or password)	4	KAPM02291-W
	Failed login (logged in as a locked user)	4	KAPM02291-W
	Failed login (logged in as a non-existing user)	4	KAPM02291-W
	Failed login (authentication failure)	4	KAPM01125-E
	Failed login (to the external authentication server)	4	KAPM02451-W
Automatic account lock	Automatic account lock (repeated authentication failure or expiration of account)	4	KAPM02292-W

For details about the information output as Hitachi File Services Manager audit log data, see Checking Hitachi File Services Manager audit log data on page 7-105.

Settings to acquire the Hitachi File Services Manager audit logs

Follow the procedure below to specify the settings to acquire the Hitachi File Services Manager audit logs.

1. Stop the services of the Hitachi Command Suite products whose versions are earlier than 8.

   This step is necessary only if Hitachi Command Suite products whose versions are earlier than 8 are installed. For details on how to stop the service of a Hitachi Command Suite product, see the documentation for that product.

2. Stop Hitachi File Services Manager and Hitachi Command Suite Common Component.

   For details on how to do this, see Starting and stopping Hitachi File Services Manager on page 7-32.

3. Edit the settings in the `auditlog.conf` file so that user operation information is output as Hitachi File Services Manager audit log data.

   The `auditlog.conf` file is stored in the following location:

   Hitachi-Command-Suite-Common-Component-installation-folder`\conf\sec\auditlog.conf`

   The following table shows the items to set in the `auditlog.conf` file.

Table 7-34 Items to set in the auditlog.conf file

Item	Description
`Log.Event.Category`	Specify the audit event categories to be generated. If `Log.Event.Category` is not specified, audit log data is not output. For information about the available categories, see Table 7-32 Categories of audit logs that can be output by Hitachi File Services Manager on page 7-103. `Log.Event.Category` is not case-sensitive. If an invalid category name is specified, the settings in the `auditlog.conf` file is ignored. Default value: (not specified)
`Log.Level`	Specify the severity level of audit events to be generated. Events with the specified severity level or lower will be output to the event log file. For details about the audit events to be output as Hitachi File Services Manager audit log data and the severity levels of audit events, see Table 7-33 Audit events that are output as Hitachi File Services Manager audit log data on page 7-103. For details about the correspondence between the severity levels of audit events and the types of event log data, see Table 7-35 Correspondence between the severity levels of audit events and the types of event log data on page 7-104. Specify one of the following numeric characters. Do not specify anything other than a numeric character from 0 to 7. Note that if a non-numeric character is specified, processing will be conducted as if the default value was specified. • Specifiable values: 0 to 7 (severity level) • Default value: 6

The table below shows the correspondence between the severity levels of audit events and the types of event log data.

Table 7-35 Correspondence between the severity levels of audit events and the types of event log data

Severity of audit events	Type of event log data
0	Error
1	

Severity of audit events	Type of event log data
2	
3	
4	Warning
5	Information
6	
7	

The following example shows how to configure the `auditlog.conf` file:

```
Log.Event.Category Authentication
Log.Level 6
```

In this example, the audit events in the `Authentication` audit log category that have a severity level in the range from 0 to 6 are output.

4. Start Hitachi File Services Manager and Hitachi Command Suite Common Component.

   For details on how to do this, see Starting and stopping Hitachi File Services Manager on page 7-32.

5. If you stopped services in step 1, start them.

   This step is necessary only if Hitachi Command Suite products whose versions are earlier than 8 are installed. For details on how to start the service of a Hitachi Command Suite product, see the documentation for that product.

Checking Hitachi File Services Manager audit log data

Hitachi File Services Manager audit log data is output to the event logs in the **General** tab of the **Event Properties** display that appears when you open an event by selecting **Event Viewer**, **Windows Logs**, and then **Application** on the management server.

Audit log data is output to the Windows event log in the following format:

```
program-name [process-ID]: message-portion
```

The format and contents of *message-portion* are described below.

Note: In *message-portion*, a maximum of 953 single-byte characters can be displayed.

The format of *message-portion* is as follows:

```
uniform-identifier,unified-specification-revision-number,serial-number,message-ID,date-and-time,detected-entity,detected-location,audit-event-type,audit-event-result,audit-event-result-subject-identification-information,hardware-identification-information,location-information,location-identification-information,FQDN,redundancy-identification-information,agent-
```

```
information,request-source-host,request-source-port-number,request-destination-
host,request-destination-port-number,batch-operation-identifier,log-data-type-
information,application-identification-information,reserved-area,message-text
```

Table 7-36 Information in message-portion

Item#	Description
uniform-identifier	Fixed to `CELFSS`.
unified-specification-revision-number	Fixed to `1.1`.
serial-number	Serial number of audit log messages.
message-ID	Message ID. For details, see Table 7-33 Audit events that are output as Hitachi File Services Manager audit log data on page 7-103.
date-and-time	The date and time when the message was output. This item is output in the format of *yyyy-mmddThh*:*mm*:*ss.s time-zone*.
detected-entity	Component or process name.
detected-location	Host name.
audit-event-type	Event type.
audit-event-result	Event result.
audit-event-result-subject-identification-information	Account ID, process ID, or IP address corresponding to the event.
hardware-identification-information	Hardware model or serial number.
location-information	Identification information for the hardware component.
location-identification-information	Location identification information.
FQDN	Fully qualified domain name.
redundancy-identification-information	Redundancy identification information.
agent-information	Agent information.
request-source-host	Host name of the request sender.
request-source-port-number	Port number of the request sender.
request-destination-host	Host name of the request destination.
request-destination-port-number	Port number of the request destination.
batch-operation-identifier	Serial number of operations through the program.
log-data-type-information	Fixed to `BasicLog` or `DetailLog`.
application-identification-information	Program identification information.

Item#	Description
reserved-area	Not output. This is a reserved space.
message-text	The contents vary according to the audit events. Characters that cannot be displayed are output as asterisks (*).

#:

Some items are not output for some audit events.

The following is an example of part of the message that is output for a `Successful login` audit event:

```
CELFSS,1.1,2,KAPM01124-I,2014-02-06T20:18:42.9+09:00,HBase-SSO,management-
host,Authentication,Success,uid=system,,,,,,,,,,,BasicLog,,,"The login
process has completed properly."
```

Maintenance of the management server

This section describes how to execute a command of Hitachi Command Suite Common Component to manage the management server.

If one of the following products is installed, perform the procedure according to the product manual of the relevant version:

- V6.1.2 or earlier of Hitachi File Services Manager
- V7.6.1 or earlier of a Hitachi Command Suite product

Backing up or restoring the database of the management server

This subsection describes how to back up and restore the database of Hitachi File Services Manager or a Hitachi Command Suite product.

We recommend that you back up the databases of Hitachi File Services Manager and Hitachi Command Suite products periodically.

Note that you must back up the databases beforehand when performing the following operations:

- Performing an upgrade installation or overwrite installation of Hitachi File Services Manager
- Installing a Hitachi Command Suite product on the management server
- Uninstalling a Hitachi Command Suite product from the management server
- Installing Hitachi File Services Manager on the management server where Hitachi Command Suite products are already installed
- Uninstalling Hitachi File Services Manager from the management server where Hitachi Command Suite products are already installed

Backing up the database

The system administrator can back up the databases of Hitachi File Services Manager and Hitachi Command Suite products by using commands.

To back up the Hitachi File Services Manager database, a folder that will contain the backup files is required. The folder requires the following amount of free space, which includes the space for temporary files created by the backup command:

Required free space:

sum-of-the-database-sizes-for-the-target-Hitachi-Command-Suite-products **x** 2 + 5 MB

The following data is backed up:

- Information about the managed cluster
- Current Hitachi File Services Manager version information
- Management information for Hitachi File Services Manager and Hitachi Command Suite products

Note that the system administrator's account information and the property file (`user.properties`) are not backed up or restored. Therefore, when you back up the data of the management server, also save the system administrator's account information and the property file (`user.properties`).

To back up the databases of Hitachi File Services Manager and Hitachi Command Suite products

1. Stop the Tuning Manager service connected to the Device Manager on the management server.

   This step is necessary if Hitachi Command Suite products including Device Manager have been installed on the management server, and Tuning Manager connected to that Device Manager has been installed on another computer. Stop the Tuning Manager service from the computer where Tuning Manager has been installed. For details about how to stop the Tuning Manager service, see the manual for the installed version of Tuning Manager.
2. Execute a command as follows to stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
   stop
   ```
3. Execute a command as follows to start HiRDB:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64dbsrv /start
   ```
4. Execute a command as follows to back up the databases:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64backups /dir backup-target-folder [/auto]
   ```

   The following explains the command options:

`/dir`

Specify *backup-target-folder* (the folder on the local disk for storing the backup file of the Hitachi File Services Manager database) by absolute path. If specifying an existing folder, make sure that it is empty.

You can use alphanumeric characters, spaces, exclamation marks (`!`), hash marks (`#`), left parentheses (`(`), right parentheses (`)`), plus signs (`+`), hyphens (`-`), periods (`.`), equal signs (`=`), at marks (`@`), left square brackets (`[`), right square brackets (`]`), carets (`^`), underscores (`_`), left curly brackets (`{`), right curly brackets (`}`), and tildes (`~`). As a path delimiter, you can use a forward slash (`/`), colon (`:`), or backslash (`\`).

When you execute the `hcmds64backups` command, a folder named `database` is created in the backup target folder and the database backup file is saved with the file name `backup.hdb`.

`/auto`

This option automatically starts and stops services of Hitachi Command Suite products.

Even if you specify the `/auto` option, if Tuning Manager connected to Device Manager is installed on a computer other than the one where the Device Manager is installed, the Tuning Manager service will not be automatically started or stopped.

5. If you stopped Hitachi File Services Manager and Hitachi Command Suite Common Component in step 2, execute the following command to restart them:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
start
```

6. If you stopped the Tuning Manager service in step 1, restart the service.

This step is necessary if Hitachi Command Suite products including Device Manager have been installed on the management server, and Tuning Manager connected to that Device Manager has been installed on another computer. Start the Tuning Manager service on the computer where Tuning Manager has been installed.

Restoring the database

The system administrator can restore the backed up database of Hitachi File Services Manager using commands. The databases of installed Hitachi Command Suite products can be restored at the same time as a batch operation, but first make sure that returning to the state at which the Hitachi Command Suite products were backed up will not cause any problems.

Note: Make sure that you restore the databases of Hitachi File Services Manager and Hitachi Command Suite products together as a batch operation if you are uninstalling and then re-installing Hitachi File Services Manager and Hitachi Command Suite products on the management server.

The following must be identical on the management server where the databases were backed up and on the management server to which the databases are being restored:

- Type, version, and revision of the installed Hitachi File Services Manager and Hitachi Command Suite products
- Installation folders of Hitachi File Services Manager, Hitachi Command Suite products, and Hitachi Command Suite Common Component
- Folders in which the databases of Hitachi File Services Manager, Hitachi Command Suite products, and Hitachi Command Suite Common Component were created
- IP address and the host name

Also, when you execute the `hcmds64db` command to restore the Hitachi File Services Manager database, temporary files are created in the folder in which the backup files exist. Make sure that you have write privilege for that folder and the following amount of free space exists.

Required free space:

sum-of-the-database-sizes-for-the-target-Hitachi-Command-Suite-products + 5 MB

To restore the database of Hitachi File Services Manager

1. Stop the Tuning Manager service connected to the Device Manager on the management server.

   This step is necessary if Hitachi Command Suite products including Device Manager have been installed on the management server, and Tuning Manager connected to that Device Manager has been installed on another computer. Stop the Tuning Manager service from the computer where Tuning Manager has been installed. For details about how to stop the Tuning Manager service, see the manual for the installed version of Tuning Manager.

2. Execute a command as follows to stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
   stop
   ```

3. Execute a command as follows to restore the databases:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64db /
   restore backup-file-name /type {FileServicesManager|ALL} [/auto]
   ```

   The following explains the command options:

   `/restore`

   Specify *backup-file-name* (the name of the backup file to be restored) by absolute path.

   `/type`

   To restore only the database of Hitachi File Services Manager, specify `FileServicesManager`.

To restore the databases of Hitachi File Services Manager and Hitachi Command Suite products installed on the management server, specify `ALL`.

`/auto`

This option automatically starts and stops services of Hitachi Command Suite products.

Even if you specify the `/auto` option, if Tuning Manager connected to Device Manager is installed on a computer other than the one where the Device Manager is installed, the Tuning Manager service will not be automatically started or stopped.

4. Execute a command as follows to start Hitachi File Services Manager and Hitachi Command Suite Common Component:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
start
```

5. If you stopped the Tuning Manager service in step 1, restart the service.

   This step is necessary if Hitachi Command Suite products including Device Manager have been installed on the management server, and Tuning Manager connected to that Device Manager has been installed on another computer. Start the Tuning Manager service on the computer where Tuning Manager has been installed.

Migrating the management server from a non-cluster configuration into a cluster configuration

This subsection describes the procedure for migrating the management server from a non-cluster configuration into a cluster configuration.

Each step assumes that the management server, which has already been started in a non-cluster configuration, will be migrated into a cluster configuration under the following prerequisites:

- Set the management server, which has already been started in a non-cluster configuration, as an executing node.
- The Hitachi Command Suite products installed on the executing node are also installed on the standby node, and licenses have been set up.

Migrating to cluster configurations prerequisites

Before migrating the management server into a cluster configuration, check the following:

- The executing node and the standby node satisfy the machine requirements.

  For details about the machine requirements of the management server, see Requirements for a management server on page 3-5.
- All software programs required for the cluster configuration are installed on the executing node and the standby node.

For the software programs required for the management server cluster configuration, see Management server cluster configuration on page 3-7.

- The shared disk is enabled on the executing node.
  For details about how to enable the shared disk, see Performing a new installation of Hitachi File Services Manager (if the management server is running in a cluster configuration) on page 7-16.
- For the executing node, the standby node, and the cluster management IP address, the IP address can be resolved from the host name.
- The version of Hitachi File Services Manager to be installed on the standby node is the same as the version on the executing node.

While performing a cluster configuration, do not access Hitachi File Services Manager.

Complete the management server settings on the executing node first, and then perform the settings on the standby node.

Settings on the executing node of the management server

The following describes the procedure to specify the settings on the executing node when you migrate the management server from a non-cluster configuration into a cluster configuration.

To specify the settings on the executing node of the management server

1. Back up the database.
   For details about how to back up the database, see Backing up or restoring the database of the management server on page 7-107.
2. Use a text editor to create a cluster-configuration file.
   Specify the following items in the cluster-configuration file:
   - `mode`
     Specify `online`.
   - `virtualhost`
     Specify the logical host name.
   - `onlinehost`
     Specify the host name of the executing node.
   - `standbyhost`
     Specify the host name of the standby node.

   You cannot specify an IP address for `virtualhost`, `onlinehost`, and `standbyhost`.
   The following shows a coding example in the cluster-configuration file:

```
mode = online
virtualhost = hicommand_cluster
onlinehost = hicommand_1
standbyhost = hicommand_2
```

3. Save the created cluster-configuration file using the name `cluster.conf` in the following location:

   Hitachi-Command-Suite-Common-Component-installation-folder`\conf\`

4. Stop the Tuning Manager service connected to the Device Manager on the management server.

   This step is necessary if Hitachi Command Suite products including Device Manager have been installed on the management server, and Tuning Manager connected to that Device Manager has been installed on another computer. Stop the Tuning Manager service from the computer where Tuning Manager has been installed. For details about how to stop the Tuning Manager service, see the manual for the installed version of Tuning Manager.

5. Execute a command as follows to stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
   stop
   ```

6. Execute a command as follows to start HiRDB:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64dbsrv /start
   ```

7. Execute a command as follows to migrate the database to a shared disk:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64dbclustersetup /createcluster /databasepath database-re-creation-
   destination-folder /exportpath data-storage-destination-folder [/auto]
   ```

   Specify command arguments under the following conditions:

   - Specify the folders by absolute path. Enter no more than 63 bytes for *database-re-creation-destination-folder* and no more than 63 bytes for *data-storage-destination-folder*.
   - Specify a location on the shared disk for *database-re-creation-destination-folder*.
   - Specify a location on the local disk for *data-storage-destination-folder*.
   - If specifying an existing folder for *data-storage-destination-folder*, make sure that it is empty.
   - For *database-re-creation-destination-folder* and *data-storage-destination-folder*, the following characters can be used: alphanumeric characters, left parentheses (`(`), right parentheses (`)`), periods (`.`), underscores (`_`), and spaces. Note that the character string cannot start or end with a period (`.`) or a space. In addition, you cannot specify two or more consecutive spaces.
   - For *database-re-creation-destination-folder* and *data-storage-destination-folder*, a backslash (`\`) can be used as a path delimiter. However, the character string cannot end with a backslash (`\`).

   The space required for *database-re-creation-destination-folder* can be calculated as follows:

required-space = 2.1 GB + *database-capacity-for-other-Hitachi-Command-Suite-products*

If the `hcmds64dbclustersetup` command execution fails because there is not enough space for *database-re-creation-destination-folder*, increase the space for the folder, and then re-execute the command.

Do not disconnect the shared disk from the executing node until the command execution ends normally.

If the command execution ends abnormally and then you restart the server, the connection target of the shared disk might be changed to the standby node.

Executing the `hcmds64dbclustersetup` command resets the port number used by HiRDB to the default (`22032`). If you omit the `/auto` option, Hitachi File Services Manager and Hitachi Command Suite Common Component restart after the command is executed.

Even if you specify the `/auto` option, if Tuning Manager connected to Device Manager is installed on a computer other than the one where the Device Manager is installed, the Tuning Manager service will not be automatically started or stopped.

8. If HiRDB uses a port number other than the default value (`22032`) when performing operations, reset the port number to the desired value.

   For details about how to change the port number used by HiRDB, see Changing the port numbers used by Hitachi Command Suite Common Component on page 7-90.

9. Execute a command as follows to stop Hitachi File Services Manager and Hitachi Command Suite Common Component if active:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /stop
   ```

10. From the Services window in Windows, open the following properties, and then change the settings of **Startup Type** from **Automatic** to **Manual**:

    - **Hitachi Command Suite product services**
    - **HiRDB/ClusterService _HD1**
    - **HBase 64 Storage Mgmt SSO Service**
    - **HBase 64 Storage Mgmt Web SSO Service**
    - **HBase 64 Storage Mgmt Web Service**
    - **HFSM Web Service**

11. In Failover Cluster Management, add the following resources to the group in which the resources to be used by Hitachi File Services Manager are registered:

    - **Hitachi Command Suite product services**
    - **HiRDB/ClusterService _HD1**
    - **HBase 64 Storage Mgmt SSO Service**
    - **HBase 64 Storage Mgmt Web SSO Service**
    - **HBase 64 Storage Mgmt Web Service**

- **HFSM Web Service**

To add HiRDB/ClusterService _HD1, HBase 64 Storage Mgmt SSO Service, HBase 64 Storage Mgmt Web SSO Service, HBase 64 Storage Mgmt Web Service, and HFSM Web Service, select **New**, and then **Resource**, specify the information shown below in dialog boxes, and then click **Finish**.

For details about how to add a Hitachi Command Suite product service, see the relevant product manual.

Table 7-37 HiRDB/ClusterService _HD1 property settings

Tab name	Setting
General	**Startup parameters** or **Startup type**: Specify nothing. If a value is specified, delete the value.
Dependencies	Register the shared disk and client access point.
Advanced Policies	**Possible Owners**: Verify that the active and standby nodes are added.
Policies	Specify nothing.
Registry Replication	Specify nothing.

Table 7-38 HBase 64 Storage Mgmt SSO Service property settings

Tab name	Setting
General	**Startup parameters** or **Startup type**: Specify nothing. If a value is specified, delete the value.
Dependencies	Register HiRDB/ClusterService _HD1.
Advanced Policies	**Possible Owners**: Verify that the active and standby nodes are added.
Policies	Specify nothing.
Registry Replication	Specify nothing.

Table 7-39 HBase 64 Storage Mgmt Web SSO Service property settings

Tab name	Setting
General	**Startup parameters** or **Startup type**: Specify nothing. If a value is specified, delete the value.
Dependencies	Register HBase 64 Storage Mgmt Web Service.
Advanced Policies	**Possible Owners**: Verify that the active and standby nodes are added.
Policies	Specify nothing.
Registry Replication	Specify nothing.

Table 7-40 HBase 64 Storage Mgmt Web Service property settings

Tab name	Setting
General	**Startup parameters** or **Startup type**: Specify nothing. If a value is specified, delete the value.
Dependencies	Register HBase 64 Storage Mgmt SSO Service.
Advanced Policies	**Possible Owners**: Verify that the active and standby nodes are added.
Policies	Specify nothing.
Registry Replication	Specify nothing.

Table 7-41 HFSM Web Service property settings

Tab name	Setting
General	**Startup parameters** or **Startup type**: Specify nothing. If a value is specified, delete the value.
Dependencies	Register HBase 64 Storage Mgmt Web SSO Service.
Advanced Policies	**Possible Owners**: Verify that the active and standby nodes are added.
Policies	Specify nothing.
Registry Replication	Specify nothing.

Settings on the standby node of the management server

To specify the settings on the standby node when you migrate the management server from a non-cluster configuration into a cluster configuration

1. On the standby node, perform a new installation of Hitachi File Services Manager. The version must be the same as the version of Hitachi File Services Manager on the executing node.

   For details about how to install Hitachi File Services Manager for the first time, see Performing a new installation of Hitachi File Services Manager on page 7-2. When performing an installation, use the default values for the folders that store the database of Hitachi Command Suite Common Component and the management server.
2. Stop the Tuning Manager service connected to the Device Manager on the management server.

   This step is necessary if Hitachi Command Suite products including Device Manager have been installed on the management server, and Tuning Manager connected to that Device Manager has been installed on another computer. Stop the Tuning Manager service from the computer where Tuning Manager has been installed. For details about how to stop the Tuning Manager service, see the manual for the installed version of Tuning Manager.

3. Execute a command as follows to stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
stop
```

4. Execute a command as follows to start HiRDB:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbsrv /start
```

5. Use a text editor to create a cluster-configuration file.
   Specify the following items in the cluster-configuration file:

   - `mode`
     Specify `standby`.
   - `virtualhost`
     Specify the logical host name.
   - `onlinehost`
     Specify the host name of the executing node.
   - `standbyhost`
     Specify the host name of the standby node.

   You cannot specify an IP address for `virtualhost`, `onlinehost`, and `standbyhost`.
   The following shows a coding example in the cluster-configuration file:

```
mode = standby
virtualhost = hicommand_cluster
onlinehost = hicommand_1
standbyhost = hicommand_2
```

6. Save the created cluster-configuration file using the name `cluster.conf` in the following location:
   Hitachi-Command-Suite-Common-Component-installation-folder`\conf\`
7. Execute a command as follows to specify the settings so that the database on the shared disk is to be used:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbclustersetup /createcluster /databasepath database-re-creation-
destination-folder /exportpath data-storage-destination-folder [/auto]
```

   Specify the command arguments according to the following rules:

   - For *database-re-creation-destination-folder*, specify the same folder as the executing node.
   - For *data-storage-destination-folder*, specify the absolute path in no more than 63 bytes.
   - Specify a location on the local disk for *data-storage-destination-folder*.
   - If specifying an existing folder for *data-storage-destination-folder*, make sure that it is empty.

- For *data-storage-destination-folder*, the following characters can be used: alphanumeric characters, left parentheses (`(`), right parentheses (`)`), periods (`.`), underscores (`_`), and spaces. Note that the character string cannot start or end with a period (`.`) or a space. In addition, you cannot specify two or more consecutive spaces.
- For *data-storage-destination-folder*, a backslash (`\`) can be used as a path delimiter. However, the character string cannot end with a backslash (`\`).

Do not disconnect the shared disk from the executing node until the `hcmds64dbclustersetup` command execution ends normally.

If the command execution ends abnormally, do not restart the server.

Executing the `hcmds64dbclustersetup` command resets the port number used by HiRDB to the default (`22032`). If you omit the `/auto` option, Hitachi File Services Manager and Hitachi Command Suite Common Component restart after the command is executed.

Even if you specify the `/auto` option, if Tuning Manager connected to Device Manager is installed on a computer other than the one where the Device Manager is installed, the Tuning Manager service will not be automatically started or stopped.

8. If HiRDB uses a port number other than the default value (`22032`) when performing operations, reset the port number to the desired value.

   For details about how to change the port number used by HiRDB, see Changing the port numbers used by Hitachi Command Suite Common Component on page 7-90.

9. Execute a command as follows to stop Hitachi File Services Manager and Hitachi Command Suite Common Component, if active:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
   stop
   ```

10. From the Services window in Windows, open the following properties, and then change the settings of **Startup Type** from **Automatic** to **Manual**:
    - Hitachi Command Suite product services
    - **HBase 64 Storage Mgmt Web Service**
    - **HiRDB/ClusterService _HD1**
    - **HFSM Web Service**
11. In Failover Cluster Management, place the group online.

Migrating the database of the management server

If you have been using Hitachi File Services Manager and Hitachi Command Suite products for a long time, and wish to add further managed objects or upgrade your programs, you might need to replace your hardware with machines that deliver better performance. In this case, database migration will be required as one of the steps of the machine replacement procedure.

You (the system administrator) can migrate databases even when the installation destinations of Hitachi File Services Manager differ between the

migration source and migration target, or when the version of Hitachi File Services Manager on the migration target is newer than that on the migration source.

This subsection describes how to migrate the database of the management server.

Migrating database prerequisites

The following provides some notes on the required type and version of Hitachi File Services Manager and Hitachi Command Suite products on the migration source and migration target, and user information on the management server.

Notes on the type and version of Hitachi File Services Manager and Hitachi Command Suite products on the migration source and migration target

- Make sure that you install all the required Hitachi File Services Manager and Hitachi Command Suite products on the migration target.

  You cannot migrate the databases of Hitachi File Services Manager and Hitachi Command Suite products if they are not installed on the migration target.
- Make sure that the versions of Hitachi File Services Manager and Hitachi Command Suite products you install on the migration target are the same as or newer than the versions on the migration source.

  You cannot migrate any of the databases of Hitachi File Services Manager or Hitachi Command Suite products if the version of any one of these programs is older than the versions on the migration source.
- If you migrate the Replication Monitor database to the Replication Manager database, first upgrade Replication Monitor on the source server to Replication Manager, and then migrate the database.
- When migrating the Tuning Manager database, you need to check whether the database is in a migratable state. For details, refer to the section that describes database management in the relevant Tuning Manager manual.

Notes on user information

- Do not migrate databases to a management server on which user information for Hitachi File Services Manager and Hitachi Command Suite products already exists.

  If user information exists on the migration target, the user information will be replaced with that of the migration source.
- Because user information is replaced during migration, you cannot migrate multiple management servers (each running Hitachi File Services Manager and one or more Hitachi Command Suite products) to a single management server.

To migrate a database

1. On the migration target server, install Hitachi File Services Manager and Hitachi Command Suite products whose databases you want to migrate.

For details about how to install Hitachi File Services Manager, see Performing a new installation of Hitachi File Services Manager on page 7-2. For details about how to install the Hitachi Command Suite products, see the relevant product manual.

2. Export the databases on the migration source server.

   For details about how to export a database on the migration source server, see Exporting the database on the migration source server on page 7-120.

3. Transfer the archive file from the migration source server to the migration target server.

4. On the migration target server, import the databases.

   For details about how to import a database on the migration target server, see Importing the database on the migration target server on page 7-121.

Exporting the database on the migration source server

To export the database of Hitachi File Services Manager, the following two folders are required: a folder for temporarily storing the database information and a folder for storing an archive file. For each folder, secure as much free space as the total size of the following folders:

- The folder that stores the database of Hitachi File Services Manager
- The folder that stores the database of Hitachi Command Suite Common Component, excluding the `SYS` folder and all the files and folders under this folder

This is an approximate value when only the database of Hitachi File Services Manager is installed. If any Hitachi Command Suite products are installed, take the size of their databases into consideration too.

If the entire database capacity is more than 2 GB, an attempt to create an archive file will fail when the database is exported. When the database capacity is more than 2 GB, use another method to migrate without using an archive file.

To export a database from the migration source server

1. Stop the Tuning Manager service connected to the Device Manager on the management server.

   This step is necessary if Hitachi Command Suite products including Device Manager have been installed on the management server, and Tuning Manager connected to that Device Manager has been installed on another computer. Stop the Tuning Manager service from the computer where Tuning Manager has been installed. For details about how to stop the Tuning Manager service, see the manual for the installed version of Tuning Manager.

2. Execute a command as follows to stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
stop
```

3. Execute a command as follows to start HiRDB:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbsrv /start
```

4. Execute a command as follows to export the database:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbtrans /export /workpath work-folder /file archive-file [/auto]
```

The following explains the command options:

`/export`

You must specify this option to export a database.

`/workpath`

For this option, specify the absolute path of the folder (a work folder) that temporarily stores information of the exported database. This work folder must be located on the local disk and must be empty.

`/file`

For this option, specify the absolute path of the archive file for the database.

`/auto`

This option automatically starts and stops services of Hitachi Command Suite products.

Even if you specify the `/auto` option, if Tuning Manager connected to Device Manager is installed on a computer other than the one where the Device Manager is installed, the Tuning Manager service will not be automatically started or stopped.

5. If an error message is output, you must take action according to the message.
6. Transfer the archive file to the migration target server.

   If the archive file could not be created, transfer all the files stored in the folder that you specified for the `/workpath` option. When doing this, do not change the file structure under the folder specified by the `/workpath` option.

Importing the database on the migration target server

To import a database into the migration target server

1. Stop the Tuning Manager service connected to the Device Manager on the management server.

   This step is necessary if Hitachi Command Suite products including Device Manager have been installed on the management server, and Tuning Manager connected to that Device Manager has been installed on another computer. Stop the Tuning Manager service from the computer where

Tuning Manager has been installed. For details about how to stop the Tuning Manager service, see the manual for the installed version of Tuning Manager.

2. Execute a command as follows to stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
stop
```

3. Execute a command as follows to start HiRDB:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbsrv /start
```

4. Execute a command as follows to import the database:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbtrans /import /workpath work-folder [/file archive-file] /type
{ALL | names-of-Hitachi-File-Services-Manager-and-Hitachi-Command-Suite-
products-being-migrated} [/auto]
```

The following explains the command options:

`/import`

You must specify this option to import a database.

`/workpath`

To import a database by using an archive file:

Specify the absolute path of the folder (a work folder) that is used to extract an archive file. This work folder must be located on the local disk and must be empty. When an archive file is used, you must specify the `/file` option.

To import a database by not using an archive file:

Specify a folder that stores the information of the database that was transferred from the migration source. Do not specify the `/file` option.

`/file`

Specify the absolute path of the database archive file transferred from the migration source server. If the database information transferred from the migration source is stored in the folder specified by using the `/workpath` option, you can omit the `/file` option.

`/type`

Specify the names of the Hitachi File Services Manager and Hitachi Command Suite products whose databases you are importing. To import the database of Hitachi File Services Manager, specify `FileServicesManager`.

To import the databases of installed Hitachi Command Suite products as well as the database of Hitachi File Services Manager, specify `ALL` or specify the individual names of Hitachi File Services Manager and Hitachi Command Suite products, delimited with commas (,). For

about the name to specify in each case, see the relevant Hitachi Command Suite product manual.

When `ALL` is specified, the databases for Hitachi File Services Manager and Hitachi Command Suite products installed on the migration target server are automatically selected from the databases on the migration source server and are imported to the migration target server.

If you choose to specify the individual names of Hitachi File Services Manager and Hitachi Command Suite products, first make sure that the databases of all the products you are specifying are contained in the *archive-file* or reside in the folder specified in the `/workpath` option, and that all the products you are specifying are installed on the migration target server. If any product does not fulfill these requirements, the import process will stop.

`/auto`

This option automatically starts and stops services of Hitachi Command Suite products.

Even if you specify the `/auto` option, if Tuning Manager connected to Device Manager is installed on a computer other than the one where the Device Manager is installed, the Tuning Manager service will not be automatically started or stopped.

5. If an error message is output, you must take according to the message.
6. Execute a command as follows to start Hitachi File Services Manager and Hitachi Command Suite Common Component:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
start
```

7. If you stopped the Tuning Manager service in step 1, restart the service.

   This step is necessary if Hitachi Command Suite products including Device Manager have been installed on the management server, and Tuning Manager connected to that Device Manager has been installed on another computer. Start the Tuning Manager service on the computer where Tuning Manager has been installed.

Changing the host name or IP address of the management server

You (the system administrator) must edit some configuration files before changing the host name or IP address of the management server. If the management server is used in a cluster configuration, information in the configuration files must be the same for the executing node and the standby node.

If you have changed the host name or IP address of the management server before editing the configuration files, use the `hostname` command or the `ipconfig /All` command to display the new host name or IP address, and then take note. Then, specify the noted host name as is in the configuration files, because a host name is case-sensitive.

The procedure for changing the host name or IP address of the management server is shown below. In the following procedure, the *host name* refers to either the host name or the IP address:

To change the host name or IP address of the management server

1. Execute the `hostname` command or the `ipconfig /ALL` command to display the host name that has been used before the change, and then take note.

   If an error occurred due to the host name change, use the noted host name specified before the change to return to the original state.

2. Execute a command as follows to stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
   stop
   ```

3. If SSL has been set, use the new host name to set SSL again.

   For details about how to set SSL, see Setting up SSL on page 7-92.

4. Use the new host name to edit the `user_httpsd.conf` file.

   If SSL has not been set, specify the new host name for the following items in the `user_httpsd.conf` file.

Table 7-42 Item for which to change the host name (when SSL has not been set)

File name	File path	Item to change
`user_httpsd.conf`	*Hitachi-Command-Suite-Common-Component-installation-folder*`\uCPSB\httpsd\conf\`	`ServerName` at the top of the file

If SSL has been set, in addition to the `user_httpsd.conf` file item above, specify the new host name for the following items.

Table 7-43 Items for which to change the host name (when SSL has been set)

File name	File path	Items to change
`user_httpsd.conf`	*Hitachi-Command-Suite-Common-Component-installation-folder*`\uCPSB\httpsd\conf\`	The following items in the `VirtualHost` tag: • `VirtualHost` • `ServerName`

5. If necessary, use the new host name to edit the `cluster.conf` file.

   This step must be performed if the management server is running in the cluster configuration.

   Specify the new host name for the relevant items in the `cluster.conf` file, as listed in the table below.

Table 7-44 Items for which to change the host name (cluster.conf file)

File name	File path	Items to change

`cluster.conf`	*Hitachi-Command-Suite-Common-Component-installation-folder*`\conf\`	If changing the logical host name:
		`virtualhost`
		If changing the host name of the executing node:
		`onlinehost`
		If changing the host name of the standby node:
		`standbyhost`

6. Change the host name of the management server, and then restart the management server.

   If the host name has already been changed, you only need to restart the management server.

7. Change the URL of the management server.

   This step is necessary if both Hitachi File Services Manager and Device Manager are installed on the same management server. For details about how to change the URL of the management server, see the relevant Device Manager manual.

8. Execute a command as follows to make sure that the service of Hitachi Command Suite Common Component is running:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
status
```

Adjusting the management server time

This subsection describes how to adjust the time in the management server after you install Hitachi File Services Manager.

To adjust the management server time after installation, use a program for adjusting the time automatically.

When using a program that adjusts the time automatically while using NTP or another protocol, make sure that when the system clock is ahead of the actual time, the program will adjust the system clock gradually over time without turning the clock back. Some synchronization programs make incremental adjustments if the time difference is within a set limit, and turn the clock back only if the time difference is more than the limit. In the synchronization program you are using, set the time adjustment frequency so that the time difference will not exceed the threshold for incremental adjustment.

For example, if you are using the Windows Time service and the system clock is ahead of the actual time by less than a set threshold, the system time can be adjusted gradually without turning back the clock. Check the value of this threshold in the Windows Time service, and set the tuning frequency so that

the difference between the system time and actual time does not exceed the threshold.

If the system clock on the management server is turned back, accesses from the management console might not receive a response until the system clock returns to the time at which the time was turned back. To prevent a large backward time offset from occurring, set an appropriate value for the MaxNegPhaseCorrection registry entry (which specifies the maximum number of seconds that the system clock can be delayed).

For details, see the following Microsoft web page:

https://support.microsoft.com/kb/884776

If accesses from the management console no longer receive a response because the clock has been turned back, and a recovery of operations is immediately required, see Adjusting the time by re-installing Hitachi File Services Manager on page 7-126.

Adjusting the time after installing Hitachi File Services Manager

If you do not have access to services for adjusting the system time automatically, or when you need to change the time immediately, set the system clock as follows:

1. Execute a command as follows to stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
   stop
   ```

2. Record the time specified for the management server, and then change the specified time.

   If you want to delay the management server time, wait until the time you recorded has expired, and then proceed to the next step.

3. Restart the management server machine.

Adjusting the time by re-installing Hitachi File Services Manager

If the clock is very far ahead (for example, by a month or a year), you can adjust the time by changing the time on the machine, uninstalling Hitachi File Services Manager on the management server, and then re-installing it. The following is the procedure for adjusting the time by re-installing Hitachi File Services Manager.

1. Execute a command as follows to stop Hitachi File Services Manager and Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /
   stop
   ```

2. Change the time that is set for the management server.
3. Uninstall Hitachi File Services Manager.

For details about how to uninstall Hitachi File Services Manager, see Uninstalling Hitachi File Services Manager on page 7-10.

4. Restart the management server machine.
5. Install Hitachi File Services Manager.

   For details about how to install Hitachi File Services Manager, see Performing a new installation of Hitachi File Services Manager on page 7-2.

Changing the JDK

After starting operation, to change the JDK used by Hitachi File Services Manager (e.g., due to security vulnerabilities), execute the `hcmds64chgjdk` command. You can change the JDK to Oracle JDK 7 or Oracle JDK 8.

The SSL certificate used by the management server to communicate with nodes is usually imported automatically when Hitachi File Services Manager is installed.

However, changing the JDK also changes the keystore, so you need to import the SSL certificate manually.

Note:

- After starting operation, if you overwrote the JDK used by Hitachi File Services Manager with Oracle JDK or performed an upgrade installation, re-register the JDK by using the `hcmds64chgjdk` command.
- After starting operation, if you changed the JDK used by Hitachi File Services Manager to Oracle JDK, and then had to uninstall Oracle JDK, change the JDK back to the one that came bundled with the product.
- If Hitachi Command Suite products version 7.0 or earlier are installed on the management server, you cannot change the JDK to Oracle JDK.

To change the JDK, perform the following procedure

1. Stop the services of Hitachi File Services Manager and Hitachi Command Suite products.

   For details on how to stop the services, see Stopping Hitachi File Services Manager on page 7-34.
2. To change the JDK, execute commands as follows:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64chgjdk
   ```

   In the window that appears, select the JDK that you want to use.
3. Start the services of Hitachi File Services Manager and Hitachi Command Suite products.

   For details about how to start the services, see Starting Hitachi File Services Manager on page 7-33.
4. Import the SSL certificate to the keystore file of the management server (`jssecacerts`).

When you import the SSL certificate, the certificate is moved inside the JDK to be used.

For details on how to import the SSL certificate to the management server, see Importing the required SSL certificate for communication between the node and management server on page 7-99.

5. In environments where Windows firewall is enabled, if you change the JDK to Oracle JDK, the `java.exe` file of Oracle JDK needs to be manually registered as an exception.

Settings required to use antivirus software on the management server

When antivirus software accesses files related to the databases used by Hitachi Command Suite products, a failure might occur due to delayed I/O operations or file locking.

To prevent this failure, while the Hitachi Command Suite products are running, configure the antivirus software to exclude the following folders from scans:

Hitachi-Command-Suite-Common-Component-installation-folder\HDB
Hitachi-Command-Suite-Common-Component-installation-folder\database
Hitachi-File-Services-Manager-installation-folder\database

These folder locations, where database files are stored, are examples of default values specified when Hitachi Command Suite products and Hitachi File Services Manager were installed. You can specify other folders as the locations where database files are stored, according to your preferences. If you have configured the system to use other folders as the locations where database files are stored, configure the antivirus software to exclude those folders from scans.

A

ACLs Created After the File System Is Migrated to That of the Advanced ACL Type

This appendix describes the ACLs that are created when a file system of the Classic ACL type is migrated to a file system of the Advanced ACL type.

ACLs Created After the File System Is Migrated to That of the Advanced ACL Type

The HDI system creates an ACL so that the inheritance relationship and access permissions can be inherited after migration of a file system from the Classic ACL type to the Advanced ACL type.

Only **Allow** access permissions are set for a file system of the Classic ACL type. To maintain the inheritance relationship and access permissions, **Deny** ACEs might be added to the ACL created after the migration. If the access permissions (represented by a mask value) for a user or group are more restrictive than the logical OR of the access permissions, then a **Deny** ACE is created for the difference between the permissions. For example, when access permissions are set to `4(r--)` for a user and `6(rw-)` for others (`Everyone`), a **Deny** ACE for `2(-w-)` is created for the user. If access permissions are set to `4(r--)` for a user, `6(rw-)` for a group, and `5(r-x)` for others (`Everyone`), the mask value of the logical OR of the access permissions for the group and `Everyone` is `7(rwx)`. As a result, a **Deny** ACE for `3(-wx)` is created for the user.

The following table shows the correspondence between the access permissions set for a file system of the Classic ACL type before migration and the **Allow** access permissions created after migration.

Table A-1 Correspondence between access permissions for a file system before and after migration

Possible access permissions before migration:		**7 rwx**	**6 rw-**	**5 r-x**	**4 r--**	**3 -wx**	**2 -w-**	**1 --x**	**0 ---**
Corresponding access permissions after migration:	Traverse Folder/ Execute File	**A**	--	**A**	--	**A**	--	**A**	--
	List Folder/ Read Data	**A**	**A**	**A**	**A**	--	--	--	--
	Read Attributes	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**
	Read Extended Attributes	**A**	**A**	**A**	**A**	--	--	--	--
	Create Files/Write Data	**A**	**A**	--	--	**A**	**A**	--	--
	Create Folders/ Write Data	**A**	**A**	--	--	**A**	**A**	--	--
	Write Attributes	**A**	**A**	--	--	**A**	**A**	--	--

Possible access permissions before migration:		7 rwx	6 rw-	5 r-x	4 r--	3 -wx	2 -w-	1 --x	0 ---
	Write Extended Attributes	**A**	**A**	--	--	**A**	**A**	--	--
	Delete Subfolders and Files	**A**	**A**	--	--	**A**	**A**	--	--
	Delete	--	--	--	--	--	--	--	--
	Read Permissions	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**
	Change Permissions	O	O	O	O	O	O	O	O
	Take Ownership	O	O	O	O	O	O	O	O

Legend: **A** = After the migration, **Allow** is set. -- = After the migration, **Allow** is not set. O = **Allow** is set for access permissions of the file owner

If the access permissions for a user or group are more restrictive than the logical OR of the access permissions before migration then, for the difference between the permissions, a **Deny** ACE is created after migration.

The mask values are calculated by the following formula:

Mask value = *r* **x** 4 + *w* **x** 2 + *x* **x** 1

Where:

r: Read permission bit (0 or 1)

w: Write permission bit (0 or 1)

x: Execution permission bit or direct research permission bit (0 or 1)

The access is allowed if the corresponding bit is 1.

For example, if the logical OR of access permissions is `7(rwx)` in the file system before migration, all the permission bits (*r*, *w*, *x*) will be 1 and the mask value will be as follows:

Mask value = *r* **x** 4 + *w* **x** 2 + *x* **x** 1

= 1 **x** 4 + 1 **x** 2 + 1 **x** 1

= 7

The following table shows how the **Deny** access permission created after migration corresponds to the differences between the following before migration:

- The more restrictive access permissions for a user or group

- The logical OR of the access permissions in the file system

Table A-2 More restrictive access permissions before migration, and the access permissions created after migration

Insufficient access permissions before migration:		**7 rwx**	**6 rw-**	**5 r-x**	**4 r--**	**3 -wx**	**2 -w-**	**1 --x**	**0 ---**
Corresponding access permissions after migration:	Traverse Folder/ Execute File	**D**	--	**D**	--	**D**	--	**A**	--
	List Folder/ Read Data	**D**	**D**	**A**	**D**	--	--	--	--
	Read Attributes	--	--	--	--	--	--	--	--
	Read Extended Attributes	**D**	**D**	**A**	**D**	--	--	--	--
	Create Files/Write Data	**D**	**A**	--	--	**A**	**D**	--	--
	Create Folders/ Write Data	**D**	**A**	--	--	**A**	**D**	--	--
	Write Attributes	**D**	**A**	--	--	**A**	**D**	--	--
	Write Extended Attributes	**D**	**A**	--	--	**A**	**D**	--	--
	Delete Subfolders and Files	**D**	**A**	--	--	**A**	**D**	--	--
	Delete	--	--	--	--	--	--	--	--
	Read Permissions	--	--	--	--	--	--	--	--
	Change Permissions	--	--	--	--	--	--	--	--
	Take Ownership	--	--	--	--	--	--	--	--

Legend: **A** = After the migration, **Allow** is set. **D** = After the migration, **Deny** is set. -- = After the migration, **Deny** is not set.

B

Using the Node Power Lamp Switch or Power Button to Start or Stop the OS

This appendix explains how the node power lamp switch or power button is used to start or stop the OS. Normally, the GUI or CLI are used to start or stop the OS, but if you need to use a node's power lamp switch or power button, follow the instructions of maintenance personnel.

First, check the product name of the node being used. You can acquire the name by using the `hwstatus` command. If Compute Rack is used for the node, use the power lamp switch. If D51B-2U or PowerEdge is used for the node, use the power button.

Starting an OS

You can start an OS by using the power lamp switch or power button to turn on the node. To start both OSs after a planned shutdown of the OSs on both nodes in a cluster is performed, turn on one of the nodes, and then turn the other node on within 10 minutes of turning on the first node. If this is not done, a failover will occur on the node for which the OS has not yet been started.

To start the OS by turning on the power to a node:

1. Make sure that the external servers connected to the node are running.
2. Make sure that the power lamp, power LED or power indicator (the LED on the power lamp switch or power button) located on the front of the node is not on.
3. Make sure that the storage systems and FC switches are running.

   If the OS is started while the storage systems and FC switches are not running, FC path errors will occur.
4. Make sure that the IP switches for the management LAN are running.

   Note that the management server and the management console can be connected to from the node only when the IP switches for the management LAN are running.
5. If you are using the local data encryption functionality, when you save system settings on the HCP system, confirm that the HCP system is running normally, and that the HDI and HCP systems can communicate normally.

   User data cannot be available unless the HCP system can be communicated with.
6. Press the power lamp switch or power button located on the front of the node.
7. Make sure that the power lamp, power LED or power indicator lights up.

Forcibly Stopping an OS

If the power lamp or power indicator cannot be turned off via the GUI or commands, you can use the power lamp switch or power button to forcibly stop an OS.

To forcibly stop the OS by turning off the power to a node:

1. Hold down the power lamp switch or power button located on the front of the node for 5 seconds or more.
2. Make sure that the power lamp, power LED or power indicator (the LED on the power lamp switch or power button) is off.

C

Layout of Node Ports

This appendix shows the layout of ports on nodes to be used for HDI of the cluster configuration.

Port layout

The port layout differs depending on the type of node in use. Depending on the type of node, you might be able to install one of the following optional cards into an expansion slot:

- GbE card: There are four GbE data ports (`eth`*number*).
- 10GbE card: There are two 10GbE data ports (`xgbe`*number*).
- FC card: There are two FC ports for connection to a storage system or tape device.

Examples of port layouts are shown in the following figures. You can check the model name of the node by using the `hwstatus` command.

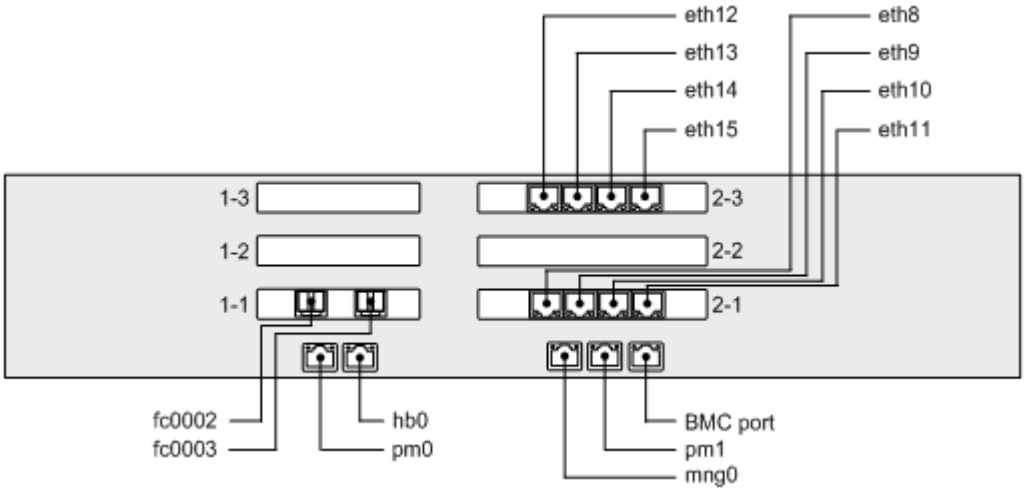


Figure C-1 Port layout example (when the node model is D51B-2U, and a GbE card is in an expansion slot)

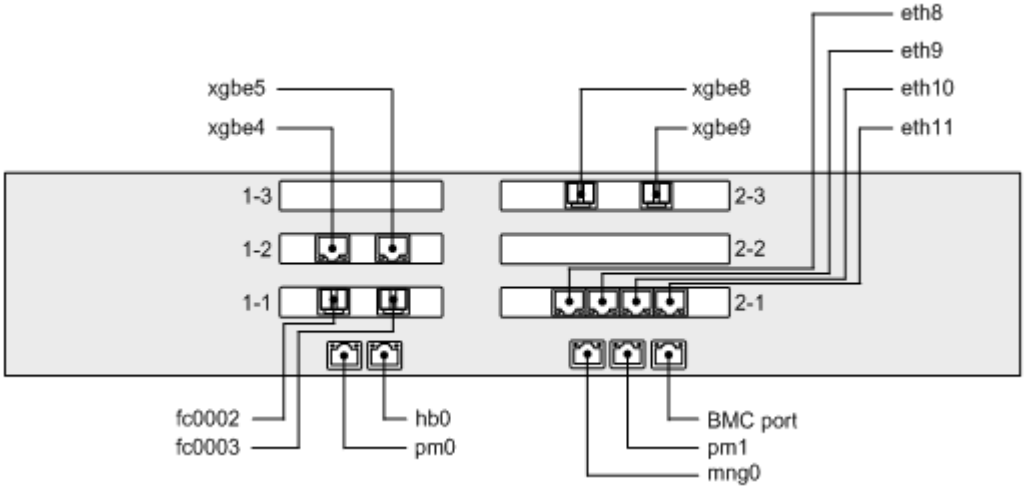


Figure C-2 Port layout example (when the node model is D51B-2U, and a 10GbE card is in an expansion slot)

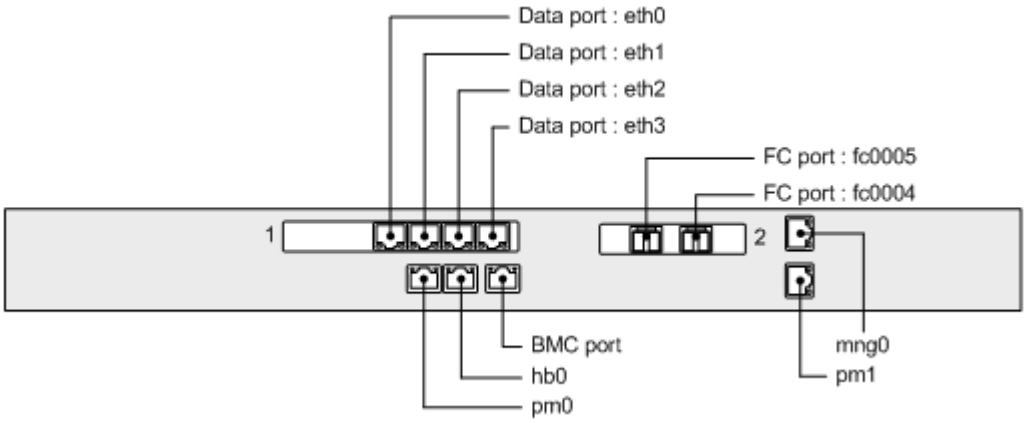


Figure C-3 Port layout example (when the node model is Compute Rack 210H, and a GbE card is in an expansion slot)

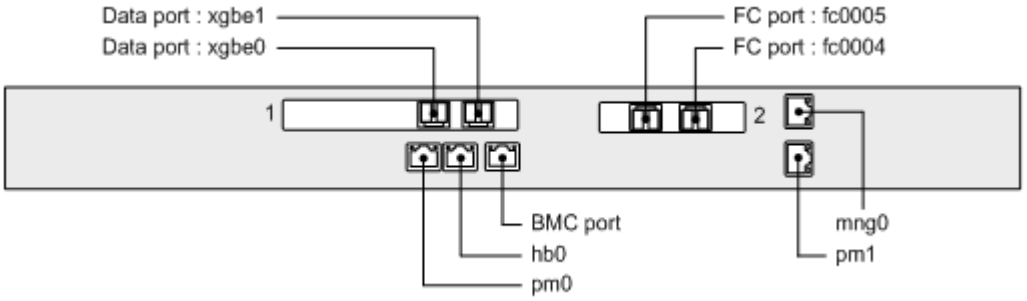


Figure C-4 Port layout example (when the node model is Compute Rack 210H, and a 10GbE card is in an expansion slot)

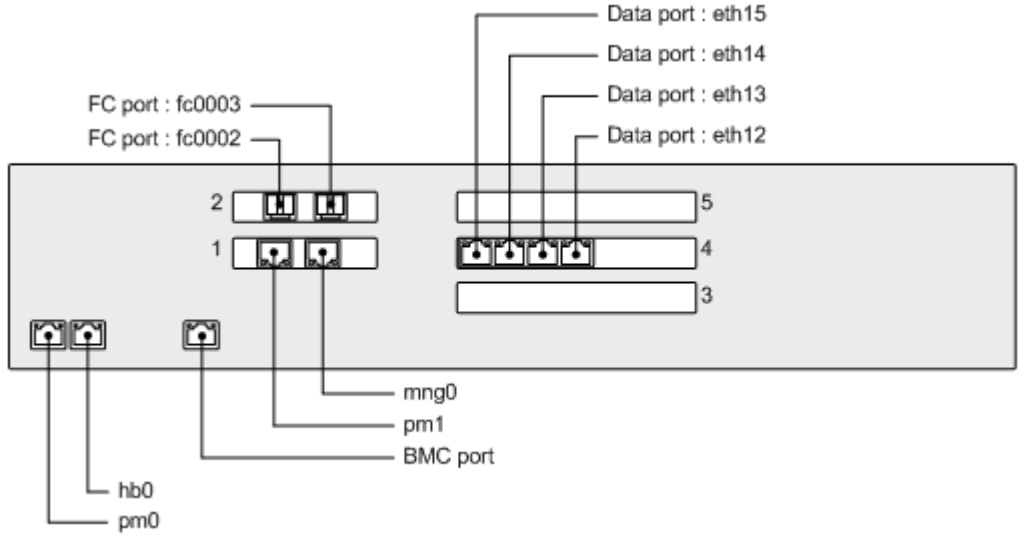


Figure C-5 Port layout example (when the node model is HA8000/RS220)

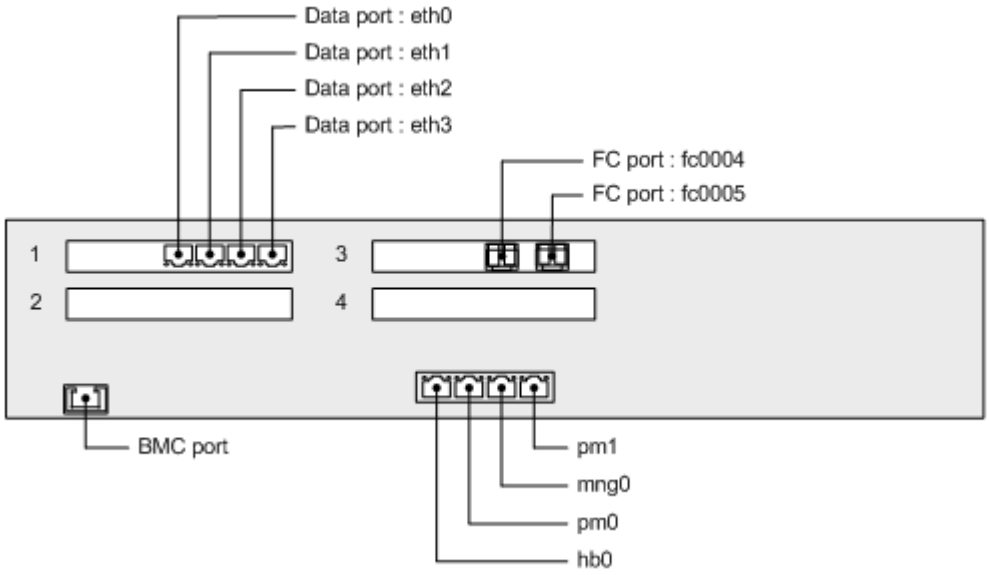


Figure C-6 Port layout example (when the node model is PowerEdge)

D

Status of IPv6 Support in External Servers and Services

HDI systems support IPv4 and IPv6. This appendix describes the status of IPv6 support for the external servers and services of HDI systems.

List of external servers and services available on IPv6

The tables below show whether external servers and the services provided by HDI systems can be used with IPv6.

Table D-1 Status of IPv6 support for external servers

Category	Availability
Management console, management server	Yes
NTP server	Yes
SNMP manager	Yes
Backup server, media server	No
DNS server	Yes
NIS server	No
KDC server	Yes#1
Domain controller	Yes
LDAP server	Yes
Scan server	Yes#2
System log transfer destination	No
SMTP server	Yes#3
HCP	No
Relaying devices used by an HCP system to be linked (such as a load balancer)	No

Legend: Yes = Available with IPv6; No = Unavailable with IPv6

#1:
Available when using Kerberos authentication for the CIFS service.

#2:
Available when using Trend Micro ServerProtect.

#3:
Available when a host name is specified.

Table D-2 Status of IPv6 support for services and functionality provided by HDI systems

Category	Availability
NFS service	Yes#1
CIFS service	Yes
SSH service	Yes
FTP service	Yes#2

Category	Availability
SFTP service	Yes#2
TFTP service	No
Real-time virus scanning functionality	Yes
NDMP functionality	No
Linkage with HCP systems	No
Linkage with Hitachi Command Suite products	Yes
Data importing from other file servers	Yes
Linkage with DHCP servers	No

Legend: Yes = Available with IPv6; No = Unavailable with IPv6

#1:

Unavailable for Kerberos authentication.

#2:

FXP is unavailable.

E

Attributes of Directories and Files to Be Backed Up or Restored

This appendix describes the file system information (quota information) and attributes of directories and files that are backed up to media or restored from media by the NDMP functionality.

Attributes to be backed up

The quota information and directory and file attributes that are backed up to media are shown in Table E-1 Quota information backed up to media on page E-2 and Table E-2 Directory and file attributes backed up to media on page E-2.

Table E-1 Quota information backed up to media

Type	Attribute	Details
Quotas set for a file system	• Default quota • User quota • Group quota	• Soft limit for block usage • Hard limit for block usage • Soft limit for inode usage • Hard limit for inode usage
	Grace period	• Grace period for block usage • Grace period for inode usage
Quotas set for a directory (subtree quota)	• Quota for the directory • Default quota • User quota • Group quota	• Soft limit for block usage • Hard limit for block usage • Soft limit for inode usage • Hard limit for inode usage
	Grace period	• Grace period for block usage • Grace period for inode usage

Table E-2 Directory and file attributes backed up to media

Attribute	Details	
inode	• Path name of file • File mode • User ID of owner • Group ID of owner • Last modified time (ctime) • Last edited time (mtime) • Last access time (atime) • File creation time • Data size • File type • Link path name	
ACL information	Classic ACL	Access ACL • Access permission • Inherited attributes Default ACL • Access permission • Inherited attributes
	Advanced ACL	• User or group

Attribute	Details	
		• Account type • Application destination • Inheritance range • ACE type • Access permissions
File attributes	Classic ACL	Read
	Advanced ACL	• Read • Archive • Hidden file • System file
WORM	WORM settings information	
Migration	• Status of HCP system migrations • Reference to the data on the migration-destination HCP system	

Attributes to be restored

When backup data is restored from media, the data at the time of backup is restored to the file system. To return the data, which you restore, to the backed-up state, the data must be restored to the file system that has the same settings as the backed-up settings.

If the ACL type of the backup data differs from the ACL type of the file system at the restore destination, the ACL information is set as shown in the following table after the restore operation is performed.

Table E-3 Restoration results when ACL types differ (backup data for non-WORM file systems)

Backup data	Restoration destination file system#	
	Advanced ACL type	Classic ACL type
Advanced ACL type	The Advanced ACL information set for the backup data is restored.	No ACL information is restored.
Classic ACL type	The Classic ACL information set for the backup data is converted to Advanced ACL information during a restore operation.	The Classic ACL information set for the backup data is restored.

#:

Both a normal file system and a WORM file system can be specified.

Table E-4 Restoration results when ACL types differ (backup data for WORM file systems)

Backup data	Restoration destination file system#	
	Advanced ACL type	Classic ACL type
Advanced ACL type	The Advanced ACL information set for the backup data is restored.	Restoration cannot be performed.
Classic ACL type	Restoration cannot be performed.	The Classic ACL information set for the backup data is restored.

#:

Only WORM file systems can be specified as restoration destinations.

When the restore operation finishes, check the restored data, and then change the ACL settings if necessary.

F

Processing Executed According to the Settings of Custom Scheduling of the File Version Restore Functionality (in Cumulative Mode)

This appendix describes the processing when the cumulative mode is used to select the past-version directories to be kept in custom scheduling of the file version restore functionality.

Behavior when a custom schedule is used

If you use a custom schedule, the past-version directories, other than those kept according to the schedule, are deleted in the following situations:

- When migration is executed
- When a value smaller than the value currently specified for the retention period of the past version directories is set
- When the custom schedule is configured for use
- When the custom schedule is changed

As shown in the table below, you can specify schedules in intervals of 15 minutes, 1 hour, 1 day, 1 week, 1 month, and 1 year.

Schedule	Unit
Every 15 minutes	Hour *n*, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59
Hourly	Hour *n*, minutes 00 to 59
Daily	Day *n*, 00:00 to 23:59
Weekly	Week *n*, Sunday, 00:00 to Saturday, 23:59
Monthly	Month *n*, 1st day, 00:00 to *last-day*, 23:59
Yearly	Year *n*, Jan 1, 00:00 to Dec 31, 23:59

Starting from the interval within which past-version directories are deleted, past-version directories of the specified number of intervals are retained in reverse chronological order. For each interval, only the oldest past-version directory is retained.

If you set multiple schedules for different intervals, the retention or deletion of past-version directories is executed in descending order of the length of each schedule interval. Thus, to avoid overlaps of past-version directories retained in intervals of each schedule, the processing according to the schedule of the longer interval can be executed, depending on the setting for schedules of a shorter interval. The processing starts from the interval that does not include the time of deletion.

When using custom scheduling, specify a number of days greater than or equal to the recommended value calculated by the following formula for the retention period of the past-version directories.

Recommended value for the retention period of past version directories (in days)
$\geq \uparrow (minutes / 60 + hours) / 24 \uparrow + days + weeks \times 7 + months \times 31 + years \times 366$

Legend:
$\uparrow \ \uparrow$: Round up to an integer

Note: If a value calculated by the formula is greater than 36,500, the recommended value is 36,500.

When using a custom schedule, we recommend that you specify settings so that directories are created every time a migration is performed. If you

change the settings by using the `arcconfedit` command so that the past-version directories are created only when a migration is performed for the first time in a single day, the past-version directories might not be kept as intended when the custom schedule was configured for use.

Example of processing executed according to a custom schedule

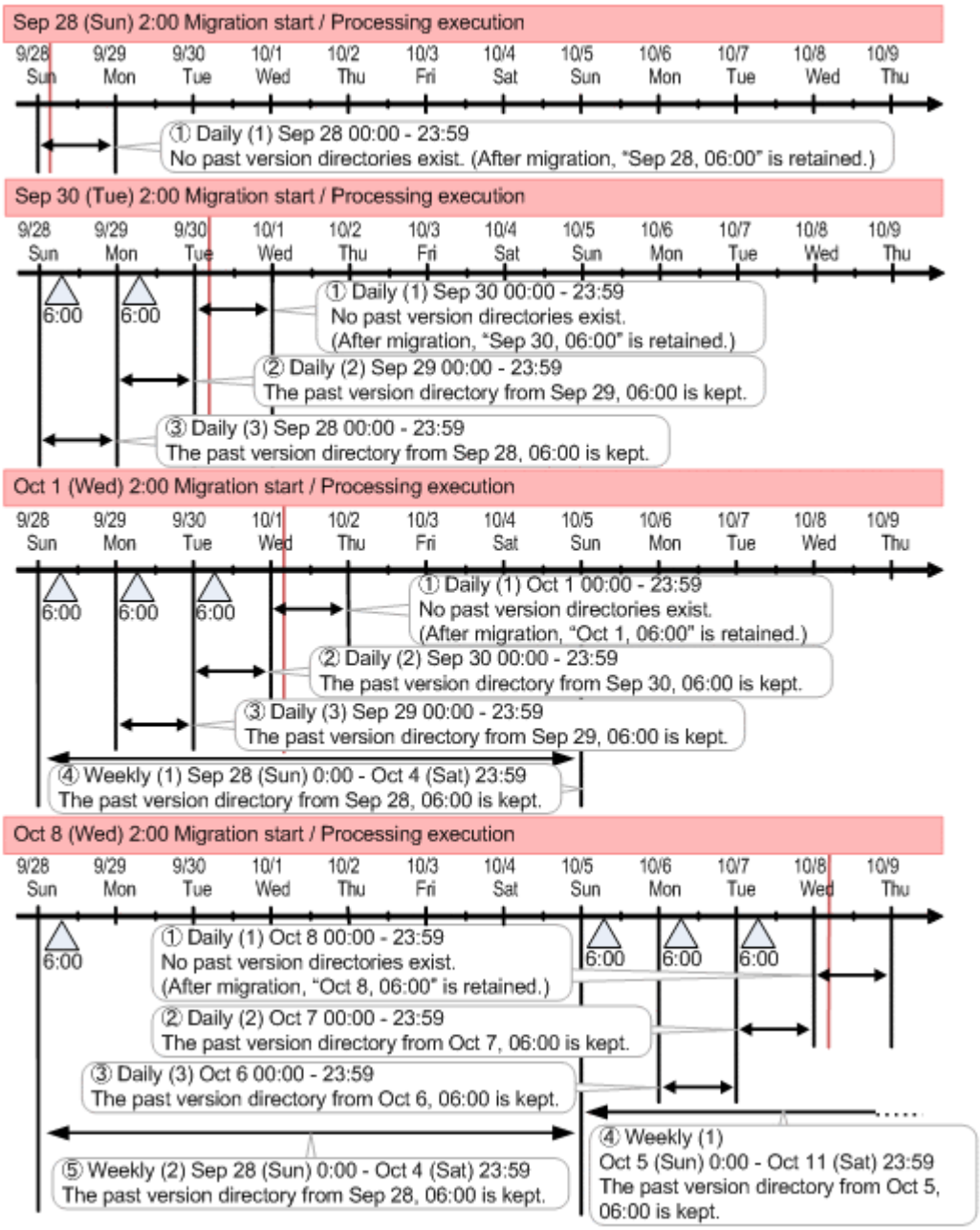
This section gives an example of processing executed according to a custom schedule.

If processing is executed when migration is executed:

If a custom schedule is used with the schedules set as described as follows, migration would take 4 hours to complete and be performed at 2:00 AM daily.

Schedule	Number of units the past directories are kept
Every 15 minutes	0
Hourly	0
Daily	3
Weekly	2
Monthly	0
Yearly	0

The following figure shows the past-version directories that are kept as a result of executing processing when migration is executed:



The past-version directories are created at 6:00, when migration is complete. Therefore, the interval in which the first processing is executed as per the daily schedule setting does not yet have a past-version directory. Even in this case, the interval is regarded as one retaining its past-version directory.

When processing is executed on Sept. 30, past-version directories for the three intervals (Sept. 28-30) are retained in accordance with the daily schedule. No retained past-version directory is created at this time in accordance with the weekly schedule.

As some processing is executed on Oct. 1, past-version directories for the three intervals (Sept. 29-Oct. 1) are retained in accordance with the daily schedule. In addition, the past-version directory for Sept. 28 (which is not

retained by the daily schedule) is retained by the weekly schedule, which is executed next.

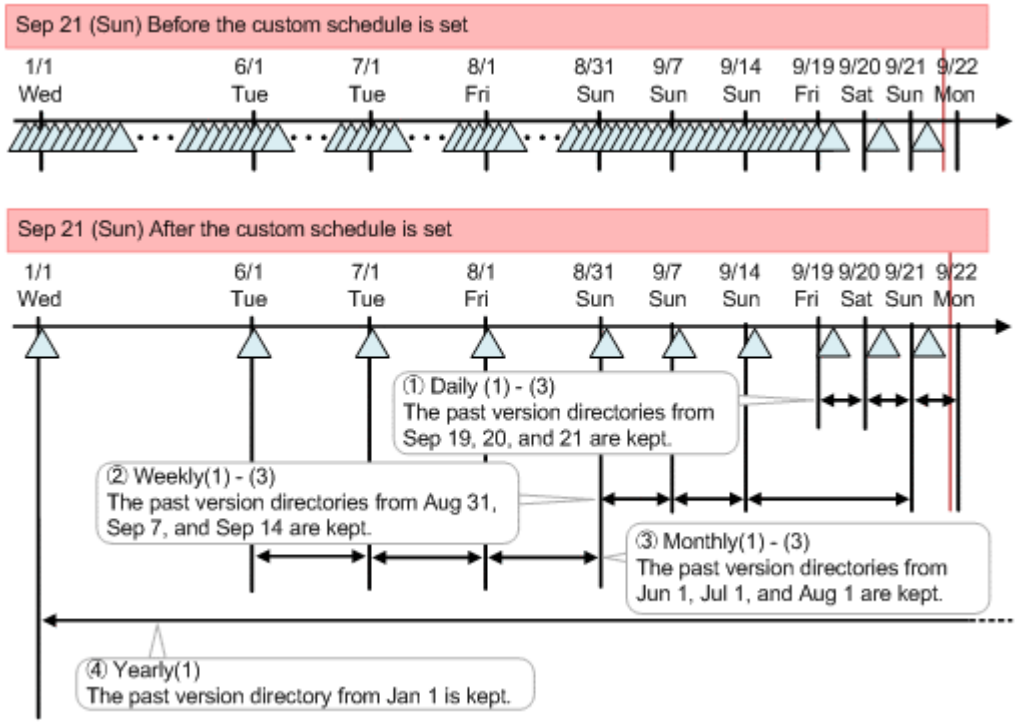
As some processing is executed on Oct. 8, past-version directories for the three intervals (Oct. 6-8) are retained in accordance with the daily schedule. In addition, the past-version directories for Sept. 28 and Oct. 5 (which are not retained by the daily schedule) are retained by the weekly schedule, which is executed next.

If processing is executed when a custom schedule is set:

If a custom schedule were to be used with the schedules set as described below for a file system, migration would take 4 hours to complete and be executed daily at 2:00.

Schedule	Number of units the past directories are kept
Every 15 minutes	0
Hourly	0
Daily	3
Weekly	3
Monthly	3
Yearly	1

Assume that you activate a custom schedule after the migration on Sept. 21 is complete. The following figure shows the past version directories that are kept as a result of executing processing when a custom schedule is set:



The past-version directories for three intervals (Sept. 19-21) are retained by the daily schedule.

In addition, the past-version directories for Aug. 31, Sept. 7, and Sept. 14 (which are not retained by the daily schedule) are retained by the weekly schedule, which is executed next.

Furthermore, the past-version directories for Jun. 1, Jul. 1, and Aug. 1 (which are retained by neither the daily nor the weekly schedule) are retained by the monthly schedule, which is executed next.

Finally, the past-version directory for Jan. 1 (which is not retained by any of the daily, weekly, or monthly schedules) is retained by the yearly schedule.

In a weekly, monthly, or yearly schedule, processing starts from the interval including the latest date of processing from among the intervals in which no retention was performed during the previous schedule (if a weekly schedule is used, the interval including Sept. 18 23:59, that is, from Sept. 14 (Sun.) 00:00 to Sept. 20 (Sat.) 23:59). Therefore, in a weekly or monthly schedule, the retention of past-version directories starts from the interval that does not include the time of deletion.

G

Performing the Roaming of Migrated Home-directory Data among HDI Systems

This appendix describes how to perform roaming for a home-directory data among HDI systems after migrating the data from another file server that is already using the home-directory or after a CIFS administrator created the data.

Operation example

You can enable roaming for home-directory data migrated from another file server among HDI systems. If an end user who uses the home-directory is added to the operating system, you can also enable roaming for home-directory data among HDI systems after a CIFS administrator creates the home-directory data.

Check the following points before you enable roaming for home-directory data migrated from another file server or created by a CIFS administrator among HDI systems:

- Third-party software is assumed to be used to migrate data from another file server that is already using the home-directory.

  We recommend the `robocopy` command for Windows as third-party software to migrate data.

  If third-party software is not used, a CIFS administrator must manually create files for the home directory and user profile.

  HDI functionality that imports data from another file server cannot be used.
- All directories immediately under the mount point of the home-directory-roaming file system are subject to roaming.
- Do not create any files or directories other than the home-directory immediately under the mount point of the home-directory-roaming file system.
- To use uppercase and lowercase characters in the name of a home directory to be migrated, the version of the HDI system must be 5.3.*x*-*xx*, 5.4.*x*-*xx* or 6.*x*.*x*-*xx* (*x* can be any number) at all sites.

The following figure shows an operation example of enabling roaming for home directory data migrated from another file server or created by a CIFS administrator among HDI systems.

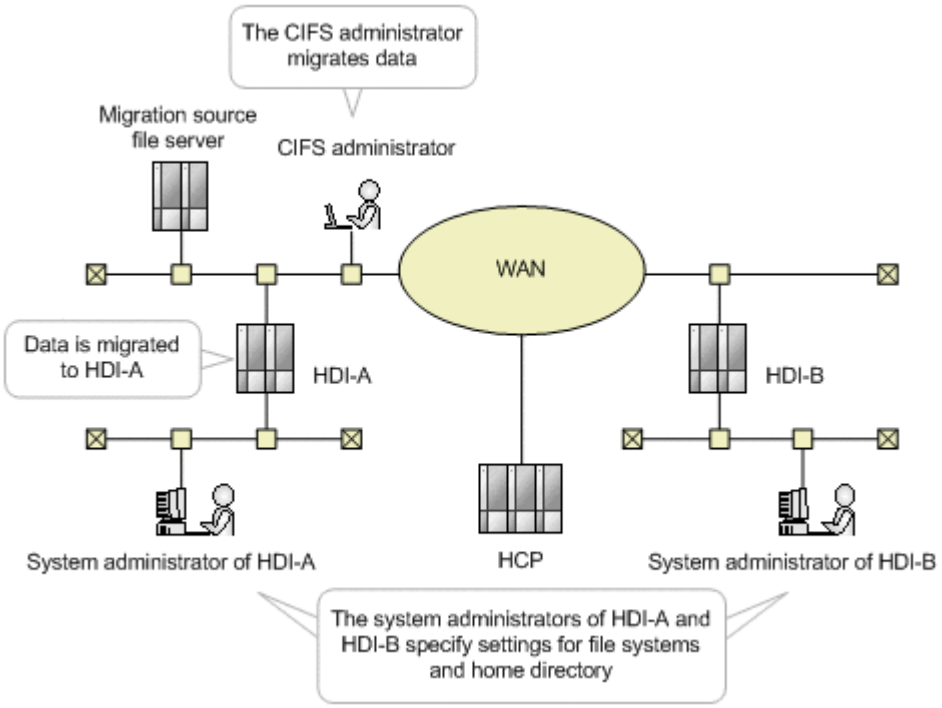


Figure G-1 Operation example of enabling roaming for migrated home-directory data among HDI systems

In this example, the home-directory data migrated to HDI-A is synchronized with HDI-B at another location via the HCP system to enable data roaming among the HDI systems.

The following describes the tasks required for enabling roaming for home-directory data migrated from another file server or created by a CIFS administrator among HDI systems, based on the example figure.

- Starting data roaming among HDI systems after migrating home-directory data on page G-3
- Creating a home directory in the operating system and then starting roaming among the HDI systems on page G-5

Starting data roaming among HDI systems after migrating home-directory data

The following table describes the tasks required for starting data roaming among HDI systems after migrating home-directory data from another file server:

Step	Performed on: (see Figure G-1)	Performed by:	Description
1	HDI-A	System administrator	Use the GUI or the `fscreate` command to create a home-directory-roaming file system, and then create a file share.
2	HDI-A	System administrator	Use the GUI or the `arccancelpolicy` command to disable the schedule of the migration task for the file system created in step 1. During the initial installation, data is migrated every hour. If the metadata of the migrated files and directories is updated by third-party software during data migration, the files and directories with updated metadata will be migrated again, and the data migration takes time to complete. Therefore, we recommend that the schedule of the migration task be disabled before starting the migration.
3	HDI-A	CIFS administrator	Use third-party software such as the `robocopy` command to migrate home-directory data from another file server to the file system created in step 1. To delete the home-directory that was migrated, execute the `archdctl` command with the `--del` option specified. If you want to delete the files or directories in the home-directory, do so after completing step 6.
4	HDI-A	CIFS administrator	Make sure that migration of all data was completed.
5	HDI-A	System administrator	Use the `archdctl` command with the `--roaming` option specified to enable roaming for the home-directory data migrated in step 3 among HDI systems.
6	HDI-A	System administrator	Use the `archdctl` command with the `--status` option specified to make sure that the roaming for the home-directory data migrated in step 3 among the HDI systems is enabled.
7	HDI-A	System administrator	If the schedule of the migration task was disabled in step 2, use the GUI or `arcschedulepolicy` command to set the schedule of the migration task again.
8	HDI-A	System administrator	Tell the end users to assign a network drive to the share created in step 1 before accessing the share.
9	HDI-A	System administrator	Use the GUI to make sure that the migration task for the file system created in step 1 was successful. Also make sure that the successful task was started after the end time of the `archdctl` command executed in step 6.
10	HDI-A	System administrator	Use the GUI to make sure that the system message KAQM37529-E has not been output.

Step	Performed on: (see Figure G-1)	Performed by:	Description
11	HDI-A	System administrator	Ask the system administrator of the other HDI system to create a home-directory-roaming file system. At this time, provide the following information: • Timestamps of nodes • Settings for client authentication • Settings for file systems (such as ACL types, the period to hold the data for past versions, and functions to be used) • Namespace for the migration destinations If a namespace was created when a file system was created by using the GUI, the administrator must be informed of the namespace name that was automatically created. If the HCP administrator created a namespace where data can be accessed from all the HDIs, provide the information given by the HCP administrator.
12	HDI-B	System administrator	Use the GUI or the `fscreate` command to create a home-directory-roaming file system, and then create a file share. Make sure that the settings listed in step 11 are identical across all the linked HDI systems.
13	HDI-B	System administrator	Tell the end users to assign a network drive to the share created in step 12 before accessing the share.

Creating a home directory in the operating system and then starting roaming among the HDI systems

To add end users to an HDI system for which roaming for home-directory data is already enabled, you can migrate data to a home directory created for each user and then enable roaming among HDI systems. Use either of the following methods.

- Creating a new home directory on page G-5
- Migrating home-directory data on page G-7

Creating a new home directory

The following table describes the tasks required for creating a home directory for each end user and for enabling roaming among HDI systems:

Step	Performed on: (see Figure G-1)	Performed by:	Description
1	HDI-A	CIFS administrator	Create a home directory for each end user immediately under the mount point of the home-directory-roaming file system. To delete the created home-directory, execute the `archdctl` command with the `--del` option specified.
2	HDI-A	CIFS administrator	Set the access privileges for the home directory created in step 1. For details about the access privileges to be set for the home directory, see Table G-1 Access privileges for the home directory on page G-7.
3	HDI-A	CIFS administrator	Create files such as user profiles in the home directory created in step 1. If you want to delete the created file, do so after completing step 5.
4	HDI-A	System administrator	Use the `archdctl` command with the `--roaming` option specified to enable roaming for the home-directory data created in step 1 among HDI systems.
5	HDI-A	System administrator	Use the `archdctl` command with the `--status` option specified to make sure that the roaming for the home-directory data created in step 1 among the HDI systems is enabled.
6	HDI-A	System administrator	Tell the end users to assign a network drive to the share in which the home-directory was created in step 1 before accessing the share.
7	HDI-A	System administrator	Use the GUI to make sure that the migration task for the file system (in which the home-directory was created in step 1) was successful. Also make sure that the successful task was started after the end time of the `archdctl` command executed in step 5.
8	HDI-A	System administrator	Use the GUI to make sure that the system message KAQM37529-E has not been output. If the KAQM37529-E message is output, a conflict occurred between locations during update of the home directory. Recover the home-directory data according to When KAQM37529-E is output to a location where a new home directory was created, or when KAQM37529-E is output even though no new home directory was created and no home directory data was migrated on page H-2. If you recovered the home-directory data, you do not need to perform the following steps. If you recovered the home-directory data, you do not need to perform the following steps.
9	HDI-A	System administrator	Tell end users that, before accessing a share for the home-directory-roaming file system on another HDI

Step	Performed on: (see Figure G-1)	Performed by:	Description
			system, they will need to assign a network drive to the share.

Table G-1 Access privileges for the home directory

The ACL type of the file system	Owner	Name	Permissions	Inheritance	Application destination
Advanced ACL type	Logged-in user	Logged-in user	Full Control	None	This folder and its subfolders and files
Classic ACL type	Logged-in user	Logged-in user	`rwx`	None	This folder only
		Logged-in user's group	`--x`	None	This folder only
		Others (Everyone)	`--x`	None	This folder only

Migrating home-directory data

The following describes the tasks required for migrating data of a home directory (created for each end user) from another file server and for enabling data roaming among HDI systems.

Note: If a large amount of data is migrated to an HDI system that is currently operating at once, the migration might not complete within an hour, and the home directory in another HDI system might remain read-only for a long period of time. Therefore, to migrate a large amount of data at once, provide a separate HDI system as the data migration destination.

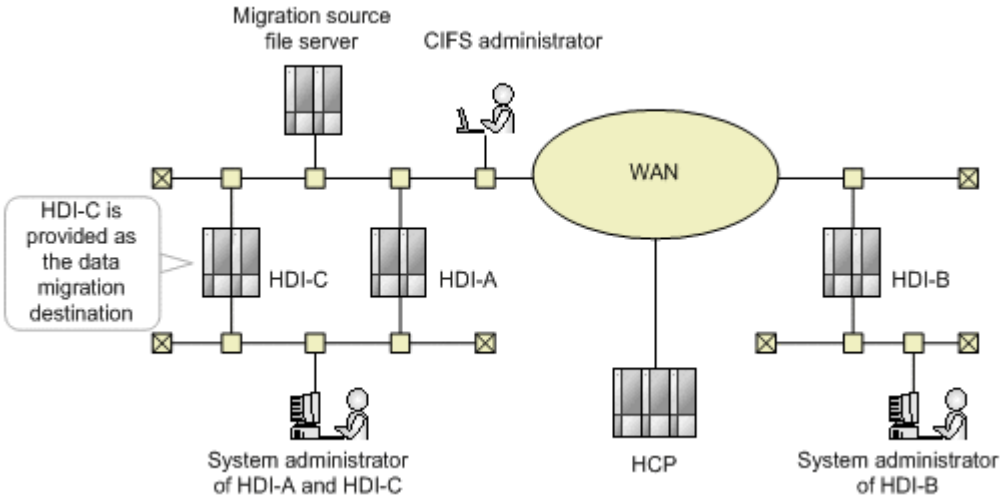


Figure G-2 Operation example of migrating home-directory data to the operating system and enabling roaming among HDI systems

Step	Performed on: (see Figure G-2)	Performed by:	Description
1	HDI-C	System administrator	Provide an HDI system as the data migration destination, and then set up the environment. Use the GUI to log in to the system, and then use the Configuration Wizard to complete all settings. Link with the HCP system and then specify the settings so that all files are migrated. In addition, make sure that the following settings are identical across all the linked HDI systems: • Timestamps of nodes • Settings for client authentication
2	HDI-C	System administrator	Use the GUI or the `fscreate` command to create a home-directory-roaming file system in the HDI system prepared in step 1, and then create a file share. Make sure that the following settings are identical across all the linked HDI systems: • Settings for file systems (such as ACL types, the period to hold the data for past versions, and functions to be used) • Namespace for the migration destinations
3	HDI-C	System administrator	Use the GUI or the `arccancelpolicy` command to disable the schedule of the migration task for the file system created in step 2. During the initial installation, data is migrated every hour. If the metadata of the migrated files and directories is updated by third-party software during data migration, the files and directories with updated

Step	Performed on: (see Figure G-2)	Performed by:	Description
			metadata will be migrated again, and the data migration takes time to complete. Therefore, we recommend that the schedule of the migration task be disabled before starting the migration.
4	HDI-C	CIFS administrator	Use third-party software such as the `robocopy` command to migrate home-directory data from another file server to the file system created in step 2. To delete the home-directory that was migrated, execute the `archdctl` command with the `--del` option specified. If you want to delete the files or directories in the home-directory, do so after completing step 7.
5	HDI-C	CIFS administrator	Make sure that migration of all data was completed.
6	HDI-C	System administrator	Use the `archdctl` command with the `--roaming` option specified to enable roaming for the home-directory data migrated in step 4 among HDI systems.
7	HDI-C	System administrator	Use the `archdctl` command with the `--status` option specified to make sure that the roaming for the home-directory data migrated in step 4 among the HDI systems is enabled.
8	HDI-C	System administrator	If the schedule of the migration task was disabled in step 3, use the GUI or `arcschedulepolicy` command to set the schedule of the migration task again.
9	HDI-C	System administrator	Tell the end users to assign a network drive to the share created in step 2 before accessing the share.
10	HDI-C	System administrator	Use the GUI to make sure that the migration task for the file system created in step 2 was successful. Also make sure that the successful task was started after the end time of the `archdctl` command executed in step 7.
11	HDI-C	System administrator	Use the GUI to make sure that the system message KAQM37529-E has not been output. If the KAQM37529-E message is output, a conflict occurred between locations during update of the home directory. Recover the home-directory data according to If the KAQM37529-E message is output to the location to which home-directory data was migrated on page H-2. If you recovered the home-directory data, you do not need to perform the following steps. If you recovered the home-directory data, you do not need to perform the following steps.
12	HDI-C	System administrator	Tell end users that, before accessing a share for the home-directory-roaming file system on another HDI

Step	Performed on: (see Figure G-2)	Performed by:	Description
			system, they will need to assign a network drive to the share.
13	HDI-C	System administrator	Tell the end users to stop accessing the share created in step 2.
14	HDI-C	System administrator	Use the GUI to stop the CIFS service.
15	HDI-C	System administrator	Use the GUI to change the schedule to immediately execute the migration task for the file system created in step 2.
16	HDI-C	System administrator	Use the GUI to make sure that the migration task executed in step 15 was successful.
17	HDI-C	System administrator	Remove the HDI system provided in step 1.

Recovering the home-directory data whose update caused a conflict

This appendix describes how to recover home-directory data when the data in the home directories created for each end user roams between HDI systems if the data causes a conflict between HDI systems, or the system message KAQM37529 is output.

- When KAQM37529-E is output to a location where a new home directory was created, or when KAQM37529-E is output even though no new home directory was created and no home directory data was migrated
- If the KAQM37529-E message is output to the location to which home-directory data was migrated
- If the KAQM37529-E message is output to a location other than the location where a home directory was created or to which home-directory data was migrated

When KAQM37529-E is output to a location where a new home directory was created, or when KAQM37529-E is output even though no new home directory was created and no home directory data was migrated

The following shows the recovery operations that must be performed when KAQM37529-E is output to a location where a new home directory was created, or when KAQM37529-E is output even though no new home directory was created and no home directory data was migrated:

Here, the location where the KAQM37529-E message is output is referred to as HDI-A, and the other location is referred to as HDI-B.

Step	Performed on:	Performed by:	Description
1	HDI-A	System administrator	Tell the end users to disconnect the network drive assigned to the share for the home-directory-roaming file system and to stop accessing the share, because there is a conflict in the processes to update the home directory.
2	HDI-B	End users	Disconnect the network drive assigned to the share for the home-directory-roaming file system.
3	HDI-A	System administrator	Ask the CIFS administrator of HDI-A to back up the data created in the home-directory to a share that the end users can access.
4	HDI-A	CIFS administrator	Back up the data in the home directory to a share that the end users can access, and then contact the system administrator of HDI-A.
5	HDI-A	System administrator	Execute the `archdctl` command with the `--del` option specified to delete the home directory whose update caused a conflict.
6	HDI-B	System administrator	Tell the end users to assign a network drive to a share in the home-directory-roaming file system of HDI-A or HDI-B, and then to copy the home-directory data manually from the backup destination in step 4.
7	HDI-A or HDI-B	End users	Assign a network drive to the share that was disconnected in step 2, access the share, and then manually copy the data from the data backup location to the home directory. (The system administrator will notify you of the data backup location in step 6.)

If the KAQM37529-E message is output to the location to which home-directory data was migrated

If the KAQM37529-E message is output to the location to which home-directory data was migrated, perform the recovery procedure below.

In this procedure, the location where the KAQM37529-E message is output is referred to as HDI-C, and other locations are referred to as HDI-A and HDI-B.

Step	Performed on:	Performed by:	Description
1	HDI-C	System administrator	Tell the end users to disconnect the network drive assigned to the share for the home-directory-roaming file system and to stop accessing the share, because there is a conflict in the processes to update the home directory.
2	HDI-A HDI-B	End users	Disconnect the network drive assigned to the share for the home-directory-roaming file system.
3	HDI-C	System administrator	Ask the CIFS administrator of HDI-C to stop any data migration processes that use third-party software (such as the `robocopy` command).
4	HDI-C	CIFS administrator	Stop all data migration processes and then contact the system administrator of HDI-C.
5	HDI-C	System administrator	Execute the `archdctl` command with the `--del` option specified to delete the home directory whose update caused a conflict.
6	HDI-C	System administrator	Tell the end users to assign a network drive to the share for the home-directory-roaming file system of HDI-C and then to manually copy the data from another file server to the home directory. If a large amount of data is migrated to an HDI system that is currently operating at once, the migration might not complete within an hour, and the home directory in another HDI system might remain read-only for a long period of time. For this reason, to manually copy data from another file server, prepare and use a different HDI system for the data migration destination.
7	HDI-C	End users	Manually copy data from the other file server to the home directory, and then contact the system administrator of HDI-C.
8	HDI-C	System administrator	Tell the end users to start access after assigning a network drive to a share in the home-directory-roaming file system of an HDI other than HDI-C.
9	HDI-C	System administrator	Tell the end users to stop accessing the share that was mentioned in step 6.
10	HDI-C	System administrator	Use the GUI to stop the CIFS service.
11	HDI-C	System administrator	Use the GUI to change the schedule so that the task to migrate the file system where a conflict in the processes to update the home directory has occurred is executed immediately.
12	HDI-C	System administrator	Use the GUI to make sure that the migration task executed in step 11 was successful.

Step	Performed on:	Performed by:	Description
13	HDI-C	System administrator	Remove the HDI system that was prepared for use as the data migration destination.

If the KAQM37529-E message is output to a location other than the location where a home directory was created or to which home-directory data was migrated

If the KAQM37529-E message is output to a location other than the location where a home directory was created or to which home-directory data was migrated, perform the recovery procedure below.

Here, the location where the KAQM37529-E message is output is referred to as HDI-B, and the other location is referred to as HDI-A and HDI-C.

Step	Performed on:	Performed by:	Description
1	HDI-B	System administrator	Tell the end users to back up the home-directory data to a location other than the share for the home-directory-roaming file system. Then, tell them to disconnect the network drive assigned to the share and to stop accessing the share.
2	HDI-B	End users	Save the home-directory data that exists in the share for the home-directory-roaming file system.
3	HDI-B	End users	Disconnect the network drive assigned to the share for the home-directory-roaming file system, and then contact the system administrator of HDI-B.
4	HDI-B	System administrator	Execute the `archdctl` command with the `--del` option specified to delete the home directory whose update caused a conflict.
5	HDI-A or HDI-C	System administrator	Tell the end users to assign a network drive to the share for the home-directory-roaming file system, and then to start access.
6	HDI-A or HDI-B	End users	Assign a network drive to the share for the home-directory-roaming file system, access the share, and then manually copy the data that was backed up in step 2 to the home directory.

I

Maximum Values for HDI

This appendix describes various maximum values for HDI.

Maximum values

The following table describes various maximum values for HDI:

Table I-1 Various maximum values for HDI

Item	Maximum value		
	Per cluster	Per single-node	Per file system
Number of user LUs that can be allocated	1,024	256	256
Number of file systems	1,024	256	-
Total number of mounted file systems	1,024	256	-
Number of NFS shares	1,024	1,024	-
Number of CIFS shares	The maximum number of CIFS shares depends on whether the settings to apply the CIFS share settings to the CIFS client environment by automatically reloading the settings are enabled in the CIFS service configuration definition. The maximum value also depends on the HDI models. For details about the maximum number of CIFS shares, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.		
File system capacity	-	-	1 PB
Total number of files and directories that can be stored in a file system	-	-	Approximately 4 billion The maximum number of files that can be created differs depending on the path length of a file or the number of files created in a single directory. We recommend keeping the total number of directories and files to be created in a single directory to no more than 10,000.
Number of directories for which quotas can be set	-	-	1,023 Quotas can be set for an unlimited number of users and groups.
Maximum size of a file that can be stored in a file system	-	-	Files other than sparse files: Maximum capacity of the file system (maximum 1 PB) Sparse files: 8 EB (Exabyte) - 1 byte
File system name	-	-	16 characters (1 character is counted as 1 byte)

Item	Maximum value		
	Per cluster	Per single-node	Per file system
Path length of the shared directory (absolute path beginning with /mnt/)	-	-	CIFS share: 256 characters (Note that a UTF-8 multi-byte character is also counted as 1 character. However, a character to which a code used to specify a specific glyph variant (Variation Selector) is added is counted as 2 characters.) NFS share: 63 characters (Note that 1 character is counted as 1 byte.)
Directory name on the share	-	-	CIFS share: 244 characters (Note that a UTF-8 multi-byte character is also counted as 1 character. However, a character to which a code used to specify a specific glyph variant (Variation Selector) is added is counted as 2 characters.) NFS share: 255 bytes (Converted by using the number of bytes when encoded in UTF-8)
File name on the share	-	-	CIFS share: 255 characters (Note that a UTF-8 multi-byte character is also counted as 1 character. However, a character to which a code used to specify a specific glyph variant (Variation Selector) is added is counted as 2 characters.) NFS share: 1,023 bytes (Converted by using the number of bytes when encoded in UTF-8)
File path length on the share (absolute path beginning with /mnt/)	-	-	CIFS share: 259 characters (Note that a UTF-8 multi-byte character is also counted as 1 character. However, a character to which a code used to specify a specific glyph variant (Variation Selector) is added is counted as 2 characters.) NFS share: The length depends on the NFS protocol version to be used. If a value smaller than the

Item	Maximum value		
	Per cluster	Per single-node	Per file system
			value shown below is set as a limit for the file path length for NFS clients, the value set for NFS clients will be valid. • NFSv2: 1,024 bytes • NFSv3 and NFSv4: 4,095 bytes The file path length might be limited depending on the functionality used, such as when the NDMP functionality is used or when linked with HCP. Check the notes for each functionality.

Legend: -: Not applicable

J

Acronyms

This appendix lists the acronyms used in the HDI manuals.

Acronyms used in the HDI manuals

The following acronyms are used in the HDI manuals.

ABE	Access Based Enumeration
ACE	access control entry
ACL	access control list
AES	Advanced Encryption Standard
AJP	Apache JServ Protocol
API	application programming interface
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
BDC	Backup Domain Controller
BMC	baseboard management controller
CA	certificate authority
CHA	channel adapter
CHAP	Challenge-Handshake Authentication Protocol
CIFS	Common Internet File System
CIM	Common Information Model
CLI	command line interface
CPU	central processing unit
CSR	certificate signing request
CSV	comma-separated values
CTL	controller
CU	control unit
CV	custom volume
DACL	discretionary access control list
DAR	Direct Access Recovery
DB	database
DBMS	database management system
DC	domain controller
DDNS	Dynamic Domain Name System
DEP	data execution prevention
DES	Data Encryption Standard
DFS	distributed file system
DHCP	Dynamic Host Configuration Protocol

DIMM	dual in-line memory module
DLL	dynamic-link library
DN	distinguished name
DNS	Domain Name System
DOM	Document Object Model
DOS	Disk Operating System
DRAM	dynamic random access memory
DSA	digital signal algorithm
DTD	Document Type Definition
ECC	error-correcting code
EUC	Extended UNIX Code
FC	Fibre Channel
FC-SP	Fibre Channel - Security Protocol
FIB	forwarding information base
FIFO	First In, First Out
FQDN	fully qualified domain name
FTP	File Transfer Protocol
FV	Fixed Volume
FXP	File Exchange Protocol
GbE	Gigabit Ethernet
GID	group identifier
GMT	Greenwich Mean Time
GPL	GNU General Public License
GUI	graphical user interface
HBA	host bus adapter
H-LUN	host logical unit number
HPFS	High Performance File System
HSSO	HiCommand single sign-on
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	input/output
ICAP	Internet Content Adaptation Protocol
ICMP	Internet Control Message Protocol
ID	identifier

IP	Internet Protocol
IP-SW	IP switch
JDK	Java Development Kit
JIS	Japanese Industrial Standards
JSP	JavaServer Pages
KDC	Key Distribution Center
LACP	Link Aggregation Control Protocol
LAN	local area network
LBA	logical block addressing
LCD	Local Configuration Datastore
LDAP	Lightweight Directory Access Protocol
LDEV	logical device
LDIF	LDAP Data Interchange Format
LDKC	logical disk controller
LED	light-emitting diode
LF	Line Feed
LTS	long term support
LU	logical unit
LUN	logical unit number
LUSE	logical unit size expansion
LVI	Logical Volume Image
LVM	Logical Volume Manager
MAC	Media Access Control
MD5	Message-Digest algorithm 5
MIB	management information base
MMC	Microsoft Management Console
MP	microprocessor
MSS	maximum segment size
MTU	maximum transmission unit
NAS	Network-Attached Storage
NAT	network address translation
NDMP	Network Data Management Protocol
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIC	network interface card

NIS	Network Information Service
NTFS	New Technology File System
NTP	Network Time Protocol
OID	object identifier
ORB	object request broker
OS	operating system
PAP	Password Authentication Protocol
PC	personal computer
PCI	Peripheral Component Interconnect
PDC	Primary Domain Controller
PDU	protocol data unit
PID	process identifier
POSIX	Portable Operating System Interface for UNIX
PP	program product
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
RAM	random access memory
RAS	Reliability Availability Serviceability
RCS	Revision Control System
RD	relational database
RFC	Request for Comments
RID	relative identifier
RPC	remote procedure call
RSA	Rivest, Shamir, and Adleman
SACL	system access control list
SAN	storage area network
SAS	Serial Attached SCSI
SATA	serial ATA
SAX	Simple API for XML
SCSI	Small Computer System Interface
SFTP	SSH File Transfer Protocol
SHA	secure hash algorithm
SID	security identifier
SJIS	Shift JIS
SLPR	Storage Logical Partition

SMB	Server Message Block
SMD5	Salted Message Digest 5
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	service pack
SSD	solid-state drive
SSH	Secure Shell
SSHA	Salted Secure Hash Algorithm
SSL	Secure Sockets Layer
SSO	single sign-on
SVGA	Super Video Graphics Array
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOS	type of service
TTL	time to live
UAC	User Account Control
UDP	User Datagram Protocol
UID	user identifier
UNC	Universal Naming Convention
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
UTF	UCS Transformation Format
VDEV	Virtual Device
VLAN	virtual LAN
VLL	Virtual LVI/LUN
WADL	Web Application Description Language
WAN	wide area network
WINS	Windows Internet Name Service
WORM	Write Once, Read Many
WS	workstation
WWN	World Wide Name
WWW	World Wide Web

XDR	External Data Representation
XFS	extended file system
XML	Extensible Markup Language

Glossary

This glossary explains the terms used in the HDI manuals.

A

ACE
An entry in an ACL. An ACE sets access permissions for directories and files for each user and group. ACE formats differ depending on the ACL type.

ACL
A list of all the ACEs for a particular directory or file. An ACL defines the access permissions for a particular directory or file.

ACL type
The type of file system or file that is supported by the ACL. The ACL types that can be used in HDI systems are the Advanced ACL type (compatible with NTFS ACL), and the Classic ACL type (compatible with POSIX ACL).

Anti-Virus Enabler
A program used to scan, in real time, for viruses in data shared with users via CIFS in an HDI system.

B

Backup Restore
A program used for backing up data in an HDI file system.

backup server
A server that manages backup and restore operations by using backup management software.

| # | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

C

CIFS
A protocol that provides file-sharing services to Windows users.

cluster
A redundant configuration that enables a service to continue when an error occurs or maintenance work is performed.

cluster management LU
An LU that is assigned to a node and stores settings information, such as cluster configuration information and file system information.

command device
A control device used to receive commands that control storage systems.

Configuration Manager
A program used to set up an HDI system and manage file system operations.

D

Data Control
One of the programs on a node OS.

data port
A node port that is used to connect to the front-end LAN.

device file
A user LU. For more information, see *user LU*.

Device Manager
A program that manages disk resources and the hardware configuration of storage systems in an integrated manner.

Dynamic Provisioning
A function that virtually allocates volumes of a given capacity to a host independent of the physical capacity of the storage system.

Dynamic Tiering
This storage system functionality automatically reallocates data based on I/O load.

E

External storage system
A storage system that is connected to by the external storage connection functionality for storage systems (Universal Volume Manager).

F

failback
The relocation of a failed-over resource group back to its original node in the cluster after an error has been recovered on the node or maintenance on the node is complete.

failover
The relocation of a resource group to the other node in a cluster when an error occurs on a node or when maintenance on a node is required. Failovers enable continuous operation of the services provided by an HDI system.

File Sharing
One of the programs on a node OS.

fixed IP address
An IP address set for a specific interface in a node.

front-end LAN
A LAN used by a client to access the data stored in a storage system.

H

HBase 64 Storage Mgmt Common Service
The Web-container service for Hitachi Command Suite Common Component.

HBase 64 Storage Mgmt Web Service
The Web-server service for Hitachi Command Suite Common Component.

heartbeat LAN
A LAN used by each node in a cluster to check the operating status of the other node.

Hitachi Command Suite Common Component
A component that provides functions, such as being able to log in to the GUI, outputting management server integrated logs, and Web services, common to all Hitachi File Services Manager and Hitachi Command Suite products.

Hitachi Content Platform (HCP)
A system used for managing and storing data for long periods of time. File system data created in an HDI system can be migrated to an HCP system.

Hitachi Data Ingestor (HDI)
A system that uses storage systems and nodes to provide a file-sharing service.

Hitachi File Services Manager
A program necessary for system administrator to operate or manage an HDI system from a GUI.

I

incremental backup
Incremental backup is a backup method that targets only data that has changed after the previous backup was performed.

interface
A logical network interface assigned to a port.

L

LDEV
A unit of storage that is created by logically partitioning a storage area within a parity group of a storage system. Although referred to as an *LDEV* in File Services Manager, it is referred to as a *logical unit* (*LU*) in Hitachi AMS2000 series or HUS100 series storage systems.

logical volume
An area created by using a volume manager to divide a volume group into one or more areas. In HDI systems, this area corresponds to a file system created by using the volume manager.

LU
An LDEV that is assigned to a port in a storage system.

LUN
A management number assigned to each LU in a storage system. Although referred to as an *LUN* in File Services Manager, it is referred to as an *H-LUN* in the Hitachi AMS2000 series or HUS100 series storage systems.

LUN Expansion
Functionality for expanding the capacity of an LU by integrating multiple LUs into one.

LVM
A type of volume manager. For more information, see *volume manager*.

M

maintenance personnel
Hitachi engineers who maintain HDI systems.

management console
A computer used by the system administrator to operate File Services Manager.

management LAN
A LAN used by the system administrator to operate and manage an HDI system.

management server
A computer on which Hitachi File Services Manager is installed. The management server can also be used as a management console.

media
Recording media, such as magnetic tape, for storing backed up data.

media server
A server that controls a tape device installed outside the storage system.

N

NFS
A protocol that provides file-sharing services to UNIX users.

node
A device that is connected to a storage system and that is used as a file server. Two nodes make up a cluster.

O

OS disk
A logical disk area in a node, that stores the OS and programs that run on the OS.

P

physical node
A node that makes up part of a processing node.

Primary Server Base
A program that provides Web server functionality.

processing node
A logical group made up of nodes. If nodes are set up in a cluster, the cluster is treated as a processing node.

Q

quota
The maximum block space and maximum number of inodes available to a user. In an HDI system, limits can be set and managed for each file system or each directory.

R

resource group
A management unit used to manage multiple resources (such as NFS share settings, CIFS share settings, file system information, and virtual IP address information) as a group. Services can be started and stopped for each resource group. If an error occurs, failover is performed for each resource group.

S

scan server
A server that scans, via a LAN, CIFS-shared data in an HDI system for viruses.

ShadowImage
A program for replicating user data within a storage system, without using a host.

subtree quota
A quota set for a directory and the users and groups of that directory.

system administrator
A user who manages an HDI system. The system administrator sets up an HDI system and monitors system operations and error information.

system LU
A collective term for the OS disks and the cluster management LU.

T

tape device
A device for storing multiple types of storage media.

target
A unit used to manage multiple LUs as one group so that a node can uniquely recognize the LUs of a storage system.

TrueCopy
A program for replicating user data between two storage systems, without using a host.

trunking
A technology used to create a virtual network interface from a group of ports. HDI allows you to configure a network by using virtual network interfaces that are assembled by using trunking.

U

Universal Replicator
A program that asynchronously reproduces user data between two storage systems without transferring the data via a host.

user LU
A generic term for an LU that is assigned to a node and that stores user data such as file system information. A user LU is also called a *device file* or an *LU* (excluding the system LU).

user LUN
A management number assigned to each user LU. A user LUN is also called a *device file number*.

user mapping
The process of assigning a user ID and group ID to a user registered in a domain controller when the user accesses a CIFS share.

V

virtual IP address
An IP address used by a user when connecting to a service running on a resource group. By using a virtual IP address, the user can continue to use the service even if an error occurs on a node and the resource group fails over to the other properly-running node.

volume group
An area that consists of one or more LUs that have been grouped together by a volume manager. A volume group is made up of one file system.

volume manager
Functionality for volume management. In the HDI system, LVM is used as the volume manager. This functionality enables you to create volume groups combining LUs and to create logical volumes out of volume groups.

W

WORM
An abbreviation for "Write Once, Read Many". The WORM status indicates that data cannot be modified. A file whose status is changed to the WORM status is called a WORM file, and a file system in which any files can be changed to a WORM file is called a WORM file system.

Index

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Hitachi Vantara

Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 95050-2639 USA
www.HitachiVantara.co
community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com