HITACHI
Inspire the Next

Hitachi Data Ingestor
Cluster Troubleshooting Guide

FastFind Links

Product Version

Getting Help

Contents

Hitachi Data Systems

MK-90HDI029-12

Contents

Preface

This manual provides troubleshooting for Hitachi Data Ingestor (HDI) systems.

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

This preface includes the following information:

Intended audience

This manual is intended for the following users:

- System administrators who operate and manage an HDI system.
- End users of 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 5.1.1 or later.

Release notes

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

Organization of HDI manuals

HDI manuals are organized as shown below.

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

Manual name	Description
Hitachi Data Ingestor Installation and	You must read this manual first if you will use an HDI system.

Manual name	Description
Configuration Guide, MK-90HDI002	This manual contains the information that you must be aware of before starting HDI system operation, as well as the environment settings for an external server.
Hitachi Data Ingestor Cluster Getting Started Guide, MK-90HDI001	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 (This manual)	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 Software User Guide*
- *Hitachi Command Suite Software CLI Reference Guide*
- *Hitachi Command Suite Software Messages Guide*
- *Hitachi Command Suite Software Installation and Configuration Guide*

- *Hitachi Command Suite Software Configuration Reference Guide*

Hitachi Content Platform

- *Hitachi Content Platform Administering HCP*
- *Hitachi Content Platform Managing a Tenant and Its Namespaces*
- *Hitachi Content Platform Managing the Default Tenant and Namespace*
- *Hitachi Content Platform Replicating Tenants and Namespaces*
- *Hitachi Content Platform HCP Management API Reference*
- *Hitachi Content Platform Using a Namespace*
- *Hitachi Content Platform Using the Default Namespace*
- *Hitachi Content Platform HCP Metadata Query API Reference*
- *Hitachi Content Platform Searching Namespaces*
- *Hitachi Content Platform Using HCP Data Migrator*
- *Hitachi Content Platform Installing an HCP System*
- *Hitachi Content Platform Third-Party Licenses and Copyrights*
- *Hitachi Content Platform HCP-DM Third-Party Licenses and Copyrights*
- *Hitachi Content Platform Installing an HCP SAIN System - Final On-site Setup*
- *Hitachi Content Platform Installing an HCP RAIN System - Final On-site Setup*

Abbreviation conventions

This manual uses the following abbreviations for product names:

Abbreviation	Full name or meaning
Active Directory	Active Directory(R)
Device Manager	Hitachi Device Manager Software
Dynamic Provisioning	Hitachi Dynamic Provisioning
File Services Manager	A generic name for the following: • Configuration Manager • Hitachi File Services Manager
Firefox	Mozilla Firefox(R)
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

Abbreviation	Full name or meaning
	• Hitachi Unified Storage 110
Internet Explorer	Windows(R) Internet Explorer(R)
Windows	Microsoft(R) Windows(R) Operating System
Windows 7	A generic name for the following: • Microsoft(R) Windows(R) 7 Enterprise • Microsoft(R) Windows(R) 7 Enterprise x64 Edition • Microsoft(R) Windows(R) 7 Professional • Microsoft(R) Windows(R) 7 Professional x64 Edition • Microsoft(R) Windows(R) 7 Ultimate • Microsoft(R) Windows(R) 7 Ultimate x64 Edition
Windows 8	A generic name for the following: • Microsoft(R) Windows(R) 8 32-bit • Microsoft(R) Windows(R) 8 64-bit • Microsoft(R) Windows(R) 8 Enterprise 32-bit • Microsoft(R) Windows(R) 8 Enterprise 64-bit • Microsoft(R) Windows(R) 8 Pro 32-bit • Microsoft(R) Windows(R) 8 Pro 64-bit
Windows NT	Microsoft(R) Windows NT(R) Server Network Operating System
Windows Server 2003	A generic name for the following: • Microsoft(R) Windows Server(R) 2003, Datacenter Edition Operating System • Microsoft(R) Windows Server(R) 2003, Enterprise Edition Operating System • Microsoft(R) Windows Server(R) 2003, Standard Edition Operating System • Microsoft(R) Windows Server(R) 2003, Web Edition Operating System
Windows Server 2012	A generic name for the following: • Microsoft(R) Windows Server(R) 2012 Datacenter • Microsoft(R) Windows Server(R) 2012 Standard

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click **OK**.

Convention	Description
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`
[ ] square brackets	Indicates optional values. Example: `[ a | b ]` indicates that you can choose a, b, or nothing.
`...`	The item or items preceding the ellipsis (`...`) can be repeated. To specify multiple items, use a comma (`,`) to delimit them. Example: `A,B...` indicates that `B` can be specified as many times as necessary after `A`.

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

Icon	Label	Description
	Note	Calls attention to important and/or additional information.

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

Getting help

The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week. If you need technical support, log on to the Hitachi Data Systems Portal for contact information: https://portal.hds.com

Comments

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

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

1

General procedure for troubleshooting

This chapter provides the procedure for identifying the cause and location of an error when an error occurs in a Hitachi Data Ingestor (HDI) system.

If you cannot identify the cause of an error, or if you find in the course of investigation that a failover has occurred, contact maintenance personnel.

Overview of troubleshooting

If you have confirmed that an error has occurred in the HDI system, first disable the periodic saving of system configuration information if the GUI or commands are available. Then, after refreshing the management server database, identify the cause of the error, and then recover the system from the error.

The figure below illustrates the general procedure for troubleshooting.

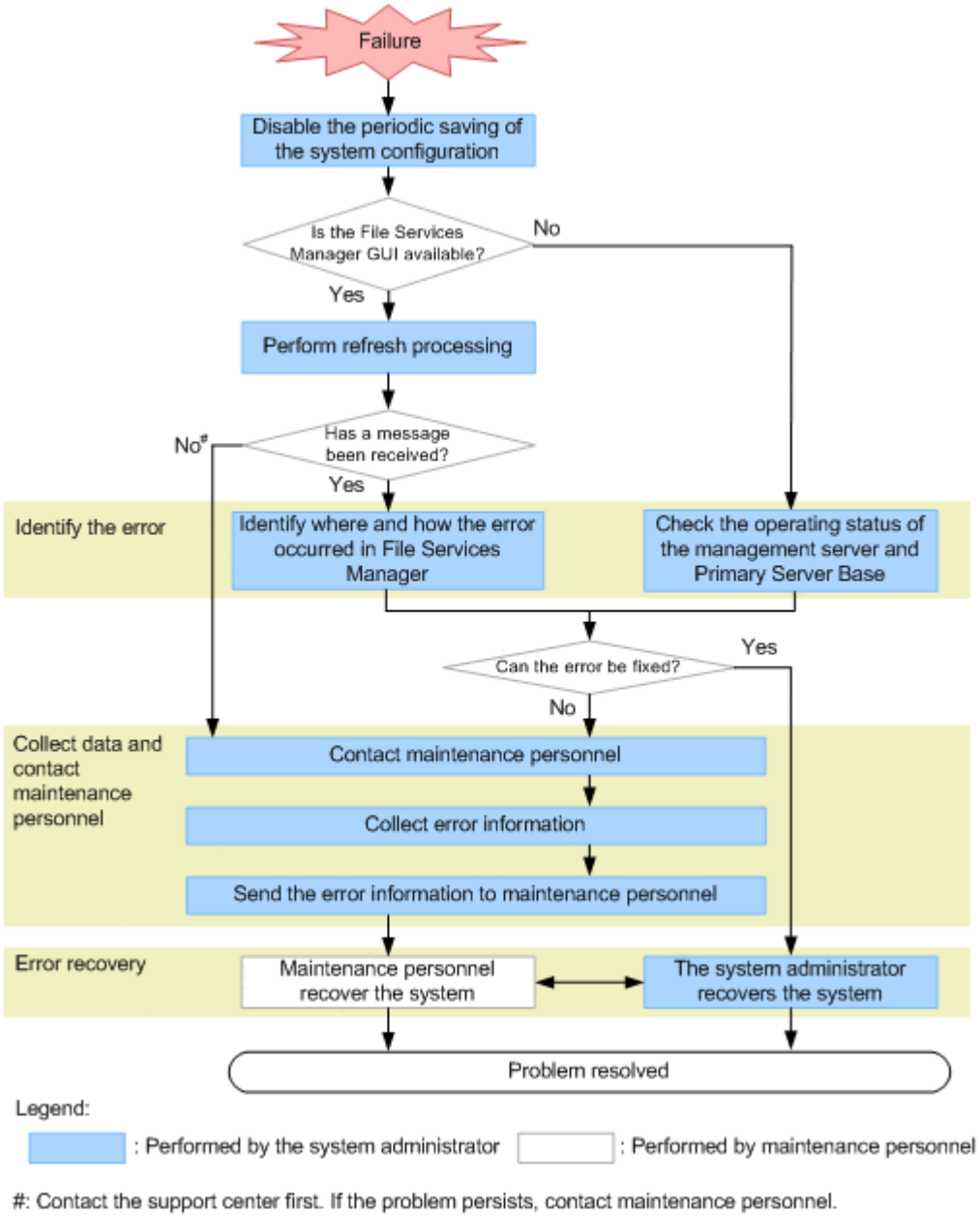

Figure 1-1 General procedure for troubleshooting

Identifying the error

Check the error information to identify the cause of the error. If a failover resulted from the error, contact the maintenance personnel immediately.

Related items

- If a file system cannot be used on page 1-4
- If the File Services Manager GUI does not work correctly on page 1-7
- If the Backup Restore functionality ends with an error on page 1-9
- Chapter 2, Identifying the Cause of an Error on page 2-1

Collecting data and contacting the maintenance personnel

In the event of a problem that you cannot fix or whose cause you cannot identify, collect the error information and send it to the maintenance personnel. For details about collecting error information, see Chapter 3, Collecting Data and Contacting Maintenance Personnel on page 3-1.

Error recovery

When you know what caused the error, take the recovery action indicated by the error message. Depending on the type of error, you might need to recover from the error in consultation with the maintenance personnel. For details about restoring the system after an error, see Chapter 4, Error Recovery on page 4-1.

After error recovery, re-enable the periodic saving of system configuration information as required.

When an HDI system is connected to a remote HCP system over a network, the HDI service might become unavailable, even if there are no problems with the HDI system. This problem occurs because the HCP system cannot be accessed. To resolve this problem, see Recovering from an HCP access failure on page 4-20.

The flow chart below illustrates the steps to take when an HDI system cannot access an HCP system.

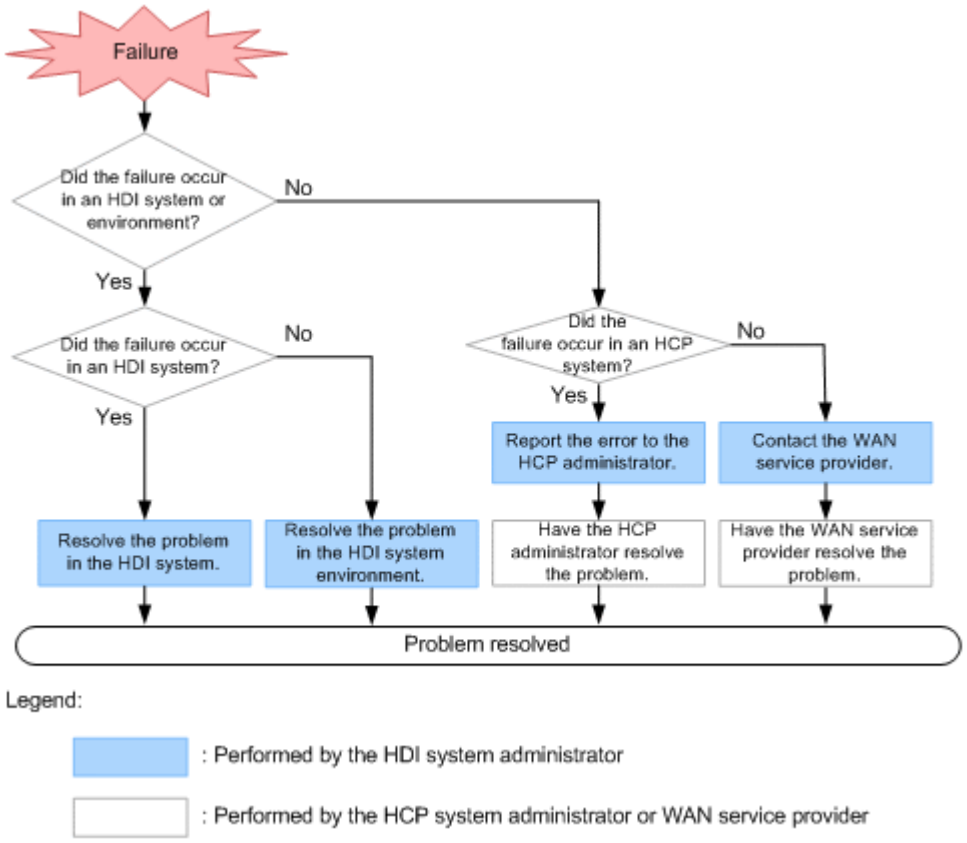

Figure 1-2 General troubleshooting procedure to follow when an HDI system is connected to a remote HCP system over a network and the HDI system fails to access the HCP system

If a file system cannot be used

This subsection describes how a system administrator can identify the cause of an error if an end user cannot use HDI services, such as file shares.

If files cannot be created even though there is free capacity, take action according to When files or directories cannot be created even though there is free capacity on page 4-16.

To identify the cause and location of an error after an end user reports the error

1. Receive a report from the end user that the file share service has stopped.

   The system administrator needs to check whether the file share used by the end user is an NFS share or a CIFS share.

   If an NFS share is stopped:

   The system administrator needs to check the virtual IP address and shared directory name for the stopped service with the end user, to determine the cluster, node, resource group, file system, or directory.

If a CIFS share is stopped:

The system administrator needs to check the shared path name for the stopped service (*node-host-name**CIFS-share-name**directory-path-used*) with the end user, to determine the cluster, node, resource group, file system, or folder.

If you are using user mapping, review the mapping information to make sure that user IDs and group IDs have been assigned correctly to those users who cannot use the service. For details, see Checking user mapping information on page 2-11.

When a resource group is migrated due to failover or failback, even if the failover or failback succeeds, services for the CIFS share using the migrated resource group will be forced to end. For notes on using a file system from a CIFS client, see the *Installation and Configuration Guide*.

2. Make sure that the nodes, the switch, and the storage system are turned on.

   If they are turned off, turn them on, and then check whether the end user can use services of the HDI system.

   Use the `arccorrection` command to rebuild the archive information (the management information for data migrated to the HCP system) as necessary.

3. Check the system messages on the node.

4. Check the access suppression status for the file system.

   Access from end users to the file system is temporarily suppressed while the file system is being expanded or the unused area of virtual LUs is being released. The file system is released from suppression when the operation terminates.

5. In the **Browse Cluster Status** page of the **Cluster Management** dialog box, check the error information of the cluster, node, and resource group.

   In the **Browse Cluster Status** page of File Services Manager, refer to the status of the cluster determined in step 1 to check whether an error occurred in the failover function.

6. In the **List of Services** page of the **Access Protocol Configuration** dialog box, check the service operation status.

   If an error did not occur in the failover function, then the service might have stopped. In the **Browse Cluster Status** (for `Resource group status`) page of the **Cluster Management** dialog box, see the **Running node** to check the node allocated to the resource group used by the end user.

   Then, in the **List of Services** page of File Services Manager, check the operation status of the service used by the end user.

7. In the **File Systems** tab of the *physical-node* subwindow, check the file system error information.

   If the service used by the end user is running and an error did not occur in the service, then an error might have occurred in the file system. See the **File Systems** tab of the File Services Manager's *physical-node*

subwindow to check the status of the file system determined in step 1 above.

8. In the **Shares** tab of the *physical-node* subwindow, check the settings of the file share.

   If the file system is properly mounted and an error did not occur in the file system, see the **Shares** tab in the File Services Manager's *physical-node* subwindow to check the settings of the file share used by the end user.

   If the tab does not display an NFS share for which a host name or net group name has been specified, the system might not be able to resolve the host name or there might be a problem with the connection with one of the following servers:

   - DNS server
   - NIS server
   - WINS server

   For details about how to check the connection to the servers, see Checking for a possible server connection problem on page 2-15. Also check the settings for the NIS server and DNS server in the **DNS, NIS, LDAP Setup** page of the **Network & System Configuration** dialog box.

9. Check the operating environment for the network and clients.

   If the file share is displayed and an error did not occur in the file share, verify whether the operating environment for the network and clients is okay.

   The operating environment for the network

   Check the configuration and operating status of the network connecting the nodes and clients.

   When link down occurs in a port connected to the network, a failover also occurs. However, if link down occurs on both nodes due to failure in a switch or cable, the failover is suppressed. For details about checking error information about ports, see Using interface and network error information for error recovery on page 4-36.

   Also check the connection between the nodes and the following servers:

   - DNS server
   - NIS server
   - LDAP server for user authentication
   - LDAP server for user mapping
   - CIFS client authentication server (domain controller or Windows NT server)
   - NFS client authentication server (KDC server)

   For details about how to check the connection to the servers, see Checking for a possible server connection problem on page 2-15.

   The operating environment for the client

If the operating environment of the client does not meet the usage conditions for the file system provided by the HDI system, file share services might become unusable when failover or failback occurs.

For details about the operating environment for clients that use file systems provided by the HDI system, see the *Installation and Configuration Guide*.

10. From the client computer of the end user who cannot use services, use the `ping` command to check the connection status for the virtual IP addresses of the nodes.

    If a node responds:

    An error might have occurred in the OS. Contact maintenance personnel.

    If a node does not respond:

    A network error might exist on the route between the client computer of the end user who cannot use services and the node. Check whether the IP address settings are correct, and contact the network administrator. If there is no error in the network, contact maintenance personnel.

11. If data is migrated to an HCP system, check whether a failure occurred in the HCP system.

    If a failure occurred on the HCP system, an attempt to access a file that has been migrated to the HCP system might result in an error. Check to see if the `KAQM37070-E` message or the `KAQM37094-E` message has been output. If either of these messages has been output, ask the HCP administrator to resolve the problem with the HCP system.

    If the HDI system is connected to the remote HCP system over a network, take action according to Recovering from an HCP access failure on page 4-20.

If you cannot identify the cause of an error from the above procedure, contact maintenance personnel.

If the File Services Manager GUI does not work correctly

If the File Services Manager GUI does not work correctly, identify the cause by performing the steps described below.

Recommendation: If you are not using SNMP or email notifications and an error that disables the File Services Manager GUI occurs, you will not be able to examine the error information. We therefore recommend that you use File Services Manager in conjunction with SNMP or email notifications.

To identify the cause of this type of error

1. From the management console, verify the following:
   - JavaScript is enabled.
   - Cookies are enabled.

If there are no problems with the above settings, see Appendix D, Troubleshooting Examples on page D-1, and take appropriate action.

2. Check that the management server is running normally.
   Check that the machine and OS are running normally.
3. Check that Hitachi Command Suite Common Component is running normally.
   If you are using Windows 7 or an earlier Windows version, choose **Start**, **Programs**, **Hitachi Command Suite**, **File Services Manager**, and then **Status - HFSM**.
   If you are using Windows 8 or Windows Server 2012, select **Status - HFSM** from the application list in the Start screen.
4. Use the `nasping` command to check the network connection.
   If you receive a response error, check the following:
   - The LAN cables are connected.
   - The nodes are attached correctly.
   - The power of the nodes, switches, and storage system is on.
   - The management LAN and heartbeat LAN connections are properly set up.

   In addition to the above cases, you might receive a response error when there is an error in the network configuration. In this case, from one of the nodes that make up the cluster, on which the GUI works normally, you need to check the **List of Interfaces** page in the **Network & System Configuration** dialog box and then recover from the error. For details about how to recover from an error, see Using interface and network error information for error recovery on page 4-36.
5. Check the Primary Server Base operating status.
   If there is an error in the Web server function of Primary Server Base, the error might be temporary. Wait for about 5 minutes, and then operate the GUI to check whether the following events occur:
   - A KAQM23101-E or KAQM23102-E message is displayed.
   - The dialog box cannot be opened from the **Settings** tab of the *physical-node* subwindow.

   Even if an error occurs in the Web server function of Primary Server Base, file share services for users will not stop.
6. If SNMP is set, use the SNMP manager to check whether an SNMP trap has been issued.
   If email notifications are enabled, check whether error information emails are being received.
7. If you cannot identify the cause of the error, collect the following log files, and then contact maintenance personnel:
   - All the node log data#
   - Management server log files

   #: Depending on the error condition, the system administrator might not be able to collect these log files.

For details about how to collect log files, see Chapter 3, Collecting Data and Contacting Maintenance Personnel on page 3-1.

If the Backup Restore functionality ends with an error

If the Backup Restore ends with an error, check if an error message was output immediately before execution ended, and then identify the site where the error occurred, and its cause.

To identify the cause of an error that occurred during the execution of one of the above functionality, check the following items.

Table 1-1 Items to check when the Backup Restore functionality ends with an error

Items to check	See
Error messages displayed in the GUI	Checking error messages displayed in the GUI or standard error output on page 2-3
Error messages displayed in the standard error output	Checking error messages displayed in the GUI or standard error output on page 2-3
System messages	Checking system messages on the node on page 2-3
Checking the status of a cluster, node, or resource group	Checking the status of a cluster, node, or resource group on page 2-4
Error status of the file system	Checking the error status of a file system on page 2-10
Operating status of the management server	Checking the operating status of the management server on page 2-14
Status of the hardware on the node	Checking the hardware status on page 2-17
Settings and status of the backup management software	Checking the backup management software status and settings on page 2-20
Status of the OS on the other node that connects to the same tape device	Checking the status of the OS on the other node when the other node is connected to the same tape device on page 2-21
Status of the tape device connected to the node via a SAN	Checking the status of the tape device connected to a node via a SAN on page 2-21

2

Identifying the Cause of an Error

This chapter explains how to check the error information and how to identify the cause of an error.

An end user might notify a system administrator that services of the HDI system are unavailable before the system administrator detects the error. For details about identifying the cause of the error in this situation, see If a file system cannot be used on page 1-4.

If you find in the course of investigation that a failover has occurred, contact maintenance personnel.

- ☐ Checking the communication of the management ports and the BMC ports
- ☐ Checking for a possible NTP time synchronization problem
- ☐ Checking the backup management software status and settings
- ☐ Checking the status of the OS on the other node when the other node is connected to the same tape device
- ☐ Checking the status of the tape device connected to a node via a SAN

Checking error messages displayed in the GUI or standard error output

If an error caused by a GUI operation occurs, an error message is displayed in the GUI. If an error caused by a command operation occurs, an error message is output to the standard error output. The system administrator needs to check the output error message to identify the cause of an error.

Check the displayed error message to identify the cause of the problem.

For details about the error messages output, see the manual *Error Codes*.

Checking system messages on the node

Important messages about errors that occurred in the hardware and software are output to the system message log.

In the event of an error, check the system messages in the **List of RAS Information** page (for `List of messages`) of the **Check for Errors** dialog box to find out where and why the error occurred.

From the system message ID, you can identify the program in which the error occurred. From the message text, you can see what caused the error.

If you cannot identify the cause of the error from the system messages, or if a message advises you to contact the maintenance personnel, download the error information and forward it to the maintenance personnel.

System messages consist of a message ID and message text.

The message ID format is as follows:

KA$X^1X^2Y^1Y^2Y^3Y^4Y^5$-Z

X^1X^2

A symbol representing the program that produced the message. The meaning is as follows:

QB: Backup Restore

QG: File Sharing

QK, QM: File Services Manager

QV: Anti-Virus Enabler

$Y^1Y^2Y^3Y^4Y^5$

A number representing the message type.

Z

A symbol representing the message level. The meaning is as follows:

E: Error level

I: Information level

W: Warning level

Q: Query level

The message IDs KAQG70000 to KAQG72999 indicate a message related to the failover functionality.

Even if the system outputs a message reporting that failover was successful, you must still recover from the error that triggered the failover. Check the system messages to identify the error cause.

If the system outputs a message that failover was unsuccessful, you must recover from the error that triggered the failover, and identify and remedy the cause of the unsuccessful failover. For details about how to identify the cause of an error that occurred in the failover functionality, see Checking the status of a cluster, node, or resource group on page 2-4.

If there is a problem with heartbeat communication between the two nodes, either the `KAQG72012-W` message or the `KAQG72013-W` message is output. In such a case, a failover might fail to be performed, or the displayed cluster status might not be correct. The main heartbeat communication path uses the heartbeat ports, and the sub heartbeat communication path uses the management ports. Check whether there is a problem with the heartbeat ports or the management ports.

If name resolution for the public destination host for an NFS share fails when the resource group starts or a failover occurs, the system message `KAQG72021-W` is output on a node. In this case, a client that uses the public destination host cannot access the HDI system.

Checking the status of a cluster, node, or resource group

You can check the status of the cluster, nodes, and resource groups in the **Browse Cluster Status** page of the **Cluster Management** dialog box.

For details about how to recover the system from an error based on the confirmed status of the cluster, node, or resource group, see Viewing error information for the cluster, nodes, and resource groups and taking recovery action on page 4-3.

System administrators can identify the cause of the error in the failover functionality by checking the system messages displayed before or after the time when the error occurred, and by checking the error status displayed in the **Browse Cluster Status** page.

If an error occurred in the system, the status of clusters and nodes might not be displayed in the **Browse Cluster Status** page of the **Cluster Management** dialog box. When such status cannot be displayed in the **Browse Cluster Status** page, the system administrator must collect the error information and contact the maintenance personnel.

You can view the status of a cluster in **Cluster status** in the **Browse Cluster Status** page (for `Cluster / Node status`). The table below lists the cluster statuses displayed in this page and the causes that generate each status.

Table 2-1 Cluster statuses and causes for display

Cluster status	Description	Causes for status display			
		Normal	Hardware error	Software error	User error
ACTIVE	Running normally.	Yes	N/A	N/A	N/A
INACTIVE	Stopped.	Yes	N/A	N/A	Yes
UNKNOWN	Status unknown.	Yes	Yes	Yes	Yes
DISABLE	The failover functionality is disabled due to an error.	N/A	Yes	Yes	N/A
Note: Yes = Applicable. N/A = Not applicable.					

You can view the status of a node in **Node status** in the **Browse Cluster Status** page (for `Cluster / Node status`). The following table lists the node statuses displayed in this page and the causes that generate each status.

Table 2-2 Node statuses and causes for display

Node status	Description	Causes for status display			
		Normal	Hardware error	Software error	User error
UP	Running normally.	Yes	N/A	N/A	N/A
INACTIVE	Stopped.	Yes	N/A	N/A	N/A
DOWN	The OS ended abnormally and the node is stopped.	N/A	Yes	Yes	N/A
UNKNOWN	Status unknown.	Yes	Yes	Yes	Yes
Note: Yes = Applicable. N/A = Not applicable.					

You can view the status of a resource group in **Resource group status** in the **Browse Cluster Status** page (for `Resource group status`). The resource group status and error information are displayed in the following form:

resource-group-status/error-information

The table below lists the resource group statuses displayed in this page and the causes that generate each status.

Table 2-3 Resource group statuses and causes for display

Resource group status	Description	Causes for status display			
		Normal	Hardware error	Software error	User error
Online	Running normally.	Err info	Err info	Err info	Err info
Online Maintenance	Automatic failover is not possible because monitoring is disabled.	Err info	Err info	Err info	Err info
Online Pending	Starting.	Yes	N/A	N/A	N/A
Online Ready#	The resource group cannot start because the cluster is inactive, or the service is not running normally because an error occurred while the cluster was stopping. If the status of the resource group does not change even after the cluster has been started, restart the OS by performing the recovery procedure 6 described in Viewing error information for the cluster, nodes, and resource groups and taking recovery action on page 4-3.	Yes	N/A	Yes	Yes
Offline#	Stopped.	Err info	Err info	Err info	Err info
Offline Pending	Stopping.	Yes	N/A	N/A	N/A
Discovery (exclusivity)	Starting.	Yes	N/A	N/A	N/A
Initializing	Starting.	Yes	N/A	N/A	N/A
Internal Error	Internal error detected. Contact the maintenance personnel.	N/A	Yes	Yes	N/A

Note: Yes = Applicable. N/A = Not applicable. Err info = The displayed message corresponds to the resource group error information.

#: Also displayed when the cluster status is DISABLE. If Online Ready or Offline appears as the resource group status, check the status of the cluster in the **Browse Cluster Status** page (for Cluster / Node status).

The following table lists the resource group error information displayed in the **Browse Cluster Status** page (for `Resource group status`) and the causes that generate the error information.

Table 2-4 Resource group error information and reasons for display

Error information	Description	Causes for error information display			
		Normal	Hardware error	Software error	User error
`No error`	No error occurred.	Yes	N/A	N/A	N/A
`Internal error - not recoverable`	An unrecoverable internal error was detected.	N/A	Yes	Yes	N/A
`Monitor activity unknown`	An error occurred in processing during monitoring or outside the monitoring scope.	N/A	N/A	Yes	N/A
`No available nodes or No available nodes in failure domain after monitor failure`	An error occurred but a failover could not be performed because it is already in a failover status.	Yes	N/A	N/A	Yes
`Node unknown`	The resource group cannot start because the **Node status** of the node is `UNKNOWN`.	N/A	Yes	Yes	Yes
`Split resource group (exclusivity)`	The duplicate resource group is active within the cluster. Perform a forced stop for the cluster, and then restart the OS on both nodes.	N/A	N/A	Yes	Yes
`srmd executable error`	An error occurred during start or stop processing.	N/A	Yes	Yes	N/A
Note: Yes = Applicable. N/A = Not applicable.					

Errors in the failover functionality can be classified as follows:

- Errors at OS startup
- Errors at cluster operation
- Errors triggering a failover
- Errors at unsuccessful failover
- Errors that made the services unavailable

The steps you should take to identify what caused the error depend on the particular situation, as described below.

Identifying errors at OS startup

An error at OS startup might cause a communication failure between the nodes in the cluster. In this case, the status of the cluster and nodes is shown as `UNKNOWN` in the **Browse Cluster Status** page (for `Cluster / Node status`) of the **Cluster Management** dialog box, and the services fail to start.

If an error occurs during startup of the OS, any of the following system messages might have been output on the node:

- KAQG72006-E
- KAQG72007-E
- KAQG72008-E
- KAQG72009-E
- KAQG72018-E

The system administrator needs to check the system messages to identify the cause of the error.

All the file systems are mounted when the OS starts and the services start. If there are a large number of file systems, the activation process of the OS and the startup process for the services can take a long time. By making a note of the standard time taken for services to start after you boot the OS, you will be able to quickly identify any problems that might occur.

If services have not started within the standard time after OS startup, check the status of the cluster and nodes in the **Browse Cluster Status** page (for `Cluster / Node status`) to identify the problem.

If you performed a planned shutdown of the entire HDI system by turning off the power to the nodes, services will automatically start when the power is restored. However, if you have performed a planned shutdown (turning off the power) of the nodes in any of the following conditions, services will not automatically start even when the power is restored:

- The cluster or node is stopped.
- The resource group is stopped.

Identifying errors at cluster operation

If a cluster operation fails due to an error, error information is displayed for the affected cluster, nodes, or resource group in the **Browse Cluster Status** page of the **Cluster Management** dialog box.

The main types of cluster operations you might need to perform are:

- Operating on the status of a cluster, node, or resource group in the **Browse Cluster Status** page

- Adding or deleting a file system
- Adding or releasing a file share
- Changing a node name or cluster name
- Adding, changing, or deleting a virtual IP address

In the HDI system, services are stopped and failover is not performed if the same error is likely to recur and disrupt services after failover. In this case, any attempt to move the resource group to the other node in the cluster without first fixing the error will fail. Also, if you attempt to mount a file system that cannot be used in the HDI system or the file system creation is unsuccessful, any cluster operations will fail.

If services stop when you attempt a cluster operation, check the status of the cluster, nodes, and resource groups in the **Browse Cluster Status** pages and identify the cause of the error.

If an error occurs during a cluster operation, any of the following system messages might have been output on a node:

- KAQG72006-E
- KAQG72007-E
- KAQG72008-E
- KAQG72009-E
- KAQG72018-E

The system administrator needs to check the system messages to identify the cause of the error.

Identifying errors triggering a failover

After a successful failover, if you keep the system running in a failover state without fixing the errors, access performance will decline and any subsequent errors might cause services to stop. You must fix an error that triggers a failover and return to normal operation as soon as possible.

If the system message KAQG70000-E has been output on a node, one of the following errors might have caused the failover:

- An error occurred on the management LAN or the front-end LAN.
- An error occurred that caused the OS on the other node to stop.
- A power failure occurred on the other node, or failures occurred on both the heartbeat LAN and the management LAN.

If the message KAQG70000-E has been output, check the messages output before and after the message, and identify the error.

If the KAQG72026-E message is output, then the power might have been cut to the other node, or failures might have occurred on both the heartbeat LAN and the management LAN. In such a case, the OS on one of the nodes has been restarted, and the resource group on the node has been forcibly failed over to and is running on the other node. Contact maintenance personnel to resolve the problem.

Identifying errors at an unsuccessful failover

If an error occurs in a failover, the failover will be unsuccessful and the provided services will stop. Before recovering from the failover error, you must first recover from the original problem that triggered the failover and restart the services. For details about how to identify the error that caused the failover, see Identifying errors triggering a failover on page 2-9.

If the system message KAQG71000-E (the message that informs the user of the failing failover) has been output on a node, check the following messages to identify the cause of the error:

- KAQG72000-E
- KAQG72001-E
- KAQG72002-E
- KAQG72003-E
- KAQG72004-E
- KAQG72005-E

Also, any of the following system messages might be output on a node:

- KAQG72006-E
- KAQG72007-E
- KAQG72009-E

If a hardware failure occurs in an LU that is shared by both nodes, the KAQG10012-E message might be output to the failover destination node as well.

The system administrator needs to check the messages to identify the cause of the error.

Identifying errors when the services have become unavailable

The daemons that constitute the failover functionality restart automatically if anything causes them to stop. Each daemon might output core files and stop.

If an error has disabled services, open the **List of RAS Information** page (for `List of Core Files`) of the **Check for Errors** dialog box and check core files of which services are generated and whether multiple core files for a certain service are generated.

Checking the error status of a file system

If an error occurs in a file system, from the **File Systems** tab of the *physical-node* subwindow, the system administrator needs to check the status of the file system, and then take corrective action.

When **Online (RW)** is displayed

The file system is mounted with both read and write operations permitted.

When **Online (RO)** is displayed

The file system is mounted as read-only.

When **Unmounted** is displayed

The file system is unmounted.

When **Expanding** is displayed

The file system is being expanded or an error occurred during expansion processing. Wait a while, and then refresh the processing node information. If the status does not change, an error might have occurred during processing. Acquire all the log data, and then contact maintenance personnel.

When **Reclaiming** is displayed

The unused area of virtual LUs that are being used by the file system is being released.

When **Data corrupted** is displayed

The file system is blocked due to insufficient pool capacity or an error in the OS.

See Recovering from file system errors on page 4-15, and then take corrective action.

When **Device error** is displayed

The file system is blocked due to an error in the LU (multiple drive failure).

See Recovering from file system errors on page 4-15, and then take corrective action.

The system administrator needs to determine the cause of the error by using the **Check for Errors** dialog box to display the **List of RAS Information** page (for `List of messages`) and check the system messages around the time that the error occurred. Take action according to the cause of the error as described in Recovering from file system errors on page 4-15.

Checking user mapping information

If an end user is unable to use the CIFS service in an environment where user mapping is enabled, user IDs and group IDs might not have been assigned correctly. In this case, the system administrator needs to check that:

- CIFS service configuration definitions are the same on both nodes

  In the **CIFS Service Maintenance** page of the **Access Protocol Configuration** dialog box, check whether the CIFS service configuration definitions have been applied the same on both nodes.
- The CIFS service is operating correctly

  In the **List of Services** page of the **Access Protocol Configuration** dialog box, make sure the **Status** of the CIFS service is **Running**.
- The nodes are connected to the domain controller

In the **CIFS Service Maintenance** page of the **Access Protocol Configuration** dialog box, make sure the **DC server connection status** is **Connectable**.

- A trust has been established between the domains

  Verify whether a trust has been established between the registered domains. For example, if you use Windows Server 2003 as the domain controller, you can check for a trust relationship by using Windows administrative tools.

- The latest user information has been applied

  If an end user accesses a CIFS share immediately after the user or the group information managed by a domain controller is changed, old user mapping information that has been cached might be applied.

  If a system administrator makes a change to the user or the group information managed by a domain controller (such as re-creating a user), the system administrator must restart the CIFS service or inform end users that the CIFS share must not be accessed for five minutes, to refresh the information.

If no particular problems are found, the system administrator must perform either of the following tasks:

- Delete the cached user mapping information in the **CIFS Service Maintenance** page of the **Access Protocol Configuration** dialog box.
- Inform end users that the CIFS share must not be accessed for five minutes

Depending on the user mapping method you are using, also check the following requirements.

User mapping using RIDs

Check the following requirements when user mapping uses RIDs:

- The domains to which users of the CIFS service belong have been set in File Services Manager.

  Users who belong to a domain that is in a direct trust relationship with the domain that the node belongs to, but is not set up in File Services Manager, will be unable to use the CIFS service provided by the HDI system.

  Make sure that the domain has been set up under **User mapping information** in the **CIFS Service Maintenance** page of the **Access Protocol Configuration** dialog box.

- The IDs of the users and groups who will use the CIFS service fall within the range of valid user IDs and group IDs that you set for each domain.

  Users whose user ID or group ID falls outside the range specified under **User mapping setup** in the **CIFS Service Management** page (**Setting Type**: `User mapping`) of the **Access Protocol Configuration** dialog box will be unable to use the CIFS service.

  When using File Services Manager commands, check that the user or group name can be converted to an ID mapped using RIDs.

User mapping using LDAP

Check the following requirements when user mapping uses LDAP:

- The LDAP server is operating correctly.
  Check whether the LDAP server set in the **CIFS Service Management** page (**Setting Type**: `User mapping`) of the **Access Protocol Configuration** dialog box is operating correctly.
- The highest value of the assigned user IDs and group IDs is within the specified range of the user ID or group ID (when user IDs and group IDs are assigned automatically).
  From the **List of RAS Information** page (for `Batch-download`) of the **Check for Errors** dialog box, download a group of user mapping information logs in a batch operation, and then check whether a user ID or group ID is assigned to an end user that cannot use the CIFS service. If there are no IDs that are assigned to end users that cannot use the CIFS service, in the **CIFS Service Maintenance** page of the **Access Protocol Configuration** dialog box, make sure that the values displayed in **Largest currently used UID** and **Largest currently used GID** are not the same as the largest values of IDs displayed in **Range of UIDs** and **Range of GIDs**.
- User IDs and group IDs are correctly assigned (when user IDs and group IDs are assigned manually).
  From the **List of RAS Information** page (for `Batch-download`) of the **Check for Errors** dialog box, download a group of user mapping information logs in a batch operation, and then check whether user IDs or group IDs are assigned within the range from 200 to 2147483147 to the end users who cannot use the CIFS service.

User mapping using the Active Directory schema

Check the following requirements when user mapping uses the Active Directory schema:

- The Active Directory of the domain controller is operating correctly.
  Check whether the Active Directory schema and configuration files used by all the domain controllers (including ones that are in a redundant configuration) are correct.
- User IDs and group IDs are correctly assigned.
  Check whether user IDs or group IDs are assigned, on the domain controllers, within the range from 200 to 2147483147 to end users that cannot use the CIFS service.
- The domains that have a trust relationship with the domain that the node is joined to are defined.
  Check the list of the domains that have a trust relationship. Redefine the domain if the domains are not displayed.

Checking the operating status of the management server

Check the operating status of the management server, the log files output to the management server, and the network status. If an error has occurred on the management server, check the Hitachi Command Suite Common Component and Hitachi File Services Manager log files to identify the cause of the error.

The table below lists and describes the Hitachi Command Suite Common Component and Hitachi File Services Manager log files.

Table 2-5 Log files of Hitachi Command Suite Common Component and Hitachi File Services Manager

Log file		Output destination	Description
Hitachi Command Suite Common Component log	Integrated trace log file	*system-drive*\Program Files\Hitachi\HNTRLib2\spool\hntr2*n*.log	Important Hitachi File Services Manager trace log data is output to the integrated trace log file. If Hitachi Command Suite products are installed on the management server, trace log data for those products will also be output.
	Event log	Event viewer	Important Hitachi File Services Manager message log data is output to the event log file. If Hitachi Command Suite products are installed on the management server, log data for those products will also be output.
Hitachi File Services Manager log	Message log	*Hitachi-File-Services-Manager-installation-folder*\logs\HFSM_Message*n*.log	Hitachi File Services Manager messages are output to the message log file. The system administrator's operation history is recorded.

Information is output to the integrated trace log file and Hitachi File Services Manager message log in the following format:

```
serial-number date time program-name process-ID thread-ID message-ID event-type message-text
```

The table below indicates the information output to the integrated trace log file and Hitachi File Services Manager server message log file.

Table 2-6 Information output to the integrated trace log file and Hitachi File Services Manager server message log on the management server

Item	Description
Serial number	The serial number of the message within the message log file is output.
Date	The message output date is output in the *YYYY*/*MM*/*DD* format.

Item	Description
Time	The message output time is output in the *hh*:*mm*:*ss*.*sss* format.
Program name	The component name or command name is output. For a Hitachi File Services Manager log, `FileServicesManager` is output.
Process ID	The ID of the process that triggered log output is output in hexadecimal.
Thread ID	The ID of the thread that triggered log output is output in hexadecimal.
Message ID	The message ID is output.
Event type	The type of the event that triggered trace output is output.
Message text	The message text is output.

Information is output to the event log in the following format:

```
date time type user computer source classification event-ID description
```

The table below indicates the information output to the event log.

Table 2-7 Information output to the event log

Item	Description
Date	The message output date is output in the *YYYY*/*MM*/*DD* format.
Time	The message output date is output in the *hh*:*mm* format.
Type	One of the following three types is output. • Information • Warning • Error
User	`N/A` is displayed.
Computer	The computer name is displayed.
Source	`HBase Storage Mgmt Log` is displayed.
Classification	`None` is displayed.
Event ID	`1` is displayed.
Description	The description is output in the following format: `HFSM [process-ID]: message-ID message-text`

Checking for a possible server connection problem

To find out whether there is a problem in the network connection to the nodes, check the status and network configuration of the following servers used by the HDI system:

- DNS server#
- NIS server#
- NTP server#
- LDAP server
- CIFS client authentication server (domain controller or Windows NT server)
- NFS client authentication server (KDC server)

System administrators should use the **List of RAS Information** page (for `Server check`) in the **Check for Errors** dialog box to check the connection status between a node and each server. For details about how to check the connection status between a node and each server, see Appendix B, Network Information on page B-1.

#: Make sure to restart the OS of the node after the problem with the connection between the node and the servers is resolved.

Confirming that there are no problems with DNS name resolution

System administrators need to confirm that there are no problems with DNS name resolution by using the `dig` command.

To confirm that there are no problems with DNS name resolution

1. Log on to the target node by using the `ssh` command.
2. Confirm that there are no problems with DNS name resolution by using the `dig` command.

   Execute the `dig` command by using the options shown below. Do not specify any other options.

   For forward lookup:

   ```
   $ dig +time=5 +tries=2 @IP-address-of-the-DNS-server name-of-a-host-to-be-resolved
   ```

   For reverse lookup:

   ```
   $ dig +time=5 +tries=2 @IP-address-of-the-DNS-server -x IP-address-of-a-host-to-be-resolved
   ```

   The following are examples of executing the `dig` command. Check the `ANSWER SECTION` field to confirm that there are no problems with DNS name resolution.

   For forward lookup:

   ```
   $ dig +time=5 +tries=2 @10.208.148.103 win104.temp.local

   ; <<>> DiG 9.2.4 <<>> +time=5 +tries=2 @10.208.148.103 win104.temp.local
   ;; global options:  printcmd
   ;; Got answer:
   ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61734
   ```

```
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;win104.temp.local.             IN      A

;; ANSWER SECTION:
win104.temp.local.      3600    IN      A       10.208.148.104

;; Query time: 1 msec
;; SERVER: 10.208.148.103#53(10.208.148.103)
;; WHEN: Mon Jul  6 12:26:40 2009
;; MSG SIZE  rcvd: 51
```

For reverse lookup:

```
$ dig +time=5 +tries=2 @10.208.148.103 -x 10.208.148.104

; <<>> DiG 9.2.4 <<>> +time=5 +tries=2 @10.208.148.103 -x 10.208.148.104
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9459
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;104.148.208.10.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
104.148.208.10.in-addr.arpa. 3600 IN    PTR     win104.temp.local.

;; Query time: 0 msec
;; SERVER: 10.208.148.103#53(10.208.148.103)
;; WHEN: Mon Jul  6 12:26:46 2009
;; MSG SIZE  rcvd: 76
```

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.

If the HDI system is connected to the remote HCP system over a network and the problem cannot be identified, take action according to Recovering from an HCP access failure on page 4-20.

Checking the FC path status

From the GUI, you can check whether there are any problems with the FC paths. You can also check the FC path statuses by using the `fpstatus` command. If a failure occurs in the FC paths, take action according to Recovering from FC path errors on page 4-32.

Checking the hardware status

From the GUI, you can check whether there are any problems with the hardware. If you prefer to use commands to check the status, execute the `hwstatus` command and the `fpstatus` command.

If the hardware status is not normal, take corrective action by following the instructions in Recovering hardware from a failure on page 4-41.

Checking the connection status with the HCP system

Check whether you can connect to the HCP system to which data is migrated from the HDI system. Execute the `hcpaccesstest` command.

Checking the communication of the management ports and the BMC ports

If maintenance personnel ask you to check the communication of the management ports and the BMC ports, execute the `ping` command for the management ports and the BMC ports.

Before starting the check procedure, prepare the worksheet as shown in Table 2-8 Worksheet for checking the communication of the management ports and the BMC ports on page 2-18. Use the worksheet to write down information acquired from the procedure.

Table 2-8 Worksheet for checking the communication of the management ports and the BMC ports

	Node 0		Node 1	
	Management port	BMC port	Management port	BMC port
IP address				
Check result				

To check the communication of the management ports and the BMC ports

1. Acquire the IP addresses of the management ports and BMC ports for both nodes, and then write them down on the worksheet.

   Check the management port IP addresses (management IP addresses). Use the `bmcctl` command to check the BMC port IP addresses.

2. Execute the `ping` command by using the IP addresses acquired in step 1, and then write down the results on the worksheet.

   Examples of a success result and a failure result are displayed in the Windows command prompt as shown below.

   Success result (The port responded):

```
C:\>ping 192.168.0.20

Pinging 192.168.0.20 with 32 bytes of data:

Reply from 192.168.0.20: bytes=32 time<1ms TTL=128
Reply from 192.168.0.20: bytes=32 time<1ms TTL=128
Reply from 192.168.0.20: bytes=32 time<1ms TTL=128
Reply from 192.168.0.20: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Failure result (The port did not respond):

```
C:\>ping 192.168.0.20

Pinging 192.168.0.20 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.0.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

If `Request timed out` is output at least once, the OS might be under a heavy load. If this happens, execute the command again and check whether the same results are returned. If the same results continue to be output and the command does not end, press the **Ctrl** and **C** keys to cancel the command.

After checking the results, write down "OK" or "Failed" in the corresponding check result boxes on the worksheet. The following is an example of a filled-out worksheet.

Table 2-9 Example of a filled-out worksheet for checking the communication of the management ports and the BMC ports

	Node 0		Node 1	
	Management port	**BMC port**	**Management port**	**BMC port**
IP address	192.168.0.20	192.168.0.22	192.168.0.21	192.168.0.23
Check result	OK	OK	Failed	OK

3. If maintenance personnel ask, inform them of the results.

Checking for a possible NTP time synchronization problem

The procedure to check for a possible NTP time synchronization problem is as follows:

1. Execute the `ssh` command to log in to the target node.
2. Execute the `ntpq` command to check the IP address or host name of the NTP server.

```
$ ntpq -np
     remote           refid      st t  when poll  reach  delay
offset    jitter
==============================================================================
===
*158.214.125.24  133.144.228.126  4 u  623 1024  377    4.256   -0.450
1.061
```

Confirm that an asterisk (`*`) is pretended to the IP address or host name under "`remote`". If there is no asterisk, the time of the target node is not properly synchronized with the NTP server. Check the following:

- Make sure that the node is properly connected with the NTP server.
- Make sure that the NTP server is correctly configured.

Note that it might take a maximum of eight hours to complete NTP time synchronization. After the node is restarted, if a message appears indicating that there is a problem with time synchronization, wait eight hours, and then check whether there is a problem again.

For details about how to check the connection status between a node and the NTP server, see Appendix B, Network Information on page B-1. For details about the environment settings for the NTP server, see the *Installation and Configuration Guide*.

Checking the backup management software status and settings

If an error that prevents you from performing a backup or restore operation occurs, the cause of the error might pertain to the settings of a backup server, media server, or backup management software.

Identify the cause of the error by checking the error messages and logs on the backup servers and media servers. For details on how to check error messages and logs from backup management software, see the documentation for the backup management software.

Checking the error messages and logs from backup servers and media servers

Backup Restore messages are sent to the backup servers. The message IDs begin with `KAQB` for Backup Restore messages.

Checking the result of a backup or restore operation

You can use backup management software to check the execution result of a backup or restore operation. For details, see the supplementary Backup Restore documentation that is provided with HDI.

Checking the settings of the backup management software

Check whether the settings specified on the backup server and media server are correct. For details on the environment settings for the backup server and media server, see the supplementary Backup Restore documentation that is provided with HDI.

Checking the status of a tape drive

When using a tape drive connected to a node via a SAN, if an error occurs in the network or SAN or if the load on the OS increases, the tape drive might become unavailable for the backup management software.

If such a problem occurs, check and revise the HDI operation by, for example, reducing the load. For details about how to make a tape drive available, see the supplementary Backup Restore documentation that is provided with HDI.

Checking the status of the OS on the other node when the other node is connected to the same tape device

When backup or restoration processing terminates with an error, make sure that the OS is not being started or restarted on the other node that shares the tape device.

When a tape device is connected to nodes via a SAN, the tape device is shared among the nodes. If the OS is started or restarted on one of the nodes, a backup or a restoration being performed on the other node might terminate with an error.

When the OS is started or restarted on the other node, try performing a backup or a restoration again after the OS has completely started or restarted.

Checking the status of the tape device connected to a node via a SAN

When you use a tape device connected to a node via a SAN, use the following procedure to check the tape drive status:

1. Execute the `tapelist` command without any options specified.
   Check the registration status of the tape drives.

   When `B` is displayed as the second of the two letters in the `Status` column:

   The connection between the tape drive and the node is blocked from the node on which you executed the command. You will need to correct the blocked connection. For details on how to correct the blocked connection, see When the connection between a tape drive and node is blocked on page 4-47.

   When the above condition does not exist:

   Use the backup management software to make sure that a backup or restore operation that uses a tape device connected to a node via a SAN is not being performed. Then proceed to step 2.
2. Execute the `tapelist` command with the `-A`, `-d`, and `-t` *WWN*:*LUN* options specified.
   Check the connection status of the tape drive you specified by *WWN*:*LUN*.

   If no tape drive information is displayed or `N` is displayed as the first of the two letters in the `Status` column:

   Possible causes are as follows:

- The tape device is not turned on.
- The node, FC switch, and tape device are not correctly connected.
- The FC switch zoning settings are specified incorrectly.
- An FC cable is disconnected.
- There is a problem with the FC switch or tape device.
- The connection between the tape drive and the node is blocked from a node other than the one on which you executed the command.

You need to take necessary action in cooperation with the SAN administrator. For details on the FC switch and tape device, see the documentation from the FC switch and tape device vendors.

Also, if there is a node from which the connection between the tape drive and the node is blocked, perform the procedure described in When the connection between a tape drive and node is blocked on page 4-47 to correct the blocked connection.

If none of the above is the cause the error, there might be a problem on the FC port of a node or in the OS. Obtain the error information output at the time of the error, and then contact maintenance personnel.

When `D,D` is displayed in the `Status` column:

The tape drive is not registered on the NDMP server. Specify *WWN*:*LUN* in the `-t` option to register the specific drive on the NDMP server.

If `Error` is displayed for `Model` and `Type`:

There might be a problem with the tape device. See the documentation from the tape device vendor, and then take appropriate action.

If the command execution results do not indicate any of the symptoms listed above, because the error might be temporary, perform a backup or restore operation again. If the problem cannot be solved, obtain the error information output at the time of the error, and then contact maintenance personnel.

3

Collecting Data and Contacting Maintenance Personnel

This chapter describes how to collect log files.

If the system administrator cannot identify the cause and location of an error or cannot fix the error, that person needs to collect error information, and then send it to maintenance personnel. To analyze the cause of an HDI error, the following log files are required:

- Management server log files

- Log files of the nodes

- Core files and dump files of the nodes

To analyze the cause of an error that occurred during the installation or uninstallation of Hitachi File Services Manager, the log files of the installer and the management server are required.

To analyze the cause of a network error, packet trace log files are also required.

To analyze and determine the cause of a network error, packet trace log files are also required. To analyze the performance of the CIFS service, the CIFS-service performance analysis log files are required.

Collecting management server log files

You can collect log files on the management server in a batch by using one of the following methods:

- Operating from the Windows menu
- Using a command

Note: If you perform operations from the Windows menu, only the following log files are collected in a batch:

- Hitachi Command Suite Common Component log files
- Hitachi File Services Manager log files

  If you need the log files for Hitachi Command Suite products, use a command to collect the log files in a batch. (This would apply, for example, if you run and manage the HDI system by logging on to the Device Manager GUI).

Do not run more than one process to collect log files on the management server at a time.

If the KAPM05318-I or KAPM05319-E message is not output as the log file collection result, the collection stopped because there is not enough space in the folder where the log files are to be stored. Ensure that the folder has enough space, and then collect the log files again.

Collecting log files by using the Windows menu

When log files are collected by using the Windows menu, the Hitachi Command Suite Common Component log files and Hitachi File Services Manager log files are stored in the following folder:
Hitachi-File-Services-Manager-installation-folder\log_archive

The log files are archived using the following names:

- HiCommand_log.jar
- HiCommand_log.hdb.jar
- HiCommand_log.db.jar
- HiCommand_log.csv.jar

To collect log files on the management server by using the Windows menu

1. Log on to Windows as an administrator or a user belonging to the Administrators group.
2. If you are using Windows 7 or earlier, from the Windows **Start** menu, select **Programs**, **Hitachi Command Suite**, **File Services Manager**, and then **Get Logs - HFSM**.

   If you are using Windows 8 or Windows Server 2012, from the list of applications in the Start window, select **Get Logs - HFSM**.

The progress is displayed at a command prompt. If the `log_archive` directory already exists, a message prompting you to confirm the deletion of the directory is displayed.

3. After processing finishes, press any key to close the command prompt.

Collecting log files by using a command

When collecting log files by using a command, you can collect not only the Hitachi Command Suite Common Component log files and Hitachi File Services Manager log files, but also the log files for the Hitachi Command Suite products installed on the management server.

To collect log files on the management server using a command

1. Log on to Windows as an administrator or a user belonging to the Administrators group.
2. Execute the command shown below to collect log files.
   When you execute the `hcmdsgetlogs` command, the following archive files are created:
   - *archive-file-name*`.jar`
   - *archive-file-name*`.hdb.jar`
   - *archive-file-name*`.db.jar`
   - *archive-file-name*`.csv.jar`

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmdsgetlogs /dir log-file-output-folder [/types product-name[ product-
name...]] [/arc archive-file-name] [/logtypes log-type[ log-type...]]
```

`/dir`

Specify a folder to which the log files are to be output (*log-file-output-folder*) on the local disk. If you specify an existing folder, make sure that the folder is empty.

For the folder path, specify no more than 41 bytes when not specifying the `/types` option, or no more than 33 bytes when specifying the `/types FileServicesManager` option. For the number of bytes that can be specified for the path when collecting the log files of Hitachi Command Suite products, see the manuals for those products.

You can use any alphanumeric character, space, exclamation mark (`!`), hash mark (`#`), left parenthesis (`(`), right parenthesis (`)`), plus sign (`+`), hyphen (`-`), period (`.`), equal sign (`=`), at mark (`@`), left square bracket (`[`), right square bracket (`]`), caret (`^`), underscore (`_`), left curly bracket (`{`), right curly bracket (`}`), and tilde (`~`). If the path contains a space, enclose the entire path in quotation marks. As a path delimiter, you can use a backslash (`\`), colon (`:`), or forward slash (`/`). However, the path cannot end with a delimiter.

`/types` *product-name*`[` *product-name*`...]`

Specify product names when you can only collect the log files for specific products because a failure occurred or you cannot ensure enough storage space. If you collect only the log files for Hitachi Command Suite Common Component and Hitachi File Services Manager, specify `FileServicesManager` or `HFSM`. For the Hitachi Command Suite product names, see the manuals for those products. If you specify multiple product names, enter a space between each product name.

If you do not specify this option, the command will collect log files for all Hitachi Command Suite products on the management server as well as the Hitachi Command Suite Common Component log files and Hitachi File Services Manager log files. Do not specify this option if you run and manage the HDI system by logging on to the Device Manager GUI.

`/arc`

Specify the archive file name. You can use any alphanumeric character, space, exclamation mark (`!`), hash mark (`#`), left parenthesis (`(`), right parenthesis (`)`), plus sign (`+`), hyphen (`-`), period (`.`), equal sign (`=`), at mark (`@`), left square bracket (`[`), right square bracket (`]`), caret (`^`), underscore (`_`), left curly bracket (`{`), right curly bracket (`}`), and tilde (`~`). If you do not specify this option, the archive file will be named `HiCommand_log`.

When you execute the command, the archive file is created directly under the folder specified in the `/dir` option.

`/logtypes` *log-type*`[` *log-type*`...]`

Specify the types of log files when you can only collect specific types of log files because a failure occurred or you cannot ensure enough storage space. If you specify multiple product names, enter a space between each product name. The following table shows the relationship between specified types and archive files to be created.

Table 3-1 Relationship between specified types and archive files to be created

Specified type	Archive files to be created
`log`	`.jar` and `.hdb.jar` files
`db`	`.db.jar` files
`csv`	`.csv.jar` files

If you do not specify this option, the command will collect all types of log files. If you use this option with the `/types` option, always specify `log`.

Collecting node log files

The system administrator can download node log files using the File Services Manager GUI.

As instructed by the message or maintenance personnel, download all log data (**All log data**) from the **List of RAS Information** page of the **Check for Errors** dialog box, and then send the collected data to the maintenance personnel.

To download system message files, system log files, and other log files in a batch operation

1. In the **Explorer** menu of the Hitachi File Services Manager main window, select **Resources**, and then **Processing Nodes**.
2. In the object tree, select the target node and, in the window that appears, click **Check for Errors** in the **Basic** subtab of the **Settings** tab.
3. On the **List of RAS Information** page of the **Check for Errors** dialog box, from the **Info. type** drop-down list select **Batch-download**, and then click **Display**.
4. Select the option for the log group you want to download, and then click **Download**.

Note: If you selected a PSB log group, before the download dialog box appears, another dialog box asking you whether to perform batch downloading appears.

5. In the Web browser download dialog box specify where to download the file.

   The log files that belong to the selected log group are archived by `tar` and compressed by `gzip`, and downloaded to the specified destination.
6. Click **Close** in the download dialog box.

When you perform batch downloading, some data might be missed if the disk selected to store the **Temporary Internet files** folder for Internet Explorer has insufficient space. In this situation, Internet Explorer does not generate an error or message.

Collecting Hitachi File Services Manager installer log files

By collecting log files on the management server in a batch by using either of the following two methods, you can obtain the necessary log files when an error occurred during Hitachi File Services Manager installation or uninstallation.

- Operating from the Windows menu
- Using a command

For details about how to collect log files on the management server in a batch, see Collecting management server log files on page 3-2.

If you cannot collect log files from the management server in a batch, collect the following log files from the folder where they are stored, and then send them to the maintenance personnel:

`Setup.ilg`

This file is stored in the following folder. *ID* is the product code internally assigned by the Hitachi File Services Manager installer.

Windows-system-drive`:\Program Files\InstallShield Installation Information\`*ID*

`hcmdsist.log`

In the case of a new installation, this file is stored directly under the root of the Windows system drive. In other cases, it is stored directly under the root of the drive on which Hitachi File Services Manager is installed.

`hcmdsrtn.inst`

In the case of a new installation, this file is stored directly under the root of the Windows system drive. In other cases, it is stored directly under the root of the drive on which Hitachi File Services Manager is installed.

`hcmdsuit.log`

In the case of a new installation, this file is stored directly under the root of the Windows system drive. In other cases, it is stored directly under the root of the drive on which Hitachi File Services Manager is installed.

`hcmdsrtn.uit`

In the case of a new installation, this file is stored directly under the root of the Windows system drive. In other cases, it is stored directly under the root of the drive on which Hitachi File Services Manager is installed.

`hcmdshdb_result`

In the case of a new installation, this file is stored directly under the root of the Windows system drive. In other cases, it is stored directly under the root of the drive on which Hitachi File Services Manager is installed.

`HFSM_`*installation-type*`_YYYY-MM-DD_hh-mm-ss.log`

installation-type will be `Install` (installation) or `Uninstall` (uninstallation) depending on the situation in which the log file was output:

The location where the log file is stored depends on the progress stage in which the error occurred. The system administrator must determine the progress stage in which installation or uninstallation terminated with an error, and then collect the log files that were output around the stage in which the error occurred.

Table 3-2 Relationship between the progress stage where installation or uninstallation ended with an error and the log file storage location

Progress stage at the time of error termination		Storage location
Installation	After the installation folder is determined	*installation-folder*\FileServicesManager\inst
	Before the installation folder is determined	New installation: Directly under the root of the Windows system drive Other cases: Directly under the root of the drive on which Hitachi File Services Manager is installed
Uninstallation	When the File Services Manager inst folder has not been deleted	*installation-folder*\FileServicesManager\inst
	When the File Services Manager inst folder has been deleted	Directly under the root of the Windows system drive

Collecting packet trace log files

You (the system administrator) can use the tcpdump command to collect the packet trace log files required when an error occurs in the network. Delete the collected packet trace log files after you send the log files to maintenance personnel.

To collect the packet trace log files from a Unix machine

1. Log on to the target node by using the ssh command.
2. Create an empty log file by using the touch command.

   Create an empty log file in the destination for a packet trace log file. Hitachi Data Systems recommend that you specify a file system with more than 1 GB of free space for the destination so that you do not fail to collect the log file because of a space shortage. If you do not create an empty log file in advance, you cannot delete the collected packet trace log file because the log file is created with root privileges.
3. Collect the packet trace log file by using the tcpdump command.

   Execute the tcpdump command with the options below specified. Do not specify any other options.

```
$ sudo tcpdump -i interface-name -s size -w packet-trace-log-file -n -c
number-of-packets-to-be-collected qualifier
```

`-i` *interface-name*

Specify the name of the interface for which you will collect a packet trace. Specify an interface on the route where the error occurred. If the interface name is unknown, or if you want to collect all the packet traces for all interfaces, specify `any`. You must specify this option. For an interface for which a VLAN is set up, specify the name in the following format:

port-name.*VLAN-ID* (Example: `eth12.0010`)

`-s` *size*

Specify the size for acquiring the trace in the packets to be collected (units: bytes). We recommend that you specify a size larger than the MTU value. However, when the network has a heavy workload, specify the default value (96 bytes).

`-w` *packet-trace-log-file*

Specify the absolute path to the packet trace log file. You must specify this option.

`-n`

Specify this option when names are not to be resolved.

`-c` *number-of-packets-to-be-collected*

Specify the maximum number of packets for collecting a trace.

qualifier

Specify in either of the following formats:

`host` *IP-address*

`port` *port-number*

Specify this option to collect only packets for communication with qualified hosts or ports. If the error occurred in communication with a specific host or port, specify this option. If you use a combination of multiple qualifiers, use `and` or `or` to separate them.

The following description is an example of executing the command when the system administrator collects a packet trace log file.

When a packet trace log file is to be collected and stored in `/mnt/fs1/tcpdump.log`:

- The name of the interface for which a packet trace is to be collected is `eth1`.
- The maximum number of packets for collecting the trace is 900,000.
- Packets for communication to the host whose IP address is `10.208.61.8` and ports whose port number is `139` or `445` are collected.

```
$ ssh -2 nasroot@nas01
$ touch /mnt/fs1/tcpdump.log
$ sudo tcpdump -i eth1 -w /mnt/fs1/tcpdump.log -c 900000 host 10.208.61.8
and port 139 or port 445
```

Note: If you do not specify the maximum number of packets for collecting a trace, make sure that the free space of the user LU does not become insufficient.
For example, if you specify the default value (96 bytes) for the size of a packet trace to be collected, and you do not specify the maximum number of packets for collecting a trace, when approximately 900,000 packet traces are collected, the packet trace log file size will be about 100 MB.

Collecting the CIFS-service performance analysis log

Maintenance personnel might ask you to collect data to help analyze the performance of the CIFS service. If they do so, use the following procedure to collect the CIFS-service performance analysis log, and send the log to the maintenance personnel.

1. Log in to the target node .
2. Use the `cifsinfogetctl` command to set the system to collect the CIFS-service performance analysis log.
   For details about this command, see the *CLI Administrator's Guide*.
3. Send the collected log data to the maintenance personnel.
   If you specified the log output directory when you executed the command, access that directory as a CIFS administrator. Send all files in the subdirectories with names that begin with `cifsinfoget_` to the maintenance personnel.
   If you did not specify the log output directory, open the **Check for Errors** dialog box, and then, on the **List of RAS Information** page, download all the log data. Send all of that downloaded data to the maintenance personnel. For details about how to download all the log data, see Collecting node log files on page 3-5.

4

Error Recovery

This chapter explains how to take recovery action.

When an error occurs, the system administrator identifies the cause by viewing the error messages and system messages, and then takes recovery action as indicated in the message text or as instructed by maintenance personnel.

If you (the system administrator) cannot fix the error, perform failover and failback operations as instructed by maintenance personnel.

If you perform an operation on a resource group or cluster or use a command when recovering the system from an error, you must refresh the view to update the information about the file systems and file shares displayed in the GUI.

- ☐ Checking and retrying any erroneous GUI operations
- ☐ Checking and retrying any erroneous command operations
- ☐ Re-registering the management server authentication password
- ☐ Checking system messages and recovering from an error
- ☐ Viewing error information for the cluster, nodes, and resource groups and taking recovery action
- ☐ Manual failover and failback
- ☐ Recovering from file system errors
- ☐ Recovering from an HCP access failure
- ☐ Restoring a file system migrated to an HCP system

- Restoring a file system from the replica HCP system when a failure occurs on both the file system and the primary HCP system
- Restoring data from the HDI system to the HCP system when stub processing are not performed for migrated files
- Restoring system configuration information
- Restoring system configuration information and user data in batch
- Recovering from FC path errors
- Using interface and network error information for error recovery
- Using error information on trunking for error recovery
- Using error information on the data port for error recovery
- Recovering hardware from a failure
- Recovering from a failure in which an LU cannot be detected during the startup of an OS
- Recovering from a failure during a data import from another file server
- Recovering from a failure related to Backup Restore functionality

Checking and retrying any erroneous GUI operations

If an error occurs due to an improper operation of File Services Manager GUI, such as a wrong setting or operation mistake, refresh the database on the management server, and then retry the operation as instructed by the messages.

For details about refreshing, see the *Cluster Administrator's Guide*.

Checking and retrying any erroneous command operations

If the error was due to a command input error, re-execute the command as instructed by the messages displayed in the standard error output.

Re-registering the management server authentication password

If `Credential error` is displayed as the processing node or physical node operating status, the management server authentication password registered from the GUI is different from the authentication password actually assigned to the node. In the **Edit Node** dialog box, re-register the management server authentication password assigned to the node.

Checking system messages and recovering from an error

From the system message ID, you can identify the program in which the error occurred. From the message text, you can see what caused the error.

For details on the appropriate action in response to a particular system message, see the manual *Error Codes*. You can use the message ID to locate the relevant message, and find out how to recover from the error.

For details about the relationship between the programs that output messages and the message IDs, see Checking system messages on the node on page 2-3.

Viewing error information for the cluster, nodes, and resource groups and taking recovery action

The system administrator can check the error status of the affected cluster, nodes, and resource groups in the **Browse Cluster Status** page of the **Cluster Management** dialog box and take recovery action by cooperating with the maintenance personnel.

Checking error information for the cluster, nodes, and resource groups and identifying a recovery method

To identify the error in the failover functionality, the system administrator must confirm the recovery method indicated in Table 4-1 Error recovery procedures for cluster statuses displayed in the Browse Cluster Status page (for Cluster / Node status) on page 4-4 to Table 4-4 Error recovery procedures for resource group error information displayed in the Browse Cluster Status page (for Resource group status) on page 4-7, according to the status of the cluster, nodes, and resource groups that were checked in the **Browse Cluster Status** page. Also, confirm the instructions of the maintenance personnel, and then specify the recovery procedure from these tables.

To view the status of a cluster, see **Cluster status** in the **Browse Cluster Status** page (for `Cluster / Node status`). The table below summarizes the error recovery procedure for each of the cluster statuses displayed in this page.

Table 4-1 Error recovery procedures for cluster statuses displayed in the Browse Cluster Status page (for Cluster / Node status)

Cluster status	Recovery procedure	
	Recovery action	See
`ACTIVE`	Running normally. No recovery action is required.	N/A
`INACTIVE`	Start the stopped cluster.	N/A
`UNKNOWN`#	Fix the problem that occurred at OS startup. Stop both nodes and fix the problem. Stop both nodes and replace the program.	Recovery procedure 1 on page 4-9
	Restart the OSs on both nodes in the cluster.	Recovery procedure 2 on page 4-9
	Restart the OSs on both nodes in the cluster, while continuing degenerated operation following the failover.	Recovery procedure 2 on page 4-9
`DISABLE`	Contact maintenance personnel.	N/A

Note: N/A = Not applicable.

#: If you display the **Browse Cluster Status** page (for `Cluster / Node status`) on a physical node that you stopped or performed a forced stop for, `UNKNOWN` is displayed as the cluster status and as the status of the other node. In this condition, you cannot view the status of the cluster or the status of the other node. To check the statuses of the cluster and the other node, display the **Browse Cluster Status** page (for `Cluster / Node status`) on the running physical node (the other node).

`UNKNOWN` is also displayed when a cluster starts up. Note that, when a cluster starts up, `UNKNOWN` is displayed until both OSs on the nodes making up the cluster complete startup (for up to 10 minutes).

To view the status of a node, see **Node status** in the **Browse Cluster Status** page (for `Cluster / Node status`). The table below summarizes the error recovery procedure for each of the node statuses displayed in this page.

Table 4-2 Error recovery procedures for node statuses displayed in the Browse Cluster Status page (for Cluster / Node status)

Node status	Recovery procedure	
	Recovery action	See
UP	Running normally. No recovery action is required.	N/A
INACTIVE	Start the stopped node.	N/A
DOWN	Restart the OS on the failed node, while continuing degenerated operation following the failover.	Recovery procedure 4 on page 4-10
	Replace the program without stopping services, while continuing degenerated operation following the failover.	Recovery procedure 5 on page 4-10
	Stop both nodes and replace the program.	Recovery procedure 6 on page 4-10
UNKNOWN#	Stop both nodes and fix the problem.	Recovery procedure 6 on page 4-10
	Stop and recover the node where the error occurred, while continuing degenerated operation following the failover.	Recovery procedure 3 on page 4-10
	Restart the OS on the failed node, while continuing degenerated operation following the failover.	Recovery procedure 4 on page 4-10
	Fix the hardware or software error that occurred on both nodes at OS startup. Stop both nodes and replace the program.	Recovery procedure 6 on page 4-10
	Fix the hardware or software error that occurred on either node at OS startup.	Recovery procedure 7 on page 4-11
	Restart the OS on both nodes in the cluster.	Recovery procedure 8 on page 4-11

Note: N/A = Not applicable.

#: `UNKNOWN` is also displayed when a cluster starts up. Note that, when a cluster starts up, `UNKNOWN` is displayed until both OSs on the nodes making up the cluster complete startup (for up to 10 minutes).

To view the status of a resource group, see **Resource group status** in the **Browse Cluster Status** page (for `Resource group status`). The resource group status and error information are displayed in the following form:
`resource-group-status/error-information`

The table below summarizes the error recovery procedure for each of the displayed resource group statuses.

Table 4-3 Error recovery procedures for resource group statuses displayed in the Browse Cluster Status page (for Resource group status)

Resource group status	Recovery procedure	
	Recovery action	See
`Online`	See the resource group error information.	Table 4-4 Error recovery procedures for resource group error information displayed in the Browse Cluster Status page (for Resource group status) on page 4-7
`Online Maintenance`	See the resource group error information.	Table 4-4 Error recovery procedures for resource group error information displayed in the Browse Cluster Status page (for Resource group status) on page 4-7
`Online Pending`	The resource group is starting. No recovery action is required. If the status does not change from `Online Pending` even after the resource group startup time has elapsed during normal operation, perform either of the following operations: • Restart the cluster. • Restart any node displayed in **Running node**.	N/A
`Online Ready`	Start the stopped cluster or node.	N/A
	The cluster was stopped at OS shutdown. Fix the error at the next session.	Recovery procedure 9 on page 4-11
	The node was stopped when the turning the power off. Fix the error at the next session. Restart the failover functionality only at the node where the error occurred.	Recovery procedure 10 on page 4-11
	Restart only the node where the error occurred.	Recovery procedure 11 on page 4-11
	Restart the OSs on the both nodes.	Recovery procedure 6 on page 4-10
	Start the resource group when the cluster is running normally.	Recovery procedure 22 on page 4-15
`Offline`	See the resource group error information.	Table 4-4 Error recovery procedures for resource

Resource group status	Recovery procedure	
	Recovery action	See
		group error information displayed in the Browse Cluster Status page (for Resource group status) on page 4-7
Offline Pending	The resource group is stopping. No recovery action is required.	N/A
Discovery (exclusivity)	Online processing is being performed for the resource group before operations begin. No recovery action is required.	N/A
Initializing	The resource group is initializing. No recovery action is required.	N/A
Internal Error	See the resource group error information.	Table 4-4 Error recovery procedures for resource group error information displayed in the Browse Cluster Status page (for Resource group status) on page 4-7
Note: N/A = Not applicable.		

The table below summarizes the error recovery procedures for the displayed resource group error information.

Table 4-4 Error recovery procedures for resource group error information displayed in the Browse Cluster Status page (for Resource group status)

Error information	Recovery procedure	
	Recovery action	See
No error	Running normally. No recovery action is required.	N/A
Internal error - not recoverable	Fix the error on the node that failed to start at OS startup in the cluster.	Recovery procedure 12 on page 4-11
	The maintenance personnel must replace the hardware.	Recovery procedure 13 on page 4-12
	Restart the resource group where the error occurred.	Recovery procedure 14 on page 4-12
	Restart the node running the resource group in which the error occurred.	Recovery procedure 15 on page 4-12
	Restart the OS on the node running the resource group in which the error occurred.	Recovery procedure 16 on page 4-12

Error information	Recovery procedure	
	Recovery action	See
	Stop only the node where the error occurred and replace the program.	Recovery procedure 17 on page 4-13
	Stop both nodes and replace the program.	Recovery procedure 18 on page 4-13
Monitor activity unknown	Stop both nodes and replace the program.	Recovery procedure 18 on page 4-13
	Take action to restore services as soon as possible, and replace the program at a later date.	Recovery procedure 20 on page 4-14
No available nodes or No available nodes in failure domain after monitor failure	If the error occurred in a resource group that was failed over to the alternate node in a cluster, and the original resource group is still active on that node, fix the error and then restart services on the original node.	Recovery procedure 13 on page 4-12
	If the error occurred in a resource group that was failed over to the alternate node in a cluster, and the original resource group on that node has been switched to the other node, fix the error and then restart the services of the failed resource group.	Recovery procedure 21 on page 4-14
Node unknown	Restart the node running the resource group in which the error occurred.	Recovery procedure 15 on page 4-12
	Restart the OS on the node running the resource group in which the error occurred.	Recovery procedure 16 on page 4-12
	Stop only the node where the error occurred and replace the program.	Recovery procedure 17 on page 4-13
	Stop both nodes and replace the program. Stop both nodes and fix the problem. Fix the hardware error that occurred on both nodes at OS startup. Stop the node where the error occurred at OS startup and replace the program on the node.	Recovery procedure 18 on page 4-13
Split resource group (exclusivity)	Fix the error that occurred at OS startup. Take action to restore the services provided by the resource group as soon as possible, and replace the program at a later date.	Recovery procedure 19 on page 4-14
	Stop both nodes and replace the program.	Recovery procedure 18 on page 4-13

Error information	Recovery procedure	
	Recovery action	See
`srmd executable error`	Stop both nodes and fix the problem.	Recovery procedure 1 on page 4-9
	Restart the OS on the failed node, while continuing degenerated operation following the failover.	Recovery procedure 4 on page 4-10
	Fix the hardware or software error that occurred on both nodes at OS startup. Stop both nodes and replace the program.	Recovery procedure 6 on page 4-10
	Fix the hardware or software error that occurred on either node at OS startup.	Recovery procedure 7 on page 4-11
	Restart the OSs on both nodes in the cluster.	Recovery procedure 8 on page 4-11
	Check whether the KAQM05256-E system message, or a system message in the range from KAQM05258-E through KAQM05264-E was output, and then take action accordingly.	N/A
Note: N/A = Not applicable.		

The recovery procedure for each of these errors is described below.

Recovery procedure 1

To recover from cluster status UNKNOWN or resource group error information srmd executable error

1. Perform a forced stop for the cluster.
2. Ask the maintenance personnel to restart the OSs on both nodes in the cluster.

   Consult with the maintenance personnel for details about error recovery operations, and then ask the maintenance personnel to restart the OSs. The maintenance personnel must start the OSs after the maintenance is complete.
3. Start the cluster.

Recovery procedure 2

To recover from cluster status UNKNOWN

1. Perform a forced stop for the cluster.
2. Restart the OSs on both nodes in the cluster.

3. Start the cluster.

Recovery procedure 3

To recover from node status UNKNOWN

1. Ask the maintenance personnel to start the OS on the repaired node.

   Consult with the maintenance personnel for details about error recovery operations, and then ask the maintenance personnel to start the OS. The maintenance personnel must start the OS after the maintenance is complete.
2. Fail back the resource group to the original node.

Recovery procedure 4

To recover from node status DOWN, node status UNKNOWN, or resource group error information srmd executable error

1. Restart the OS on the failed node.
2. Fail back the resource group to the original node.

Recovery procedure 5

To recover from node status DOWN

1. Ask the maintenance personnel to start the OS on the repaired node.

   Consult with the maintenance personnel for details about error recovery operations, and then ask the maintenance personnel to start the OS. The maintenance personnel must start the OS after the maintenance is complete.
2. Change the execution node of both resource groups.
3. Ask the maintenance personnel to restart the OS on the other node in the cluster.

   Consult with the maintenance personnel for details about error recovery operations, and then ask the maintenance personnel to restart the OS. The maintenance personnel must start the OS after the maintenance is complete.
4. Fail back the resource group to the original node.

Recovery procedure 6

To recover from node status DOWN, node status UNKNOWN, resource group status Online Ready, or resource group error information srmd executable error

1. Perform a forced stop for the cluster.
2. Restart the OSs on the both nodes.
3. Start the cluster.

Recovery procedure 7

To recover from node status UNKNOWN

1. Perform a forced stop for the node where the error occurred.
2. Ask the maintenance personnel to restart the OS on the failed node.
   Consult with the maintenance personnel for details about error recovery operations, and then ask the maintenance personnel to restart the OS. The maintenance personnel must start the OS after the maintenance is complete.
3. Start the repaired node.
4. Fail back the resource group to the original node.

Recovery procedure 8

To recover from node status UNKNOWN or resource group error information srmd executable error

1. Perform a forced stop for the cluster.
2. Shut down the OS on the active node.
3. Start the OSs on both nodes in the cluster.
   Turn on the power to the nodes.
4. Start the cluster if it is in `INACTIVE` status.

Recovery procedure 9

To recover from resource group status Online Ready

1. Start the cluster.

Recovery procedure 10

1. Start the node.

Recovery procedure 11

To recover from resource group status Online Ready

1. Start the OS on the failed node.
   Turn on the power to the node.

Recovery procedure 12

To recover from resource group error information Internal error - not recoverable

1. Perform a forced stop for the resource group where the error occurred.
2. Stop the node where the error occurred.

3. Start the resource group that was running on the node where the error occurred.
4. Ask the maintenance personnel to start the OS on the repaired node.

   Consult with the maintenance personnel for details about error recovery operations, and then ask the maintenance personnel to restart the OS. The maintenance personnel must start the OS after the maintenance is complete.
5. Start the repaired node.
6. Fail back the resource group to the original node.

Recovery procedure 13

To recover from resource group error information Internal error - not recoverable, no available nodes, or No available nodes in failure domain after monitor failure

1. Perform a forced stop for the resource group that was running on the node where the error occurred.
2. Restart the OS on the failed node.
3. Start the resource group.

Recovery procedure 14

To recover from resource group error information Internal error - not recoverable

1. Perform a forced stop for the resource group where the error occurred.
2. Start the resource group.

Recovery procedure 15

To recover from resource group error information Internal error - not recoverable or Node unknown

1. Perform a forced stop for the resource group where the error occurred.
2. Stop the node.
3. Start the node.
4. Start the resource group.

Recovery procedure 16

To recover from resource group error information Internal error - not recoverable or Node unknown

1. Perform a forced stop for the resource group where the error occurred.
2. Stop the node.
3. Restart the OS on the stopped node.
4. Start the node.

5. Start the resource group.

Recovery procedure 17

To recover from resource group error information Internal error - not recoverable or Node unknown

1. Perform a forced stop for the resource group where the error occurred.
2. Stop the node on which the error occurred.
3. Ask the maintenance personnel to restart the OS on the stopped node.

   Consult with the maintenance personnel for details about error recovery operations, and then ask the maintenance personnel to restart the OS. The maintenance personnel must start the OS after the maintenance is complete.
4. Start the node.
5. Start the resource group.
6. Fail over the resource group on the other node in the cluster.
7. Stop the node in step 6.
8. Ask the maintenance personnel to restart the OS on the other node in the cluster.

   The maintenance personnel must start the OS after the maintenance is complete.
9. Start this node.
10. Fail back the resource group to the original node.

Recovery procedure 18

To recover from resource group error information Internal error - not recoverable or Monitor activity unknown, and Node unknown or Split resource group (exclusivity)

1. Perform a forced stop for the resource group where the error occurred.
2. Stop the other resource group in the cluster.
3. Stop the cluster.
4. Ask the maintenance personnel to restart the OSs on both nodes in the cluster.

   Consult with the maintenance personnel for details about error recovery operations, and then ask the maintenance personnel to restart the OSs. The maintenance personnel must start the OSs after the maintenance is complete.
5. Start the cluster.
6. Start both resource groups.

Recovery procedure 19

To recover from resource group error information Split resource group (exclusivity)

1. Perform a forced stop for the resource group where the error occurred.
2. Stop the other resource group in the cluster.
3. Stop the cluster.
4. Restart the OSs on both nodes in the cluster.
5. Start the cluster.
6. Start both resource groups.

Recovery procedure 20

To recover from resource group error information Monitor activity unknown

1. Monitor the resource group.
2. Exclude the resource group from monitoring.
3. Repeat steps 1 and 2.

Recovery procedure 21

To recover from resource group error information No available nodes or No available nodes in failure domain after monitor failure

1. Perform a forced stop for the resource group where the error occurred.
2. Stop the failover node to which the resource group was relocated.
3. Ask the maintenance personnel to restart the OS on the stopped (failover source) node.

   Consult with the maintenance personnel for details about error recovery operations, and then ask the maintenance personnel to restart the OS. The maintenance personnel must start the OS after the maintenance is complete.
4. Start the repaired failover node.
5. Change the execution node on which the active resource group runs.
6. Stop the original node from which the resource group was relocated.
7. Ask the maintenance personnel to restart the OS on the stopped (failover target) node.

   The maintenance personnel must start the OS after the maintenance is complete.
8. Start the original node.
9. Start the resource group on the original node.

Recovery procedure 22

To recover from resource group status Online Ready

1. Start the resource group.

Manual failover and failback

When maintenance or error recovery of a node is required, the system administrator must perform a failover and failback manually from the **Browse Cluster Status** page (for `Resource group status`) of the **Cluster Management** dialog box as instructed by the maintenance personnel. On receiving instructions to proceed, fail over the resource group in which services are active. After verifying that maintenance performed by maintenance personnel has finished, fail back the resource group to the original node. For details about manual failover and failback to recover from error, see Viewing error information for the cluster, nodes, and resource groups and taking recovery action on page 4-3.

Manual failover involves relocating one resource group to the other node when resource groups are running on separate nodes in the cluster. The purpose of this operation is to ensure that the services provided by the resource group remain continuously available when maintenance or error recovery is required at a node.

Manual failback means migrating the failed-over resource group from the node where the both resource groups are running to the original node. The purpose of this operation is to restore the failed-over resource group on its original node after error recovery has finished.

If an error occurred during a manual failover or failback and is interfering with the processing, see Viewing error information for the cluster, nodes, and resource groups and taking recovery action on page 4-3.

Recovering from file system errors

If an error occurs in a file system operated by HDI, the recovery procedure differs depending on the cause of the error. See **Mount Status** in the GUI or execute the `fslist` command to check the file system status, and then take action as required.

If the GUI displays `Data corrupted` in **Mount Status** or the `fslist` command displays `Normal` in **Device Status** and `Fatal error` in **Mount Status**:

The file system might be blocked due to an error in the OS or a pool capacity shortage. Check whether virtual LUs are used and automatic failovers (in the event of file system blockage) are enabled.

- When virtual LUs are used in the file system:
  Check whether the `KAQG90009-E` system message is output to the node. If the message has been output, take action according to the

procedure described in When the file system is blocked due to insufficient pool capacity on page 4-19.

- When the automatic failover functionality is enabled:
  Take action according to the procedure described in When the file system is blocked due to an error in the OS (when the automatic failover functionality has been enabled) on page 4-17.
- When the automatic failover functionality is not enabled:
  Take action according to the procedure described in When the file system is blocked due to an OS error (when the automatic failover functionality has not been enabled) on page 4-17.

If the GUI displays `Device error` in **Mount Status** or the `fslist` command displays `Error` in **Device Status** and `Fatal error` in **Mount Status**:

The file system is blocked due to an error in the FC path or the storage system. Check the target of the LU used in the file system in the *file-system* subwindow, and then use **Status** in the **FC Path** subtab of the GUI or the `fpstatus` command to check for errors in the FC path associated with the target.

If an error has occurred in the FC path, take action according to the procedure described in Recovering from FC path errors on page 4-32.

If no errors have occurred in the FC path, take action according to the procedure described in When the file system is blocked due to a storage system error on page 4-18.

We recommend that you regularly back up data for the HDI system in case of failure. The following describes how to restore a file system, assuming that there is backup data available (stored in a medium other than the storage system).

If the data of the file system was migrated to an HCP system, follow the procedures in Restoring a file system migrated to an HCP system on page 4-21 to recreate the file system and recover the backup data. If a failure has occurred on both the file system and the primary HCP system, follow the procedures in Restoring a file system from the replica HCP system when a failure occurs on both the file system and the primary HCP system on page 4-22 to recover the systems.

When files or directories cannot be created even though there is free capacity

In the initial settings, the inode information is stored in the first 1-TB area of the file system. If the area that stores inode information is already full, files or directories cannot be created even if there is free capacity. Perform one of the following methods:

- Execute the `fsinodespace` command to reconfigure the inode area.
- If the file system is created by a previous version, specify the `-m alloc1TB` option and execute the `fsinodectl` command, and then set the file system to store the file expansion attributes in an area different from

the inode. After mounting the file system, use the `fsmoveattr` command to move the file expansion attribute from the inode area.

If the problem still occurs, perform the following steps:

1. Move a large file that was created around the time the file system capacity shortage occurred to another file system.
2. Return the file moved in step 1 to its original location.

After the above procedure, if files and directories still cannot be created, retry the procedure with another file.

You can also eliminate a shortage of an inode area by using the `fsinodectl` command to handle 64-bit inodes. For notes on the handling of 64-bit inodes, see the *Installation and Configuration Guide*.

When the file system is blocked due to an error in the OS (when the automatic failover functionality has been enabled)

To restore a file system that is blocked due to an error in the OS.

1. Fail back the resource group to the original node.
2. Delete the file system.
   Delete the blocked file system.
3. Re-create the file system.
4. Restore the backup data to the re-created file system.
5. Re-create the file share.
   You must select **Use existing directory as is** for **Export point owner** in the **Add Share** dialog box because the file system is restored from backed-up data.

When the file system is blocked due to an OS error (when the automatic failover functionality has not been enabled)

To restore a file system that is blocked due to an error in the OS, by working with maintenance personnel.

1. Ask the maintenance personnel to collect the error information.
   A failover of the resource group starts along with the collection of the error information.
2. Perform a failback for the resource group to the original node.
3. Delete the file system.
   Delete the blocked file system.
4. Re-create the file system.
5. Restore the backup data to the re-created file system.
6. Re-create the file share.

You must select **Use existing directory as is** for **Export point owner** in the **Add Share** dialog box because the file system is restored from backed-up data.

When the file system is blocked due to a storage system error

To restore a file system that is blocked due to an error on the storage system, by working with maintenance personnel.

1. Check the LU being used by the blocked file system.
   Review the following information in the *file-system* subwindow:
   - The target associated with the path to the LU
   - The model and serial number of the storage system containing the LU
   - The LDEV number of the LU
2. Check with maintenance personnel whether you can continue to use the file system.
   In some cases, you might be able to continue using the file system when it is blocked due to an error on the storage system.

   When continued use is possible:
   Go to step 3.

   When continued use is not possible:
   End the procedure here, and then restore the file system from the backup data by following the procedure in When the file system can no longer be used on page 4-18.
3. Ask the maintenance personnel to resolve the problem with the storage system.
4. Check the status of the resource group in which an error occurred.

   If the resource group was failed over:
   Go to step 6.

   If the resource group was not failed over:
   Go to step 5.
5. Manually fail over the resource group on the node.
6. Stop the node.
7. Restart the OS.
8. Start the node.
9. Fail back the resource group to the original node.
10. Execute steps 5 to 9 on the other node in the cluster.

When the file system can no longer be used

In When the file system is blocked due to a storage system error on page 4-18, if you can no longer use the file system, you need to use backed-up data to restore the file system.

To restore a file system from backed-up data.

1. Use the `lumapctl` command to change the settings for automatically assigning LUs to the maintenance mode.
2. Ask maintenance personnel to resolve the problem in the storage system.
3. Delete the file system.
   Delete the blocked file system.
4. If the resource group that was running on the other node was failed over, fail it back.
5. If the resource group on the node you are using has not been failed over, manually fail it over.
6. Stop the node in step 4.
7. Restart the OS on the node in step 4.
8. Start the node in step 4.
9. Fail back the resource group to the original node.
10. Execute steps 4 to 9 on the other node in the cluster.
11. Re-create the file system.
12. Restore the backup data to the re-created file system.
13. Re-create the file share.
    You must select **Use existing directory as is** for **Export point owner** if the **Add Share** dialog box because the file system is restored from backed-up data.
14. Use the `lumapctl` command to change the settings for automatically assigning LUs to the normal operation mode.

When the file system is blocked due to insufficient pool capacity

To restore a file system that is blocked due to a pool capacity shortage:

1. Ask the storage system administrator to resolve the pool capacity shortage.
   If the pool is being formatted in the storage system, there might be a temporary capacity shortage even if the pool has free capacity. If this is the case, ask the storage system administrator to inform you of when the formatting has completed.
2. Manually fail over the resource group on the node.
3. Stop the node.
4. Restart the OS.
5. Start the node.
6. Fail back the resource group to its original node.
7. Execute steps 2 to 6 on the other node in the cluster.

Recovering from an HCP access failure

If any of the following HCP access failures occur, identify the cause and resolve the problem:

- Clients cannot access files that have been migrated to an HCP system.
- A migration failed.
- Migration policies cannot be set.

To recover from an HCP access failure.

1. If clients cannot access files that have been migrated to an HCP system, wait 20 minutes, and then ask the clients to access the files again.

   If clients can access the files, no further action is necessary. If they cannot access the files, go to the next step.
2. Check the HCP system connection status and settings.

   Use the `hcpaccesstest` command to check whether you can access the HCP system. If you cannot access the HCP system, use the `archcpget` command to check whether the HCP information has been properly set. If the information has not been set properly, use the `archcpset` command to reset the information, and then use the `hcpaccesstest` command to check whether you can now access the HCP system.
3. Check the error messages.

   If the `KAQM37070-E` message or the `KAQM37094-E` message has been output, then a failure occurred in the HCP system. Ask the HCP administrator to resolve the problem.

   If any of the following messages has been output, the HCP system load might be heavy or a failure might have occurred on the network between the HDI system and the HCP system:

   `KAQM37037-E`, `KAQM37042-E` to `KAQM37045-E`, `KAQM37049-E`, or `KAQM37120-E`

   Inform the HCP administrator that the HCP access failure is being investigated, and then go to step 4.

   If any other message that starts with `KAQM37` has been output, take action according to the corrective action for the message.
4. Check the status of the hardware and the cluster.

   If you find a problem, contact maintenance personnel. If you do not find any problems, go to the next step.
5. Check the NAT settings, the front-end LAN switch, and the DNS server.

   Resolve any problems you find. If you do not find any problems, go to the next step.
6. Verify the HCP system status with the HCP administrator.

   If the HCP system has been stopped, ask the HCP administrator when operation will resume. Ask clients to wait until the HCP maintenance or recovery procedure is completed before accessing the data again.

   If there are no problems with the HCP system status, a network failure must have occurred. Contact the WAN service provider's maintenance personnel.

7. Ask the end-users of home-directory-roaming file systems to verify that the `.conflict` directory does not exist under the home directory.

   If the `.conflict` directory does exist, ask the end-users to check the files in the `.conflict` directory and to apply any changes to the original files in the home directory.

Note: Even after the failure is recovered from, it is not possible to access the HCP system that you specified using the `arcconfedit` command until the waiting time for reconnecting to the HCP system has elapsed. Therefore, temporarily change the setting of the waiting time to "`0`" and check whether you can access the HCP system. After ensuring that you can access the HCP system, return the setting to the previous value.

Restoring a file system migrated to an HCP system

If the file system whose data was migrated to the HCP system is disabled due to LU failure, restore the file system by using the data that was migrated to the HCP system. Before restoring the metadata, recover the system from the failure.

To restore data from the HCP system to a file system in an HDI system:

1. Create the file system to which you will restore.

   Specify a file system size that is equal to or larger than that of the file system in which the failure occurred. In addition, make sure that the following settings are the same as those for the file system in which the failure occurred:

   - ACL type
   - How the HCP system is linked to (at the file system or share level)
   - Whether the home-directory-roaming functionality is enabled
   - Whether older versions of files are shown to clients
   - Whether the WORM function is enabled
   - Whether CIFS bypass traverse checking is enabled

   If the file system in which the failure occurred supported 64-bit inodes, use the `fsinodectl` command to set the file systems to support 64-bit inodes. If you restore the data in a file system that does not support 64-bit inodes, the number of files might exceed the maximum number of files that can be created in the file system.
2. Mount the file system with both read and write operations permitted.
3. Restore the file system by using the `arcrestore` command.

Note:

- You cannot execute the `arcrestore` command if files or directories have already been created in the file system that you want to restore. If a file share has been created before executing the `arcrestore` command, data restoration from the HCP system might fail.

- If restoration is interrupted with message KAQM37080-E, take appropriate action according to the message. Then, re-execute the `arcrestore` command with the `--skip` option specified.

4. Create a file share for the file system.
5. Set a migration policy.

Note that when file systems are restored, the creation of hard links is disabled.

Due to the amount of time it takes to completely restore a file system, there is the possibility that a client might unknowingly access data that has not yet been restored. This can cause access attempts to fail due to timeouts occurring from the CIFS client. Timeouts occur when it takes too long to display the intended files because the parent directory contains a large amount of data. If a network error or some other error is displayed on the CIFS client, wait a while, and then try to access the file again.

If backups are saved to tape devices, restore the tape device data as well.

If an error occurs during migration, some files might not be restored. If this happens, restore the files from a past version directory. If files cannot be restored from the past version directory, restore the files by performing the following procedure:

1. Make sure the restored files do not have any inconsistencies by executing the `hcporphanrestore` command without the `--display` option.
2. If inconsistencies exist in any recovered files, copy the recovered files to an appropriate location.

   Files that have inconsistencies will be recovered to either of the following directories:

   If data has been migrated to the HCP system at the file system level:

   `/mnt/`*`file-system-name`*`/.lost+found/`

   If data has been migrated to the HCP system at the share level:

   `/mnt/`*`file-system-name`*`/`*`shared-directory-name`*`/.lost+found/`

You can perform this procedure while the file system is operating. However, if you migrate the file system to the HCP system during the execution of the procedure above, files that do not have any inconsistencies might also be recovered. Make sure that no recovered files exist in the file system before copying the recovered files.

Restoring a file system from the replica HCP system when a failure occurs on both the file system and the primary HCP system

If a failure occurs on a file system and the primary HCP system, the file system can be restored from the replica HCP system to the HDI system.

1. Perform a failover from the replica HCP system, and put the file system in a state where both read and write operations are permitted.
2. Set the host name of the replica HCP system for the HCP host name by using the `archcpset` command or the GUI.
3. Re-create the file system that will perform a migration operation for the HCP system by using the `fscreate` command or the GUI.

   Specify a file system size that is equal to or larger than that of the file system in which the failure occurred. In addition, make sure that the following settings are the same as those for the file system in which the failure occurred:

   - ACL type
   - How the HCP system is linked to (at the file system or share level)
   - Whether the home-directory-roaming functionality is enabled
   - Whether older versions of files are shown to clients
   - Whether the WORM function is enabled
   - Whether CIFS bypass traverse checking is enabled

   If the file system in which the failure occurred supported 64-bit inodes, use the `fsinodectl` command to set the file systems to support 64-bit inodes. If you restore the data in a file system that does not support 64-bit inodes, the number of files might exceed the maximum number of files that can be created in the file system.
4. Mount the file system with both read and write operations permitted.
5. Restore the file system from the replica HCP system to the HDI system by using the `arcrestore` command. #

Note:

- You cannot execute the `arcrestore` command if files or directories have already been created in the file system that you want to restore. If a file share has been created before executing the `arcrestore` command, data restoration from the HCP system might fail.
- If restoration is interrupted with message KAQM37080-E, take appropriate action according to the message. Then, re-execute the `arcrestore` command with the `--skip` option specified.

6. Create a file share for the file system.
7. Set a migration policy.
8. Start operation from the replica HCP system.
9. Recover the primary HCP system from the failure.
10. Perform a data recovery from the replica HCP system, and then copy the data on the replica HCP system to the primary HCP system.
11. Finish the data recovery between the primary HCP system and the replica HCP system.
12. Reset the host name of the primary HCP system for the HCP host name by using the `archcpset` command or the GUI.

13. Start operation from the primary HCP system.

Note: If data must be made immediately accessible, you can do so by performing from steps 2 to 5. This will, however, cause the recovery of some past version directories to fail in step 4, because the replica HCP system will be in the read-only status.

If an error occurs during migration, some files might not be restored. If this happens, restore the files from a past version directory. If files cannot be restored from the past version directory, restore the files by performing the following procedure:

1. Make sure the restored files do not have any inconsistencies by executing the `hcporphanrestore` command without the `--display` option.
2. If inconsistencies exist in any recovered files, copy the recovered files to an appropriate location.

   Files that have inconsistencies will be recovered to either of the following directories:

   If data has been migrated to the HCP system at the file system level:

   `/mnt/`*`file-system-name`*`/.lost+found/`

   If data has been migrated to the HCP system at the share level:

   `/mnt/`*`file-system-name`*`/`*`shared-directory-name`*`/.lost+found/`

You can perform this procedure while the file system is operating. However, if you migrate the file system to the HCP system during the execution of the procedure above, files that do not have any inconsistencies might also be recovered. Make sure that no recovered files exist in the file system before copying the recovered files.

#: The most recent data might not be copied to the replica HCP system for files that have been updated within three hours of the time noted in **Backlog time**, which can be checked from the replica HCP window.

Restoring data from the HDI system to the HCP system when stub processing are not performed for migrated files

If stub processing is not performed on files migrated to the HCP system and a failure occurs on the HCP system, and then the HCP system is initialized during recovery, restore data from an HDI system to the HCP system.

To restore data from an HDI system to the HCP system when stub processing is not performed for migrated files:

1. Verify the migration information by executing the `archcpget` command with the `--migrate-info` option.

   Verify the migration-destination namespace and the namespace in which the system configuration information is saved.
2. Create a tenant as well as the namespaces verified in step 1 on the HCP system.

Set the user account permissions so that the account can access all namespaces that were created.

3. Verify the connection to the namespaces created in step 2 by executing the `hcpaccesstest` command with the `--namespace` *namespace-name* option.
4. Transfer the system configuration information to the HCP system by executing the `syslusave` command with the `-d trans` option.
5. Set up all file systems whose data is migrated to the HCP system for migration by executing the `arccorrection` command.

   Specify the options as follows:

   `arccorrection -t all -V --file-system` *file-system-name*

   If the KAQM37140-E message is output after the KAQM37137-I and KAQM37378-I messages for the operation result, after taking action according to the KAQM37140-E message, re-execute the `arccorrection` command. If the KAQM37137-I and KAQM37378-I messages are not output, verify the specified options, and then execute the `arccorrection` command.

   When a migration is performed after the `arccorrection` command is executed, the file system data is migrated to the HCP system. If you want to immediately migrate data to the HCP system, set up a new policy that will immediately execute a migration.

Restoring system configuration information

This subsection describes how to take action when the system configuration information is invalid due to an error that occurred in the OS disk of a node, or the cluster management LU. Work with maintenance personnel to resolve any problems. If data is migrated to an HCP system, you can restore the system configuration information and user data from the HCP system in a batch operation. To restore the system configuration information and user data from the HCP system in a batch operation, see Restoring system configuration information and user data in batch on page 4-29.

Restoration procedures differ depending on the failed component as follows.

When a failure occurs in an OS disk in one of the nodes:

See When an error occurs on an OS disk on page 4-26.

When an error occurs in the cluster management LU:

See When an error occurs in a cluster management LU on page 4-26.

When failures occur in both OS disks or at least one failure occurs in an OS disk and at least one error occurs in the cluster management LU:

See When an error occurs on the OS disk of a node or the cluster management LU on page 4-27.

When an error occurs on an OS disk

If the system configuration information is invalid due to an error that occurred in the OS disk of a node, a system administrator needs to restore the system configuration information on the OS disk.

To restore the system configuration information when an error has occurred in the OS disk of a node:

1. Ask maintenance personnel to replace the hardware in which the error occurred and to perform initial setup.

   Notes:

   Do not execute the GUI **Configuration Wizard** after the maintenance personnel finish the initial setup.

   If you execute the **Configuration Wizard**, the attempt to restore system configuration information will fail.

2. Prepare the SSH secret key on the management console.

   The secret key is provided in a file on the installation media, but the file to be used differs depending on the situation. Use the appropriate file as shown below.

   To use PuTTY

   installation-media-drive:`system\ssh\defaultsetupkeyputty.ppk`

   To use an SSH client other than PuTTY

   installation-media-drive:`system\ssh\defaultsetupkey`

   Use this key to log in to the node to be recovered with the account for SSH `nasroot`, and then execute the commands in the following steps. The corresponding public key is automatically deleted from the node after you complete step 4 of the procedure.

3. Check the fixed IP address of the other node.
4. Restore the OS disk by using the `syslurestore` command with the fixed IP address specified, that you checked in step 3.

   Execute the command on the node of the OS disk on which the error occurred.

5. Start the restored node.
6. Fail back the resource group to the restored node.
7. If you were using an NDMP server, change the password of the NDMP server.

   If you were using an NDMP server, the password of the NDMP server will be initialized. Change the password to prevent unauthorized access.

When an error occurs in a cluster management LU

If the system configuration information is invalid due to an error that occurred in the cluster management LU, a system administrator needs to restore the system configuration information on the cluster management LU.

To restore the system configuration information when an error has occurred in the cluster management LU:

1. Ask maintenance personnel to replace the hardware in which the error occurred.

   Notes:

   Do not execute the GUI **Configuration Wizard** after the maintenance personnel finish replacing the hardware.

   If you execute the **Configuration Wizard**, the attempt to restore system configuration information will fail.

2. Restore the cluster management LU by using the `syslurestore` command.

   Execute the command on either node.

3. Redefine the cluster.
4. Start the cluster and all resource groups.
5. Reconfigure the NFS service information and the virtual IP address information if a warning message appears that prompts you to reconfigure the information.

When an error occurs on the OS disk of a node or the cluster management LU

If the system configuration information is invalid due to an error that occurred in the OS disk of a node or the cluster management LU, the system administrator must restore the system configuration information on the OS disks of both nodes and the cluster management LU. Note that even after the system configuration is restored, the management server authentication password registered on the node is still the initial password. Perform step 8 to change the password if necessary.

Note that after you use the `syslurestore` command to restore the system configuration information, to execute commands, you will need the SSH secret key that corresponds to the SSH public key that was registered in the node before the error occurred. Check the SSH secret key and ensure that it is usable before beginning this procedure.

To restore the system configuration information when an error occurred in the OS disks of the nodes or the cluster management LU:

1. Ask maintenance personnel to replace the hardware in which the error occurred and to perform the initial setup.

   Notes:

   Do not execute the GUI **Configuration Wizard** after the maintenance personnel finish the initial setup.

   If you execute the **Configuration Wizard**, the attempt to restore system configuration information will fail.

2. Prepare the SSH secret key on the management console.

The secret key is provided in a file on the installation media, but the file to be used differs depending on the situation. Use the appropriate file as shown below.

To use PuTTY

installation-media-drive:`system\ssh\defaultsetupkeyputty.ppk`

To use an SSH client other than PuTTY

installation-media-drive:`system\ssh\defaultsetupkey`

Use this key to log in to the node with the account for SSH `nasroot`, and then execute the commands in the following steps. The corresponding public key is automatically deleted from the node after you complete step 4 of the procedure.

3. Upload the downloaded system configuration file.

   Upload the file on either node.

   If you use the GUI to upload the file, use the initial password of the management server.

   To upload a system configuration file:

   a. In the **Advanced** subtab of the **Settings** tab in the *physical-node* subwindow, click **Backup Configuration** to open the **Save System Settings Menu** page of the **Backup Configuration** dialog box.

   b. Click the **Upload Saved Data** button.

   c. From the **Upload Saved Data** page, click the **Upload** button.

   d. For **Saved file** on the **Select Saved Data File** page, use an absolute path for the path to the system configuration file to be uploaded, and then upload the file. Click the **Browse** button to view the file names.

4. Restore all system LUs by using the `syslurestore` command.

   Execute the command on the node on which you uploaded the system configuration file in step 3.

   The system configuration information is restored on the OS disks of both nodes and the cluster management LU. The public key that was registered before the error occurred will also be restored. Next time you log in, use the SSH secret key that corresponds to the restored public key.

5. Redefine the cluster.

6. Start the cluster and the resource groups.

7. Check whether error messages related to file systems or file shares have been output.

   If error messages related to file systems or file shares have been output, revise the system connections and settings, and then take action according to the messages. After resolving any issues, re-create the file shares.

8. If you used the GUI to upload the system configuration file, change the management server authentication password registered on the node and in File Services Manager.

   Change the management server authentication password registered on the node, and then register the same password in File Services Manager.

Use the `hnasmpasswd` command to change the management server authentication password registered on the node.

9. Ask NFS clients to mount the file shares.
10. Delete the uploaded system configuration file.

    To delete the uploaded system configuration file by using the GUI:

    a. In the **Advanced** subtab of the **Settings** tab in the *physical-node* subwindow, click **Backup Configuration** to open the **Save System Settings Menu** page of the **Backup Configuration** dialog box.

    b. Click the **Upload Saved Data** button.

    c. From the **Upload Saved Data** page, click the **Delete** button to delete the system configuration file.
11. If you were using an NDMP server, change the password of the NDMP server.

    If you were using an NDMP server, the password of the NDMP server will be initialized. Change the password to prevent unauthorized access.

Restoring system configuration information and user data in batch

This subsection explains what to do if the system configuration file is saved to an HCP system, user data is migrated to the same HCP system, and the system configuration information and user data become invalid due to an error occurring on the OS disk of a node, the cluster management LU, or a user LU. Use the system configuration information and the user data that is saved in the HCP system to perform a restoration. Work with maintenance personnel to resolve any problems. In addition, make sure you know the HCP information (the host name (FQDN), IP address, tenant name, and account information) in advance.

Note that after you use the `syslurestore` command to restore the system configuration information and the user data, to execute commands, you will need the SSH secret key that corresponds to the SSH public key that was registered in the node before the error occurred. Check the SSH secret key and ensure that it is usable before beginning this procedure.

To restore the system configuration information and user data when an error has occurred on the OS disk of a node, the cluster management LU, or a user LU:

1. Ask maintenance personnel to replace the hardware in which the error occurred and to re-initialize everything.

   After this is done, acquire the information regarding the data port that communicates with the HCP system (the IP address, netmask, and routing information).

   Notes:

   Do not execute the GUI **Configuration Wizard** after the maintenance personnel finish the initial setup.

If you execute the **Configuration Wizard**, the attempt to restore system configuration information will fail.

2. Prepare the SSH secret key on the management console.

   The secret key is provided in a file on the installation media, but the file to be used differs depending on the situation. Use the appropriate file as shown below.

   To use PuTTY

   installation-media-drive:`system\ssh\defaultsetupkeyputty.ppk`

   To use an SSH client other than PuTTY

   installation-media-drive:`system\ssh\defaultsetupkey`

   Use this key to log in to the node with the account for SSH `nasroot`, and then execute the commands in the following steps. The corresponding public key is automatically deleted from the node after you complete step 5 of the procedure.

3. If a proxy server was used for communication with the HCP system, use the `arcproxyset` command to set the proxy server information.

   Make sure to specify the IP address, not the host name, of the proxy server. Host names cannot be resolved until the system configuration information is restored.

4. If HTTP was used for communication with the HCP system, use the `arcsslctl` command to change the communication protocol to HTTP.

5. Restore the system configuration information and user data by using the `syslurestore` command.

   Specify the `--trans` option, and then execute the `syslurestore` command. If multiple pieces of the system configuration information are saved on a single tenant, also use the `--system-name` option to specify the name of the cluster when you saved the system configuration information.

   The public key that was registered before the error occurred will also be restored. Next time you log in, use the SSH secret key that corresponds to the restored public key.

   If the KAQM13186-W message is output, after re-defining the cluster in the next step, check the system messages for error details, re-create any file systems, and then restore the backup data. For details about how to re-create file systems and restore backup data, see Restoring a file system migrated to an HCP system on page 4-21.

6. Re-define the cluster.

7. Start the cluster and the resource group.

8. Check whether error messages related to the file system or file shares have been output.

   If error messages related to the file system or file shares have been output, revise the system connections and settings, and then take action according to the messages. After resolving any issues, re-create the file shares.

9. Change the management server authentication password registered on the node and in File Services Manager.

   Change the management server authentication password registered on the node, and then register the same password in File Services Manager. Use the `hnasmpasswd` command to change the management server authentication password registered on the node.

10. Ask NFS clients to mount the file shares.
11. If you were using an NDMP server, change the password of the NDMP server.

    If you were using an NDMP server, the password of the NDMP server will be initialized. Change the password to prevent unauthorized access.

Note that the following information cannot be restored:

- The configuration information for the file system that was not mounted when saving the information, including:
  - The minimum and maximum retention periods
  - The auto commit settings
  - Whether to send requests to delete files stored in an HCP system
  - 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
- Configuration information regarding the initial mode for executing a migration task or single-instancing task
- User data that has not been migrated to an HCP system
- The configuration information for 64-bit inodes

Default values are used for the configuration information listed above for file systems that have not been mounted. Change the settings as necessary. Also, if the file system that supported 64-bit inodes existed before the error occurred, after executing the `syslurestore` command, use the `fsinodectl` command to set the file systems to support 64-bit inodes. If a file system does not support 64-bit inodes, the number of files might exceed the maximum number of files that can be created in the file system. In addition, when file systems are restored, the creation of hard links is disabled.

If an error occurs during migration, some files might not be restored. If this happens, restore the files from a past version directory. If files cannot be restored from the past version directory, restore the files by performing the following procedure:

1. Make sure the restored files do not have any inconsistencies by executing the `hcporphanrestore` command without the `--display` option.
2. If inconsistencies exist in any recovered files, copy the recovered files to an appropriate location.

Files that have inconsistencies will be recovered to either of the following directories:

If data has been migrated to the HCP system at the file system level:

`/mnt/file-system-name/.lost+found/`

If data has been migrated to the HCP system at the share level:

`/mnt/file-system-name/shared-directory-name/.lost+found/`

You can perform this procedure while the file system is operating. However, if you migrate the file system to the HCP system during the execution of the procedure above, files that do not have any inconsistencies might also be recovered. Make sure that no recovered files exist in the file system before copying the recovered files.

Recovering from FC path errors

If there is a possibility that an error occurred in the FC path, the system administrator can check the status of the FC path from the **FC Path** subtab under the **Network** tab in the Health Monitor subwindow or the `fpstatus` command, and then recovers from the error if necessary.

When Error is displayed for one of the paths to a given target

If `Error` is displayed as the status of a path to a given target, any of the following might have occurred or been performed:

(a) An error occurred in the FC path because of a reason such as a disconnected FC cable.

(b) The OS has not been restarted after you changed or deleted an FC path.

(c) The FC path is not set up properly because no LUs have been assigned to the host group for the FC path.

For (a) and (b), take action according to the procedure below. For (c), take action according to the procedure in When Unknown is displayed for both paths to a given target on page 4-35.

To correct Error displayed for path to a given target

1. Check the model name (`Model`) and serial number (`Serial`) for the path whose status is `Error`, to identify the storage system.
2. Check the status of the FC port on the node (`HostPort`) for this path, FC cable connected to the FC port on the storage system (identified in step 1) (`ArrayPort`), and the FC switches.

   If an error occurred:

   Remove the cause of the error, and then place the relevant FC path online by using the `fponline` command.

   If no error occurred:

   Restart the OS.

3. Check the statuses of the relevant FC paths by using the `fpstatus` command.

When Online (LU Error) is displayed for both paths to a given target

If `Online (LU Error)` is displayed as the status for both paths to a given target, a temporary failure might have occurred in the paths, or an error might have occurred in one or more of the LUs accessed over those paths.

The following procedure might correct the problem of `Online (LU Error)` being displayed because of a temporary path failure (or for any other reason).

1. Place the relevant FC paths online by using the `fponline` command.
2. Check the statuses of the relevant FC paths by using the `fpstatus` command.

If the error is still not resolved, perform the following procedure:

1. Work with maintenance personnel to recover the LU(s) from the error. If the LU where the error occurred is used by a file system, take action according to the procedure described in Recovering from file system errors on page 4-15.
2. Place the relevant FC paths online by using the `fponline` command.
3. Check the statuses of the relevant FC paths by using the `fpstatus` command.

When Error is displayed for both paths to a target

If `Error` is displayed as the status for both paths to a given target, either of the following might have occurred or been performed:

(a) An error occurred in all LUs accessed via those FC paths, or an error occurred in the paths themselves.

(b) The OS has not been restarted after you changed or deleted an FC path.

(c) The FC path is not set up properly because no LUs have been assigned to the host group for the FC path.

For (a) and (b), take action according to the procedure below. For (c), take action according to the procedure in When Unknown is displayed for both paths to a given target on page 4-35.

To correct Error when displayed for both paths to a target

1. Check the model name (`Model`) and serial number (`Serial`) for the path whose status is `Error`, to identify the storage system.
2. Check the status of the FC port on the node (`HostPort`) for this path, the FC cable connected to the FC port (`ArrayPort`) on the storage system (identified in step 1), and the FC switches.

   If an error occurred:

Remove the cause of the error, and then go to step 3.

If no error occurred:

Restart the OS, and then confirm that the status of the FC path is displayed correctly.

3. From the node that is working properly, check the status of the resource group that was running on the node where the path failure occurred.

   If the resource group was failed over:

   Go to step 5.

   If the resource group was not failed over:

   Go to step 4.

4. From the node that is working properly, force stop the resource group that is running on the node where the path failure occurred.
5. From the node that is working properly, check the status of the node where the path failure occurred.

   If the status is `UP` or `DOWN`:

   Go to step 6.

   If the status is something other than `UP` or `DOWN`:

   Go to step 7.

6. From the node that is working properly, force stop the node where the path failure occurred.
7. Restart the OS on the node where the path failure occurred.

   Execute the `nasreboot` command with the `--force` option.

8. On the node where the path failure occurred, start the node itself.

   Which step is performed next depends on the state of the resource group in step 3.

   If the resource group was failed over to the node where the path failure occurred:

   Go to step 11.

   If the resource group was failed over to the node that was working properly:

   Go to step 10.

   If the resource group was not failed over:

   Go to step 9.

9. On the node where the path failure occurred, start the resource group that was stopped in step 4.

   After the resource group has been restarted, go to step 11.

10. From the node where the path failure occurred, fail back the resource group that was failed over to the node that is running properly.
11. Check the statuses of the target FC paths by using the `fpstatus` command.

If the FC path status is normal, end the procedure here. If the FC paths are still in an error status or a file system on the recovered FC path is blocked, go to step 12.

12. Work with maintenance personnel to recover the LUs from the error.

    If the LU where the error occurred is being used by a file system, take action according to the procedure described in Recovering from file system errors on page 4-15. If the LU where the error occurred is being used as the cluster management LU, see Restoring system configuration information on page 4-25.

13. Check the status of the relevant FC paths.

When Configuration Mismatch is displayed for both paths to a given target

If `Configuration Mismatch` is displayed as the status for both paths to a given target, allocation of LUs to the host groups for one FC path might differ from the allocation for the alternate path.

To correct Configuration Mismatch status when displayed for both paths to a given target

1. Check the model name (`Model`) and serial number (`Serial`) for the path whose status is `Configuration Mismatch`, to identify the storage system.
2. If no alternate path is set, ask maintenance personnel to set one.
3. Check whether the same LUs are allocated to each host group set up for the FC port on the storage system (`ArrayPort`) identified in step 1.

   If the settings differ, re-allocate the LUs so that the settings are the same for each host group. If you need to move or delete LU paths when allocating LUs, see the *Cluster Administrator's Guide*.
4. Check the status of the relevant FC paths.

When Unknown is displayed for both paths to a given target

If `Unknown` is displayed for both paths to a given target, a possible cause is that the host port or storage port cannot be identified. If this happens, or when the FC path is not set up properly because no LUs have been assigned to the host group for the FC path, take action according to the following procedure.

To correct when Unknown is displayed for both paths to a given target

1. Check whether the HBA card is installed properly.
2. Check whether the FC port on the storage system (`ArrayPort`) for this path is set up correctly.

   If the FC port is not set up correctly, ask maintenance personnel to reconfigure the FC path.

3. Check the status of the FC port on the node (`HostPort`) for this path, FC cable connected to the FC port on the storage system (`ArrayPort`), and FC switches.
4. Ask the SAN administrator to check the host security for this path.
5. Ask the SAN administrator to allocate the same LUs to each host group set up for the FC port on the storage system (`ArrayPort`) for this path.

   If you need to move or delete LU paths when allocating LUs, see the *Cluster Administrator's Guide*.
6. Check the status of the relevant FC paths.

When Partially Online is displayed for a specific FC path

If `Partially Online` is displayed as the status for a specific FC path, an LU might be inaccessible because some of the FC paths are `Offline`.

To correct when Partially Online is displayed for a specific FC path

1. Place the relevant FC paths online by using the `fponline` command.
2. Check the status of the relevant FC paths.

When Configuration Mismatch is displayed for one of the paths to a given target

If `Configuration Mismatch` is displayed as the status for one of the paths to a given target and nothing is displayed for the other path, an alternate path might not be set up. Take action according to When Error is displayed for one of the paths to a given target on page 4-32, regarding the status of the path for which nothing is displayed as `Error`.

When FC path information is not displayed

If a connected FC path is not displayed, an error might have occurred in the FC path during the startup of the OS.

To correct when FC path information is not displayed

1. Check the connections of the FC cables and the FC switches used for the relevant paths, and then remove the cause of the error.
2. Check the status of the relevant FC paths again.

Using interface and network error information for error recovery

If an error occurs in the interface or network, a system administrator checks the status of the error in the **List of Interfaces** page of the **Network & System Configuration** dialog box and recovers the error by working with maintenance personnel as necessary.

When Unknown is displayed

If the node that you are not accessing, among the nodes making up the cluster, is marked `Unknown` in the **List of Interfaces** page of the **Network & System Configuration** dialog box, perform the action described below.

Check whether the OS is running.

Check whether the OS is running on the node that you are not accessing among the nodes that make up the cluster.

If the OS is not running, turn on the power to the node to start the OS.

After starting the OS, recheck the interface and network information in the **List of Interfaces** page.

Check the IP address for the management port

Check whether the fixed IP address and netmask for the management port are specified correctly. If the specified value is incorrect, specify the correct value.

Specify the fixed IP address and netmask for the management port in the **Edit Interface** page.

After specifying the correct values for the fixed IP address and netmask, recheck the interface and network information in the **List of Interfaces** page.

Check the LAN cable

Make sure that the LAN cable is connected correctly. If not, reconnect the LAN cable, and then recheck the interface and network information in the **List of Interfaces** page.

Check communication devices such as hubs

Make sure that there are no problems with communication devices such as hubs. If a problem exists in a communication device such as a hub, remove the problem and recheck the interface and network information in the **List of Interfaces** page.

Check the negotiation mode of the management port

Make sure that the negotiation mode setting of the management port is the same as that of the switch. If they are not the same, specify the same negotiation mode. Depending on the switch type, even if the auto negotiation mode is specified for both management port and the switch, they might not be able to communicate with each other. If this happens, specify a fixed negotiation mode so that the setting will be the same for the management port and the switch.

You can specify the negotiation mode in the **Negotiation Mode Setup** page.

After specifying the negotiation mode, recheck the interface and network information in the **List of Interfaces** page.

If `Unknown` is still displayed in the **List of Interfaces** page even after taking the above actions, contact maintenance personnel.

When Invalid is displayed for the management port

Among the nodes making up the cluster, if the node that you are not accessing is marked `Invalid` for the management port in the **List of Interfaces** page of the **Network & System Configuration** dialog box, check the IP address settings.

If `Invalid` is displayed in the display items for the fixed IP address or netmask, make sure the settings for the fixed IP address or netmask are correct. If the specified value is incorrect, specify the correct value. Specify the IP address for the management port in the **Edit Interface** page.

If `Invalid` is still displayed in the **List of Interfaces** page even after taking the above actions, contact maintenance personnel.

When Invalid is displayed for a data port

If the node that you are not accessing, among the nodes making up the cluster, is marked `Invalid` for one or more data ports in the **List of Interfaces** page of the **Network & System Configuration** dialog box, delete all the interfaces that are marked `Invalid`, and then re-add the interfaces with the correct values.

If `Invalid` is still displayed in the **List of Interfaces** page even after taking the above actions, contact maintenance personnel.

Using error information on trunking for error recovery

If an error occurs in the trunking settings, a system administrator checks the status of the error in the **List of Trunking Configurations** page of the **Network & System Configuration** dialog box, and then recovers the error.

When Down is displayed in the Link status

If `Down` is displayed in **Link status** in the **List of Trunking Configurations** page of the **Network & System Configuration** dialog box, the link might have been disconnected. The following describes actions to take when the link is disconnected:

To correct when Down is displayed in Link status

1. Check whether a cable is connected to the port in use. If the cable is not connected, connect the cable correctly.
2. Check the cable. If the link remains disconnected even though the cable is connected correctly, there might be a problem with the cable. Replace the cable.
3. Check the switch. If there is no problem with the cable, there might be a problem with the switch. In such a case, resolve the switch problem.
4. If there is no problem with the cable or switch, there might be a problem with the HDI system hardware. Contact maintenance personnel to resolve the problem.

When Not aggregated is displayed in Aggregate of LACP

If `Not aggregated` is displayed in **Aggregate** of **LACP** in the **List of Trunking Configurations** page of the **Network & System Configuration** dialog box, wait for 10 seconds or more, and then click **Refresh** to update the information displayed in the dialog box. If `Not aggregated` is still displayed even after clicking **Refresh** several times, the port might not have joined link aggregation.

The following describes actions to take when the port cannot join link aggregation.

When `Up` is displayed in **Link status**:

- Make sure that the switch supports IEEE802.3ad (Dynamic LACP).
- The cable might be inserted in the wrong place. Check the cable connection between the node and the switch. If a problem exists, connect the cable correctly.
- There might be a problem in the switch settings. Verify that the link aggregation settings on the switch are the same as those on File Services Manager. If these settings do not match, configure the switch settings correctly.
- Depending on the switch type, there are limitations on the port combination that can perform link aggregation. Check the switch specifications.
- Depending on the switch type, the communication speed might become lower than expected and the port might not be able to join link aggregation even if the auto negotiation mode is set for both the port and switch. In this case, configure the fixed negotiation modes so that the settings on both the port and switch are the same.

When `Down` is displayed in **Link status**:

The link might have been disconnected. Take action according to the procedure described in When Down is displayed in the Link status on page 4-38.

When Standby is displayed in Status of Active port for the port normally in use

When Link Alternation is set, if `Standby` is displayed in **Status** for **Active port** of the port normally in use (the port selected in **Default active port** in the **Link Alternation Setup** page of the **Network & System Configuration** dialog box), an error might have occurred on the port. The following describes actions to take when an error occurs on the port normally in use.

When `Up` is displayed in **Link status**:

Select the Link Alternation port (`rdn`*number*) in the **List of Trunking Configurations** page, and then click **Change Active Port Status**. `Active` is displayed in **Status** for **Active port**, and normal operation

begins. If **Status** for **Active port** does not change to `Active`, contact maintenance personnel to resolve the error.

When `Down` is displayed in **Link status**:

The link might have been disconnected. Take action according to the procedure described in When Down is displayed in the Link status on page 4-38.

Using error information on the data port for error recovery

If an error occurs with the data port, in the **List of Data Ports** page of the **Network & System Configuration** dialog box, a system administrator checks the transmission status of the data port, and then recovers the error.

When Down is displayed in Link status

If `Down` is displayed in **Link status** in the **List of Data Ports** page of the **Network & System Configuration** dialog box, the link might have been disconnected. Take the following actions if the link has been disconnected:

Check whether a cable is connected to the port in use:

Check whether a cable is connected to the port in use. If not, connect the cable correctly.

Check the cable:

If the link remains disconnected even though the cable is connected correctly, there might be a problem with the cable. Replace the cable.

Check the switch settings:

Verify that the negotiation mode settings on the switch are the same as those on File Services Manager.

Check the switch:

If there is no problem with the cable, there might be a problem with the switch. In such a case, resolve the switch problem.

If there is no problem with the cable or switch, there might be a problem with the HDI system hardware. Contact the maintenance personnel to resolve the problem. When performing a failover as instructed by maintenance personnel for recovery from a port error, you need to perform operations from the management LAN even when the HDI system is managed from the management console located on the front-end LAN.

When an incorrect communication speed is displayed for Speed in Connected status

In the **List of Data Ports** page of the **Network & System Configuration** dialog box, if an incorrect value (an inappropriate value) is displayed for the communication speed with the switch as follows, a switch setting might be wrong: `10Base` is displayed for **Speed** in **Connected status**, or `100Base` is

displayed even though the appropriate communication speed is 1,000 Mbps. Verify that the negotiation mode settings on the switch are the same as those on File Services Manager. If these settings do not match, configure the switch settings correctly.

Depending on the switch type, the communication speed might become lower than expected even if the auto negotiation mode is set for both the port and switch. In this case, configure the fixed negotiation modes so that the settings on both the port and switch are the same.

Recovering hardware from a failure

When hardware status is not normal, recover the hardware from the failure. If you are using the GUI and notice a failure in FC paths or Ethernet interfaces, take action according to Recovering from FC path errors on page 4-32 or Using interface and network error information for error recovery on page 4-36. For other failures, execute the `hwstatus` command. If `failed` is indicated for `connection` under `BMC Information` in the execution result of the `hwstatus` command, check the network status of BMC on the other node.

For other hardware failures, contact maintenance personnel for recovery.

Recovering from a failure in which an LU cannot be detected during the startup of an OS

If any of the following problems occur during the startup of an OS, you might not be able to operate the HDI system because the OS cannot detect LUs:

- It takes longer for power to be supplied to the storage system than to the nodes.
- No power is supplied to the storage system.
- There is a connection problem with one or more FC cables.

In any of the above cases, the `KAQG10104-E` message is output as a system message.

To recover from a failure in which an LU cannot be detected during the startup of an OS

1. Turn off the power switch for the node.
   For details about how to operate the node power lamp switch, see the *Installation and Configuration Guide*.
2. Turn on the storage system power switch if it is off.
3. Check the FC cable connections, and then connect them properly if there is a problem.
4. Turn on the power switch for the node.
   The OS will be restarted.

If the same error still occurs after you perform the above procedure, contact maintenance personnel.

If a power outage occurs and the OSs start up earlier than the storage system after the power outage is recovered from, the nodes might not detect the LUs. To avoid this issue, make sure that you use the same power supply for the nodes and storage system, unless, for some reason, you need to separate the power supplies.

Recovering from a failure during a data import from another file server

If a failure occurred during a data import from another file server, take recovery action according to the type of failure.

If communication with the import-source file server has failed

If communication with the import-source file server has failed, check the following items, and correct the problem:

To check the status when communication with the import-source server has failed

1. Check the network status between the HDI system and the import-source file server. Check the communication by using the `nasping` and `nastraceroute` commands.
2. Check the status of external servers such as DNS servers and LDAP servers. Check the connection status between the nodes and the external servers in the **List of RAS Information** page (for `Server check`) in the **Check for Errors** dialog box.
3. Check the operation status of the import-source file server, network settings, share settings (share path settings), and I/O status. Check whether you can access the import-source file server with the current settings by using the `datamigrateaccesstest` command. Also check various statuses from the console of the file server if available.
4. Check the host name, IP address, share name, account, and share path that were specified when the import command was executed. Check whether the settings are correct by using the `datamigrateconflist` command. Also check whether you can access the import-source file server with the current settings by using the `datamigrateaccesstest` command.

When an I/O failure occurred in the HDI system

When an I/O failure occurred in the HDI system, take action according to the content of the message that was output.

Table 4-5 The messages and action to take when an I/O failure occurred in the HDI system during a data import from another file server

Message content	Action	See
Insufficient capacity of the file system	Delete unnecessary files or expand the file system to make enough space for the file system.	N/A
FC path failure	Follow the recovery procedure for FC path failure.	Recovering from FC path errors on page 4-32
LU failure	Follow the recovery procedure for when a file system is blocked because of a storage system failure.	Recovering from file system errors on page 4-15
File system blockage	Follow the recovery procedure for when a file system is blocked.	Recovering from file system errors on page 4-15
Note: N/A = Not applicable.		

When the importing of some files fails

After a data import finishes, run the `datamigratestatus` command with the `--migfailedlist` option specified to verify the import results. If there are files for which importing failed, recover from the failure according to the action for the output error messages. After recovery, start the import procedure again from the execution of the `datamigratestart` command.

If some files failed to be imported because an account specified as a file owner or the ACE is deleted from the file server environment of the import-source, the action you take depends on whether the account mapping of HDI is already set up. Take action according to the following If the account mapping is already set up on page 4-43 or If the account mapping is not set up on page 4-44:

If the account mapping is already set up

If the account mapping is already set up, the following steps show how to deal with an import failure due to accounts being deleted from the file server environment of the import-source:

1. With HDI, specify the `--mapdef` option, execute the `datamigrateconflist` command, and save the output mapping information as a file.
2. Check the SID of the deleted account (or accounts), by using the properties of the file on the import-source file server.

   An SID is displayed as a character string that consists of alphanumeric characters starting with an `S`, or hyphens in a group-name field or a user-name field. Record all SIDs that are displayed.
3. Add mapping entries that correspond to the SIDs obtained in Step 2, at the end of the mapping file created in Step 1.

Specify the following values for each item (nothing must be specified for SRC_NAME).

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

The following shows an example of specifying values to items:

```
[MAPDEF]
SID=S-1-5-21-2348534987-2915341303-3818173629-10003
SRC_NAME=
KIND=u
DST_NAME=usr10003
```

Use UTF-8 encoding.

4. If an account that was specified as DST_NAME in Step 3 is not yet registered, register the account to HDI or an external server.
5. Transfer the mapping file to HDI.

   Transfer the mapping file to the directory below the home directory of an SSH account (/home/nasroot).
6. With HDI, specify the --mapdef option and the mapping file name, execute the datamigrateconfedit command, and reset the mapping.
7. Perform the import procedure again by executing the datamigratestart command.

If the above steps do not work, specify the --migrate-replace-owner option, execute the arcconfedit command, set the account name to be assigned to the deleted accounts, and start performing the import procedure by executing the datamigratestart command. After the import is completed, execute the arcconfedit command with two double quotation marks ("") or two single quotation marks ('') specified for the --migrate-replace-owner option in order to delete the allocated account settings.

If the account mapping is not set up

If the account mapping is not set up, the following steps show how to deal with an import failure due to accounts being deleted from the file server environment of the import-source:

1. Check the SID of the deleted account (or accounts), by using the properties of the file on the import-source file server.

   An SID is displayed as a character string that consists of alphanumerical characters starting with an S or hyphens in a group-name field or a user-name field. Record all SIDs that are displayed.
2. Create a new file, and add mapping entries that correspond to the SIDs obtained in Step 1.

   Specify the following values for each item (nothing must be specified for SRC_NAME).

   ```
   [MAPDEF]
   SID=obtained-SID-value
   ```

```
SRC_NAME=
KIND=u(user) or g(group)
DST_NAME=import-target-account-name
```

The following shows an example of specifying values to items:

```
[MAPDEF]
SID=S-1-5-21-2348534987-2915341303-3818173629-10003
SRC_NAME=
KIND=u
DST_NAME=usr10003
```

Use UTF-8 encoding.

3. If an account that was specified as `DST_NAME` in Step 2 is not yet registered, register the account to HDI or an external server.
4. Transfer the created mapping file to HDI.

   Transfer the mapping file to the directory below the home directory of an SSH account (`/home/nasroot`).
5. With HDI, specify the `--mapdef` option and the mapping file name, execute the `datamigrateconfedit` command, and reset the mapping.
6. Perform the import procedure again by executing the `datamigratestart` command.

If the above steps do not work, specify the `--migrate-replace-owner` option, execute the `arcconfedit` command, set the account name to be assigned to the deleted accounts, and start performing the import procedure by executing the `datamigratestart` command. After the import has completed, execute the `arcconfedit` command with two double quotation marks ("") or two single quotation marks ('') specified in the `--migrate-replace-owner` option in order to delete the allocated accounting settings.

When import settings are deleted before an import finishes

If you delete the import settings by using the `datamigrateconfdel` command before all files are imported, and a client accesses the image of a file that was not import, an access error occurs. If you need the file, start the import procedure again from the execution of the `datamigrateconfadd` command. If you do not need the file, execute the `datamigrateconfadd` command, execute the `datamigratestart` command with the `--type on-demand` option specified, and then delete the file.

If name resolution of an account fails

If name resolution of an account fails, check that the system can connect to the external servers, such as the DNS servers and LDAP servers, on the **List of RAS Information** page (for `Server check`) of the **Check for Errors** dialog box. Also make sure that the account is registered to the external server. If the system can connect to the external server and the account is registered, check that the mapping is correct with the `datamigrateconflist` command. If the mapping is not set, set the mapping with the

datamigrateconfedit command. After setting the mapping, continue the import procedure.

If multibyte characters are included in an account name

If multibyte characters are included in an account name of the import-source, change the import-target account name (DST_NAME) of the target account to a name without multibyte characters, based on the information output from a mapping generation tool (sidlist.exe). After that, register the account to HDI or an external server, and reset the mapping with the datamigrateconfedit command. After resetting the mapping, continue the import procedure.

Recovering from a failure related to Backup Restore functionality

This section describes the actions that the system administrator must take when a failure occurs while using Backup Restore functionality. If you cannot identify the cause of an error or resolve the problem, contact maintenance personnel.

If you can identify the cause of an error from the error messages, check the required recovery procedure to resolve the problem.

When a problem exists on the connection between a backup or media server and the NDMP server

If a problem exists on the connection between a backup or media server and the NDMP server, perform the following operations to check for a connection error or setting error, and then take appropriate action:

- Use the nasping command to check the status of the network and routing.
- In the **Network & System Configuration** dialog box, on the **List of Interfaces** and **List of Routings** pages, check the interface information and routing information.
- Use the backup management software to check whether the user name and password registered on the backup server and those registered on the NDMP server and media server are the same.

  For details on how to use the backup management software for checking, see the supplementary Backup Restore documentation that is provided with HDI.
- On the **Edit System File** page in the **Network & System Configuration** dialog box, check the contents of the /etc/hosts file, and then correct the information for the registered backup servers.
- On the **List of RAS Information** page (for List of other log files) in the **Check for Errors** dialog box, check the NDMP server log (/enas/

log/ndmpserver.log), and then take action as indicated by the messages.

When a problem exists in the execution status of a job or in the status of a tape device

While a backup or restore job, which is using a tape device connected to a node via a SAN, is running, a failover or an error on the connection to the tape device or on the tape device might cause problems. For example, the job might not be able to terminate or the backup media might not be ejected from a drive in the tape device.

If such a problem occurs, use the following procedure to resolve the problem, and then restart the operation.

1. Check whether there are any jobs in progress or waiting for execution.
   Cancel any jobs in progress. If there are any queued jobs, take appropriate action such as canceling these jobs, so that backup or restore operations are not performed.
2. Check whether there is backup media in tape drives.
   If backup media is in the tape drives, proceed to steps 3 and 4.
3. Eject the backup media from the tape drives.
   Reset the drives in which backup media remains.
4. Confirm that the backup media has been ejected from the tape drives.
   If the backup media is not ejected from the tape drives, manually eject the backup media from the tape device. For details on how to operate the tape device, see the documentation from the tape device vendor.
5. Check that the tape device is operating normally.
   If an error has occurred on the tape device, see the documentation from the tape device vendor, and then take appropriate action.

If the problem has not been resolved even after following this procedure, contact maintenance personnel.

When the connection between a tape drive and node is blocked

When the connection between a tape drive and node is blocked, perform the following procedure to correct the blocked connection:

1. Stop the NDMP server.
2. Unplug the FC cable connected to the tape device.
   Unplug the FC cable used to connect the tape drive to the node.
3. Wait until the OS on the node connected to the tape drive no longer recognizes the device.
   It might take as long as 30 seconds for the device to no longer be recognized.
4. Check whether a problem has occurred on the tape drive.

If a problem has occurred, see the documentation provided by the vendor to resolve the problem.

5. Execute the `tapelist` command with the `-A`, `-d`, and `-t WWN:LUN` options specified.

   Check that the `Status` of the tape drive specified in `WWN:LUN` is `N,A`. If `N,A` is not displayed for `Status`, restart the OS on the node connected to the tape drive.

6. Reconnect the FC cable that was unplugged in step 2 to the tape device.
7. Start the NDMP server.

If timeouts occur frequently during Backup Restore processing

Other operations might be executing at the same time. Make sure that multiple operations or schedules are not executed at the same time.

If the same error still occurs even after you revise the operations, collect the error information from the time at which the timeout occurs, and then contact maintenance personnel.

Performing a backup or restore operation while the system is running in a degenerated mode

This subsection describes how to perform a backup or restore operation that uses a tape device connected to a node via a SAN while the system is running in degenerate mode.

Notes on performing a backup or restore operation while the system is running in degenerate mode

Note the following when performing a backup or restore operation while the system is running in degenerate mode.

- A failover occurring while a backup or restore job is running might cause problems. For example, the job might not be able to terminate or the backup media might not be ejected. If such problems occur, take appropriate action as described in When a problem exists in the execution status of a job or in the status of a tape device on page 4-47, and then restart the job.

When both nodes share the tape drive

To perform a backup or restore operation when both nodes share the tape drive:

1. Use backup management software to confirm that the tape drive to be used for the operation is available.
2. Perform a backup or restore operation.

After failback, use the backup management software to confirm that the tape drive being used is available.

When both nodes use separate tape drives

To perform a backup or restore operation when both nodes use separate tape drives:

1. Stop the failover-destination NDMP server by using the `ndmpcontrol` command.
2. Register the tape drive being used with the failover-source node on the NDMP server of the failover-destination node.
   Specify the `-t` option, *WWN*, and *LUN* in the `tapeadd` command, and then register the specific tape drive on an NDMP server.
3. Start the failover-destination NDMP server by using the `ndmpcontrol` command.
4. Use backup management software to confirm that the tape drive to be used for the operation is available.
5. Perform a backup or restore operation.

After failback, perform the following procedure to unregister the tape drive information registered when performing a backup or restore operation, and then use the backup management software to confirm that the tape drive being used is available.

1. Stop the NDMP server by using the `ndmpcontrol` command.
2. Unregister the tape drive information registered during a backup or restore operation by using the `tapedel` command.
3. Start the NDMP server by using the `ndmpcontrol` command.
4. Use backup management software to confirm that the tape drive to be used for the operation is available.

A

Installation History

This appendix explains the file to which software installation history is logged, and the data logged to the file.

Checking the software installation history log file

The System Software subwindow displays only the latest installation information. A system administrator can check the software installation history by using the installation history file (`/enas/data/pp/history/product_install.log`) of the software information log group downloaded on the **List of RAS Information** page (for `Batch-download`) in the **Check for Errors** dialog box.

In the installation history file, the installation information is output in the following format:

```
I,operation,product-name,version,operation-date-and-time
```

The following table lists and describes the information that will be output in the installation history file.

Table A-1 Information to be output in the installation history file

Item	Description

Operation	Information on the specific operation performed is output.
	`configure`
	Indicates that a new installation has been performed.
	`upgrade`
	Indicates that an upgrade installation has been performed.

Product name	The product name is displayed.
Version	The product version is displayed. This is the actual version of the system managed by the internal system. This version might differ from the version displayed in the GUI.
Operation date and time	The date and time the product was operated is displayed.

The following shows an example of information output in the installation history file:

```
I,configure,Hitachi Data Ingestor,03-01-00-00-00-00,2011/06/01 10:32:55
+0000(UTC)
```

B

Network Information

This appendix explains the file to which network information is logged, and the data logged to the file.

Checking the network information log file

System administrators can use the information in the network information log group downloaded from the **List of RAS Information** page (for `Batch-download`) of the **Check for Errors** dialog box to check routing and external server settings.

The network information log group includes the following log files:

- `enas_routelist.log`
- `log_ifconfig`
- `log_interfaces_check`

For a VLAN interface, the port name is output in the following format:

port-name.*VLAN-ID* (Example: `eth12.0010`)

Also, the information of interfaces that are used for internal communications between nodes is output to these log files.

The `log_interfaces_check` file can be viewed in **Results** of the **List of RAS Information** page (for `Server check`).

The enas_routelist.log file

The following shows an output example of the `enas_routelist.log` file.

```
node 0(D6P67NBX)  2010/01/20 20:57:59
Target          Netmask         Gateway         Flags   MSS Iface
10.208.15.1     255.255.255.255 0.0.0.0         UH        - eth2
172.19.200.0    255.255.255.0   172.19.10.1     UG      400 eth0.1000
172.16.2.0      255.255.255.0   0.0.0.0         U         - eth2
172.19.10.0     255.255.255.0   0.0.0.0         U         - eth0.1000
10.0.0.0        255.255.255.0   0.0.0.0         U         - hb0
192.168.0.0     255.255.255.0   0.0.0.0         U         - pm0
10.213.88.0     255.255.252.0   0.0.0.0         U         - mng0
default         0.0.0.0         10.213.88.10    UG        - mng0
```

The following table lists and describes the information that is output to the `enas_routelist.log` file.

Table B-1 Information that is output to the enas_routelist.log file

Output line	Output contents
Line 1	Outputs the title in the following format: *node-number* (*host-name*) *output-date-and-time* The output date and time appear in the format of *YYYY*/*MM*/*DD* *hh*:*mm*:*ss*, for example, `2004/11/22 13:14:15`.
Line 2	Outputs the column header for the items output in the third line and below.
Line 3 and below	Outputs the contents of each item: `Target`

Output line	Output contents

	Outputs the network address of the output target. For the default route, `default` is output.
	`Netmask`
	Outputs the netmask of the output target network. `255.255.255.255` is output for the host. `0.0.0.0` is output for the default route.
	`Gateway`
	Outputs the IP address of the gateway.
	`Flags`
	Outputs the following statuses of the output target network:
	`U`
	Indicates that the usual route settings are used.
	`H`
	Indicates that the host is used as the method for setting the routing destination.
	`G`
	Indicates that a gateway is set.
	`R`
	Indicates that the route is set to be dynamically reinstated.
	`D`
	Indicates the dynamic settings made by demon or replacement.
	`M`
	Indicates that dynamic settings are performed by a route control daemon or by replacement.
	`A`
	Indicates the settings are made by the `addrconf` command.
	`C`
	Indicates that a cached entry is set.
	`!`
	Indicates that a rejected route is set.
	`MSS`
	Outputs the default maximum segment in the TCP connection of this route. When a routing is added and this item is not set, – is output.
	`Iface`
	Outputs the port name.

The log_ifconfig file

The following shows an output example of the `log_ifconfig` file.

```
hb0       Link encap:Ethernet  HWaddr 00:26:b9:5b:ed:6b
          inet addr:10.0.0.21  Bcast:10.0.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

```
          RX packets:376753 errors:0 dropped:0 overruns:0 frame:0
          TX packets:376655 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:31957682 (30.4 MiB)  TX bytes:31818224 (30.3 MiB)
          Interrupt:36 Memory:d4000000-d4012700

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:915538 errors:0 dropped:0 overruns:0 frame:0
          TX packets:915538 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:81211031 (77.4 MiB)  TX bytes:81211031 (77.4 MiB)

mng0      Link encap:Ethernet  HWaddr 00:26:b9:5b:ed:6f
          inet addr:10.213.89.117  Bcast:10.213.89.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2980044 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2443046 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1304242346 (1.2 GiB)  TX bytes:185251556 (176.6 MiB)
          Interrupt:32 Memory:d8000000-d8012700

mng0:1    Link encap:Ethernet  HWaddr 00:26:b9:5b:ed:6f
          inet addr:10.213.89.118  Bcast:10.213.89.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:32 Memory:d8000000-d8012700

pm0       Link encap:Ethernet  HWaddr 00:26:b9:5b:ed:6d
          inet addr:10.197.181.50  Bcast:10.197.181.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:48 Memory:d6000000-d6012700
```

The following table lists and describes the information that is output to the `log_ifconfig` file.

Table B-2 Information that is output to the log_ifconfig file

Output item	Output contents

`hb0`
`lo`
`mng`*number*
`pm`*number*
`agr`*number*
`rdn`*number*
`eth`*number*
`xgbe`*number*
	Outputs a port name.
	When `lo` is output for the port name, it indicates a loopback.
	When *number*.*VLAN-ID* is output for the number, it indicates a VLAN interface.
	In addition, when *number*:*alias-number* is output for the number, it indicates a virtual IP address#. One of the following values is output for *alias-number*:
	`0`
	This is output for a virtual IP address that belongs to a resource group on the node where `log_ifconfig` is output.
	`1`
	This is output for a virtual IP address that belongs to a resource group that has failed over from the other node to the node where `log_ifconfig` is output.

`Link encap`	Outputs the type of the link media.

Output item	Output contents
HWaddr	Outputs the MAC address.
inet addr	Outputs the IP address for IPv4.
Bcast	Outputs the broadcast address for IPv4.
Mask	Outputs the subnet mask for IPv4.
inet6 addr	Outputs the IP address for IPv6.
Scope	Outputs the IP address scope for IPv6.
UP	Outputs UP when the interface is running.
BROADCAST	Outputs BROADCAST when the broadcast is used.
RUNNING	Outputs RUNNING when the interface is in a ready state.
MULTICAST	Outputs MULTICAST when multicast is enabled.
MTU	Outputs the MTU size.
Metric	Outputs a metric value.
RX, TX	Outputs a statistical value of the interface.
Interrupt	Outputs the interrupt number used by the interface.
Base address	Outputs the base address for which the driver module is loaded.
Memory	Outputs the memory address for which the driver module is loaded.
#: If resource groups have been failed over or stopped, the information of virtual IP addresses might not be output to the log_ifconfig file, or that the information of both nodes is output. For example, when the nodes Node-01 and Node-02 make up a cluster, the output information varies as follows depending on the condition. When a resource group on Node-01 has been stopped: The information of virtual IP addresses for Node-01 is not output to the log_ifconfig file. When a resource group on Node-02 has been failed over to Node-01: As the information of virtual IP addresses for Node-01, the information of Node-01 and Node-02 is output to the log_ifconfig file.	

The log_interfaces_check file

The following table lists and describes the information that is output to the log_interfaces_check file.

Table B-3 Items that are output to the log_interfaces_check file

Messages	Description	See
Checking DNS configuration...	Outputs the status of the connection with the DNS server.	Table B-4 Information that is output as the status of the connection with the DNS server on page B-6

Messages	Description	See
`Checking NIS configuration...`	Outputs the status of the connection with the NIS server.	Table B-5 Information that is output as the status of the connection with the NIS server on page B-7
`Checking NTP configuration...`	Outputs the status of the connection with the NTP server.	Table B-6 Information that is output as the status of the connection with the NTP server on page B-8
`Checking LDAP configuration (for user authentication)...`	Outputs the status of the connection with the LDAP server used for user authentication.	Table B-7 Information that is output as the status of the connection with the LDAP server used for user authentication on page B-9
`Checking authentication server configuration (for CIFS)...`	Outputs the status of the connection with the authentication server for CIFS clients.	Table B-8 Information that is output as the status of the connection with the authentication server for CIFS clients on page B-10
`Checking authentication server configuration (for NFS)...`	Outputs the status of the connection with the authentication server for NFS clients.	Table B-9 Information that is output as the status of the connection with the authentication server for NFS clients on page B-11
`Checking LDAP configuration (for user mapping)...`	Outputs the status of the connection with the LDAP server used for user mapping.	Table B-10 Information that is output as the status of the connection with the LDAP server used for user mapping on page B-12

Note: If the status of the connections with multiple external servers cannot be acquired, the message `Aborted: More than 1 errors occurred` might be output, and the status of the connections with the external servers might not be output.

Information that is output in the `log_interfaces_check` file is described in the tables below (from Table B-4 Information that is output as the status of the connection with the DNS server on page B-6 to Table B-10 Information that is output as the status of the connection with the LDAP server used for user mapping on page B-12).

Table B-4 Information that is output as the status of the connection with the DNS server

Output contents	Description	Action
`OK`	A DNS server has been correctly specified.	None.

Output contents	Description	Action
`unusing DNS`	A DNS server has not been specified in File Services Manager.	When you use a DNS server, specify the information of the DNS server in the **DNS, NIS, LDAP Setup** page of the **Network & System Configuration** dialog box.
`Warning: DNS server does not respond.` `No respond servers:` *IP-address-of-the-DNS-server-specified-in-File-Services-Manager*	The DNS server specified in File Services Manager does not respond.	Make sure that the following are satisfied: • Devices on the path between a node and the DNS server to be used are working normally. • The IP address of the DNS server that is specified in File Services Manager is correct. • The DNS server is working normally.
`Error: cannot access DNS server.` *cause-of-the-error*	Another error has occurred.	Contact the maintenance personnel.

Table B-5 Information that is output as the status of the connection with the NIS server

Output contents	Description	Action
`OK`	An NIS server has been correctly specified.	None.
`unusing NIS`	An NIS server has not been specified.	When you use an NIS server, specify the information of the NIS server in the **DNS, NIS, LDAP Setup** page of the **Network & System Configuration** dialog box.
`Warning: NIS server does not respond.` `No respond servers:` *name-or-IP-address-of-the-NIS-server-specified-in-File-Services-Manager*[#]	The NIS server specified in File Services Manager does not respond.	Make sure that the following are satisfied: • Devices on the path between a node and the NIS server to be used are working normally. • The name or IP address of the NIS server that is specified in File Services Manager is correct. • The NIS server is working normally.

Output contents	Description	Action
`Warning: The specified NIS server name cannot be resolved.` `NIS server name:` *name-of-the-NIS-server-specified-in-File-Services-Manager*	Resolving the name of the NIS server specified in File Services Manager failed.	Make sure that the name of the NIS server can be correctly resolved.
`Warning: The specified NIS domain is invalid.` `NIS domain name:` *NIS-domain-name-of-the-NIS-server-specified-in-File-Services-Manager*	The NIS domain name specified in File Services Manager is incorrect.	Make sure that the NIS domain name is correctly specified in the **DNS, NIS, LDAP Setup** page of the **Network & System Configuration** dialog box.
`Error: cannot access NIS server.` *cause-of-the-error*	Another error has occurred.	Contact the maintenance personnel.
#: When broadcast is used, `Broadcast` is output.		

Table B-6 Information that is output as the status of the connection with the NTP server

Output contents	Description	Action
`OK`	An NTP server has been correctly specified.	None.
`unusing NTP`	An NTP server has not been specified.	If necessary, specify the NTP server in the **Time Setup** page of the **Network & System Configuration** dialog box.
`Warning: NTP server does not respond.` `No respond servers:` *name-or-IP-address-of-the-NTP-server-specified-in-File-Services-Manager*	The NTP server specified in File Services Manager does not respond.	Make sure that the following are satisfied: • Devices on the path between a node and the NTP server to be used are working normally. • The name or IP address of the NTP server specified in File Services Manager is correct. • The NTP server is working normally.
`Warning: The specified NTP server name cannot be resolved.` `NTP server name:` *name-of-the-NTP-server-specified-in-File-Services-Manager*	Resolving the name of the NTP server specified in File Services Manager failed.	Make sure that the name of the NTP server can be correctly resolved.
`Error: cannot access NTP server.` *cause-of-the-error*	Another error has occurred.	Contact the maintenance personnel.

Table B-7 Information that is output as the status of the connection with the LDAP server used for user authentication

Output contents	Description	Action
`OK`	An LDAP server for user authentication has been correctly specified.	None.
`unusing LDAP`	An LDAP server for user authentication has not been specified.	When you perform user authentication on an LDAP server, specify the information of the LDAP server in the **DNS, NIS, LDAP Setup** page of the **Network & System Configuration** dialog box.
`Error: LDAP server(`*IP-address-of-the-LDAP-server-specified-in-File-Services-Manager*`:`*port-number*`) has not been connected.`	The LDAP server specified in File Services Manager does not respond.	Make sure that the following are satisfied: • Devices on the path between a node and the LDAP server to be used are working normally. • The name or IP address of the LDAP server specified in File Services Manager is correct. • The LDAP server is working normally.
`Warning: LDAP server(`*IP-address-of-the-LDAP-server-specified-in-File-Services-Manager*`:`*port-number*`) has been connected, but the time limitation occurred.`	A timeout occurred while checking the connection between a node and the LDAP server specified in File Services Manager.	Make sure that the information of the LDAP server is correctly specified in the **DNS, NIS, LDAP Setup** page of the **Network & System Configuration** dialog box.
`Warning: LDAP server(`*IP-address-of-the-LDAP-server-specified-in-File-Services-Manager*`:`*port-number*`) has been connected, but the size limitation occurred.`	The number of entries that can be acquired from the LDAP server (which is specified in File Services Manager) has reached the limit. The number of entries that can be acquired from the LDAP server might be limited.	Make sure that the information of the LDAP server is correctly specified in the **DNS, NIS, LDAP Setup** page of the **Network & System Configuration** dialog box. Also, check the setting for the number of entries that can be acquired from the LDAP server.
`Warning: The password of LDAP administrator seems to be invalid.`	The password of the LDAP server administrator set in File Services Manager is incorrect.	Check whether the password of the LDAP server administrator has been set correctly.
`Error: /etc/libnss-ldap.conf is not found.`	The configuration file for the LDAP server does not exist. There might be a problem in the OS.	Contact the maintenance personnel.

Table B-8 Information that is output as the status of the connection with the authentication server for CIFS clients

Output contents	Description	Action
`OK`	An authentication server for CIFS clients has been correctly specified.	None.
`unusing authentication server`	File Services Manager authenticates CIFS clients. The NT server authentication, NT domain authentication, and Active Directory authentication are not used.	When you use the NT server authentication, NT domain authentication, or Active Directory authentication, specify the information of the server to be used in the **CIFS Service Management** page (**Setting Type**: `Basic`) of the **Access Protocol Configuration** dialog box.
`Error: rpc error. Server:` *name-of-the-authentication-server-specified-in-File-Services-Manager*	The authentication server for CIFS clients that is specified in File Services Manager does not respond.	Make sure that the following are satisfied: • Devices on the path between a node and the authentication server for CIFS clients to be used are working normally • The name or IP address of the authentication server for CIFS clients that is specified in File Services Manager is correct. • The authentication server for CIFS clients is working normally.
`Error: timeout. Server:` *name-of-the-authentication-server-specified-in- File-Services-Manager*	A timeout occurred while checking the connection with the authentication server for CIFS clients that is specified in File Services Manager.	Make sure that the following are satisfied: • Devices on the path between the node and the authentication server for CIFS clients to be used are working normally. • The name or IP address of the authentication server for CIFS clients that is specified in File Services Manager is correct. • The authentication server for CIFS clients is working normally.
`Error: name resolution failure. Server:` *name-of-the-authentication-server-*	Resolving the name of the authentication server for CIFS clients failed.	Make sure that the name of the CIFS server can be correctly resolved.

Output contents	Description	Action
specified-in- File-Services-Manager		
`Error:` *cause-of-the-error*. `Server:` *name-of-the-authentication-server-specified-in- File-Services-Manager*	Another error has occurred.	Contact the maintenance personnel.
`Warning: The SRV DNS records might not be created for a domain controller.`	The SRV records for deploying the Active Directory service might not be registered on the DNS server.	Check whether the SRV records for deploying the Active Directory service is registered on the DNS server. Register the records if they are not registered.

Table B-9 Information that is output as the status of the connection with the authentication server for NFS clients

Output contents	Description	Action
`OK`	A KDC server has been correctly specified.	None.
`unusing KDC server`	A KDC server has not been specified.	If you use Kerberos authentication, specify the information of the KDC server to be used in the **NFS Service Management** page of the **Access Protocol Configuration** dialog box.
Error: KDC error. Server: *name-of-the-KDC-server-specified-in-File-Services-Manager*	The KDC server specified in File Services Manager does not respond.	Make sure that the following are satisfied: • Devices on the path between a node and the KDC server to be used are working normally. • The name or IP address of the KDC server that is specified in File Services Manager is correct. • The KDC server is working normally.
`Error: timeout. Server:` *name-of-the-KDC-server-specified-in-File-Services-Manager*	A timeout occurred while checking the connection with the KDC server that is specified in File Services Manager.	Make sure that the following are satisfied: • Devices on the path between the node and the KDC server to be used are working normally. • The name or IP address of the KDC server that is specified in File Services Manager is correct.

Output contents	Description	Action
		• The KDC server is working normally.
`Error: name resolution failure. Server:` *name-of-the-KDC-server-specified-in-File-Services-Manager*	The name of the KDC server could not be resolved.	Make sure that the name of the KDC server can be correctly resolved.
`Error:` *cause-of-the-error*. `Server:` *name-of-the-KDC-server-specified-in-File-Services-Manager*	Another error has occurred.	Contact the maintenance personnel.

Table B-10 Information that is output as the status of the connection with the LDAP server used for user mapping

Output contents	Description	Action
`OK`	An LDAP server for user mapping has been correctly specified.	None.
`unusing LDAP`	An LDAP server for user mapping has not been specified.	When you use an LDAP server for user mapping, specify the information of the LDAP server in the **CIFS Service Management** page (**Setting Type**: `User mapping`) of the **Access Protocol Configuration** dialog box.
`Error: LDAP search timeout.`	The LDAP server specified in File Services Manager does not respond.	Make sure that the following are satisfied: • Devices on the path between a node and the LDAP server to be used are working normally. • The name or IP address of the LDAP server specified in File Services Manager is correct. • The LDAP server is working normally.
`Error: LDAP server is down, LDAP server name is invalid, or LDAP server port number is invalid.`	The name or port number of the LDAP server that is specified in File Services Manager is incorrect, or the LDAP server has been stopped.	Make sure that the following are satisfied: • Devices on the path between the node and the LDAP server to be used are working normally. • The name or IP address of the LDAP server that is specified in File Services Manager is correct. • The LDAP server is working normally.

Output contents	Description	Action
`Error: LDAP suffix is not specified.`	The LDAP server root DN has not been specified in File Services Manager.	Specify the LDAP server root DN in the **CIFS Service Management** page (**Setting Type**: `User mapping`) of the **Access Protocol Configuration** dialog box.
`Error: LDAP administrator DN is not specified.`	The LDAP server administrator DN has not been specified in File Services Manager.	Specify the LDAP server administrator DN in the **CIFS Service Management** page (**Setting Type**: `User mapping`) of the **Access Protocol Configuration** dialog box.
`Error: LDAP administrator password is not specified.`	The LDAP server administrator password has not been specified in File Services Manager.	Specify the LDAP server administrator password in the **CIFS Service Management** page (**Setting Type**: `User mapping`) of the **Access Protocol Configuration** dialog box.
`Error: LDAP user map DN or LDAP server root DN is invalid.`	Either of the following specified in File Services Manager is incorrect: • The user mapping account DN • LDAP server root DN	Make sure that each DN is correctly specified in the **CIFS Service Management** page (**Setting Type**: `User mapping`) of the **Access Protocol Configuration** dialog box.
`Error: LDAP administrator password is invalid.`	The LDAP server administrator password specified in File Services Manager is incorrect.	Check the password specified in the LDAP server, and then change the password in the **CIFS Service Management** page (**Setting Type**: `User mapping`) of the **Access Protocol Configuration** dialog box.
`Error: LDAP server root DN or LDAP administrator DN or LDAP administrator password is invalid.`	The LDAP server root DN, administrator DN, or administrator password specified in File Services Manager is incorrect.	Make sure that the LDAP server root DN, administrator DN, and administrator password are correctly specified in the **CIFS Service Management** page (**Setting Type**: `User mapping`) of the **Access Protocol Configuration** dialog box.
`Error: objectClass=sambaUnixIdPool does not exist.`	The initial setup for the LDAP server failed. Entries used for user mapping cannot be updated.	Restart the CIFS service after confirming that: • The schema file created for the LDAP server has been loaded correctly. • Write permissions have been set on the entries to be used for user mapping. • The user specified for the LDAP server administrator DN in the **CIFS Service Management** page (**Setting Type**: `User mapping`) of the

Output contents	Description	Action
		Access Protocol Configuration dialog box has administrator privileges.
`Error: objectClass=sambaUnixIdPool is multiple.`	The initial settings for the LDAP server are incorrect.	Multiple entries that were used for the LDAP user mapping account exist on the specified LDAP server. Among those entries, delete the entries other than ones used for the LDAP user mapping account entry specified in the **CIFS Service Management** page (**Setting Type**: `User mapping`) of the **Access Protocol Configuration** dialog box.
`Error: open CIFS.conf failed.`	The `/etc/cifs/CIFS.conf` file could not be opened because of a problem in the OS.	Contact the maintenance personnel.
`Error: open cifs.conf failed.`	The `/enas/conf/cifs.conf` file could not be opened because of a problem in the OS.	Contact the maintenance personnel.
`Error: cannot access LDAP server.` *cause-of-the-error*	Another error has occurred.	Contact the maintenance personnel.

C

How To Check Network Communication

A system administrator needs to make sure that network communication can be established between the HDI system and clients. This section describes how to take actions for the problem that network communication between the HDI system and clients cannot be established due to the network setting error in File Services Manager.

Before checking network communication

To make sure that no hardware or link failure occurred in the network and that no failover occurred in the HDI system, and identify any problems in the File Services Manager network settings

1. From the client, execute the `ping` command for a machine that belongs to the same network as the HDI system, or for the router that routs communications.

   Make sure that the client can communicate with machines that do not belong to the HDI system, and that it cannot communicate only with the HDI system. If the client cannot communicate with machines that do not belong to the HDI system, make sure that relay devices are running normally. For example, make sure that relay devices such as switches and routers are powered on, and all cables are plugged in.
2. In the **List of RAS Information** page (for `List of messages`) in the **Check for Errors** dialog box, make sure that a warning-level link-down message is not output.

   If a warning-level link-down message is output, contact maintenance personnel.
3. In the **List of RAS Information** page (for `List of messages`) page, make sure that the message KAQG70000-E is not output (make sure that a failover is not occurring).

   If a failover is occurring, contact maintenance personnel.

Performing checks for each network configuration

Before checking network communication, check whether the HDI system and the client belong to the same network.

The following shows an example when the HDI system and the client belong to the same network.

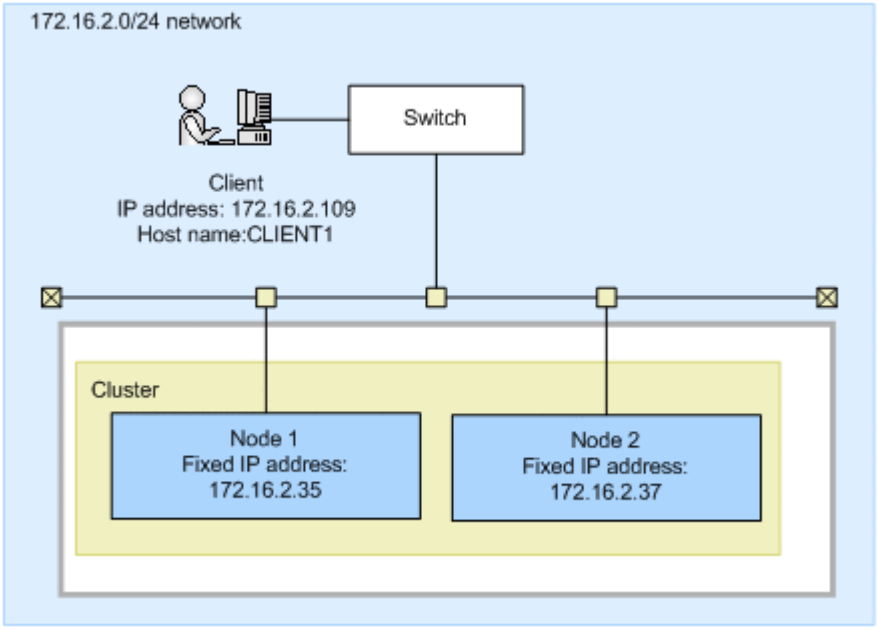

Figure C-1 Configuration example when the HDI system and the client belong to the same network

The following shows an example when the HDI system and the client belong to different networks.

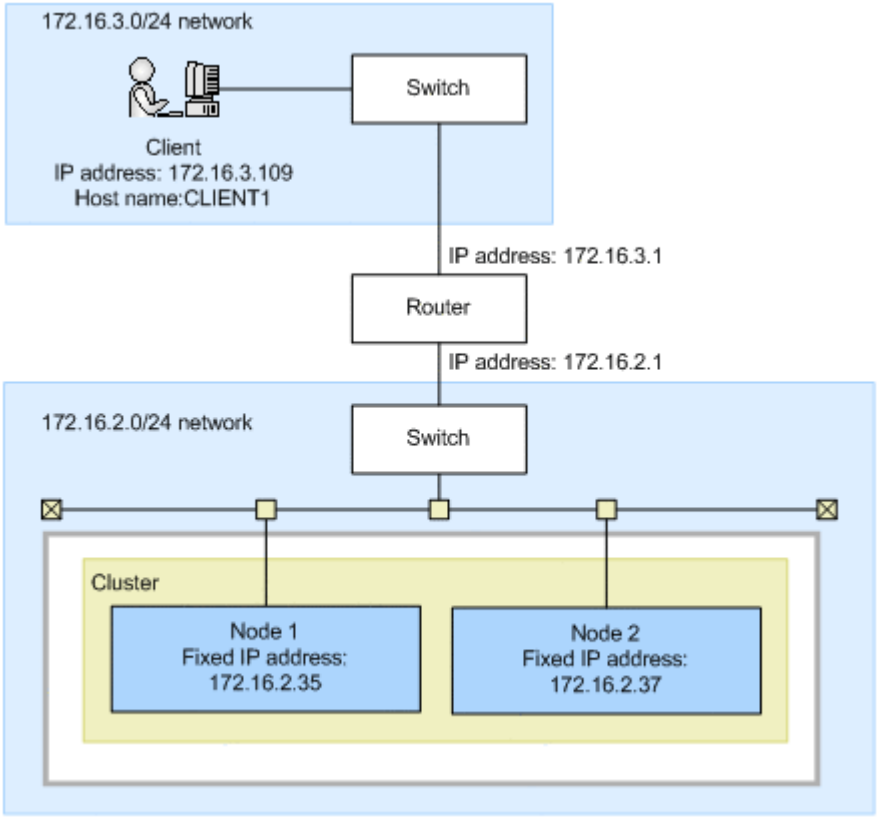

Figure C-2 Configuration example when the HDI system and the client belong to different networks

Checking communication within the network

When the HDI system and the client belong to the same network, perform the following steps to check the communication within the network. When the HDI system and the client belong to different networks, perform the same steps, assuming the router is the client.

To check communication within the network:

1. From one node, specify the fixed IP address of the other node, and execute the `nasping` command.

   If communication cannot be established, the setting of the IP address or netmask for the HDI system is invalid, or the setting of the VLAN for the HDI system or switch is invalid. For actions to be taken, see Checking the IP address and netmask on page C-5 and Checking the VLAN ID on page C-5.
2. From one node, specify the `-s` option in the `nasping` command, and execute it for the other node.

   If communication cannot be established, the setting of the MTU value for the HDI system or switch is invalid. For actions to be taken, see Checking the MTU value on page C-5.
3. Execute the `nasping` command for the client.

   If communication cannot be established, the setting of the IP address or netmask for the client is invalid, or the setting of the VLAN for the switch or client is invalid. For actions to be taken, see Checking the IP address and netmask on page C-5 and Checking the VLAN ID on page C-5.
4. Specify the `-s` option in the `nasping` command, and execute it for the client.

   If communication cannot be established, the setting of the MTU value for the switch or client is invalid. For actions to be taken, see Checking the MTU value on page C-5.

Checking communication between different networks

To check communication between different networks when the HDI system and the client belong to different networks

1. Specify the network gateway address on the client side, and execute the `nasping` command.

   When `Network is unreachable` is output, the routing setting for the HDI system is invalid. When the communication cannot be established, the routing setting for the router is invalid. For actions to be taken, see Checking the routing on page C-6.
2. Specify the `-n` option and the client's IP address in the `nastraceroute` command, and execute it.

   If communication cannot be established, an error occurs in the network from the router to the client. Check if there are any problems from the router to the client.

Actions to be taken when communication cannot be established

If you check the network communication and find that communication is not available, you must check the settings. If the settings are invalid, change them to the correct settings, and check the operation again.

Checking the IP address and netmask

Check the network addresses for the HDI system and client.

HDI system

In the **List of Interfaces** page of the **Network & System Configuration** dialog box, check the fixed IP address, virtual IP address, and netmask.

Client

Check the IP address and netmask.

If the network addresses for the HDI system and the client are different, change the settings to be the same network address.

Checking the VLAN ID

When the VLAN is set, check the VLAN settings for the HDI system, switch, and client.

HDI system

Check the VLAN ID in the **List of Interfaces** page of the **Network & System Configuration** dialog box.

Switch

Check the VLAN setting for the port connected to the HDI system and client. When multiple switches are routed, check the VLAN setting for the port connected between switches. Also, check whether the port is set to be tagged or untagged.

Client

When the tagged VLAN is set, check the VLAN ID for the tagged VLAN.

If the VLAN ID settings are different among the HDI system, switch, and client, change the setting so that they have the same VLAN ID. If the tagged or untagged setting for the switch is incorrect, specify the correct setting.

Checking the MTU value

When you change the MTU setting, for example, to use a Jumbo Frame, check the settings of the MTU values for the HDI system, switch, and client.

HDI system

Check the MTU value in the **List of Interfaces** page of the **Network & System Configuration** dialog box.

Switch

Check the MTU value of the port connected to the HDI system and client. When multiple switches are routed, check the MTU value for the port connected between switches.

Client

Check the MTU value.

When the MTU value for the switch is smaller than the MTU values set for the HDI system and client, increase the value for the switch so that it is larger than the values for the HDI system and client.

Checking the routing

Check whether gateways appropriate for the HDI system, router, switch, and client are set.

HDI system

In the **List of Routings** page of the **Network & System Configuration** dialog box, check whether the gateways (such as router and switch) that can reach the client are specified.

Router and switch

Check whether the gateways that can reach the client and HDI system are specified.

Client

Check whether the gateways that can reach the HDI system are specified.

If gateways appropriate for the HDI system, router, switch, and client are not set, change the appropriate gateway setting.

Note that if a host name is specified when routing information is added, and one of the following operations is performed while the host name cannot be resolved, the routing information specified by the administrator might be inconsistent with that enabled on a node:

- Restarting the OS
- Releasing trunking
- Interface modification or deletion
- Deleting routing information

In this case, perform the following to resolve this problem.

The following explanation assumes that the following routing information is set for the example in Figure C-2 Configuration example when the HDI system and the client belong to different networks on page C-3.

```
$ sudo routelist
Target          Netmask         Gateway         Method Type    MSS   Iface
CLIENT1         -               172.16.2.1      Allow  host    -     eth2
```

Checking the enabled routing:

The **List of Routings** page and `routelist` command can be used to display the routing information set by the system administrator.

The `routelist` command needs to be executed with the `-l` option specified to check whether the set routing information is enabled.

```
$ sudo routelist -l
Target          Netmask         Gateway         Flags   MSS   Iface
172.16.3.109    255.255.255.255 172.16.2.1      UGH     -     eth2
172.16.2.0      255.255.255.0   0.0.0.0         U       -     eth2
10.0.0.0        255.255.255.0   0.0.0.0         U       -     hb0
192.168.0.0     255.255.255.0   0.0.0.0         U       -     pm0
10.213.88.0     255.255.252.0   0.0.0.0         U       -     mng0
```

Note: Output is performed in the IP address format. The routing set by the OS is also displayed.

Countermeasures for when the set routing information is not enabled:

When a host name is used to add routing information, and then the OS is restarted while the host name cannot be resolved, the routing information specified by the system administrator might not be enabled on a node.

To check if the set routing information is not enabled

a. Compare the routing information set by the system administrator with that enabled on a node.

```
$ sudo routelist
Target          Netmask         Gateway         Method Type    MSS
Iface
CLIENT1         -               172.16.2.1      Allow  host    -
eth2
```

```
$ sudo routelist -l
Target          Netmask         Gateway         Flags   MSS   Iface
172.16.2.0      255.255.255.0   0.0.0.0         U       -     eth2
10.0.0.0        255.255.255.0   0.0.0.0         U       -     hb0
192.168.0.0     255.255.255.0   0.0.0.0         U       -     pm0
10.213.88.0     255.255.252.0   0.0.0.0         U       -     mng0
```

In this example, the results of the `routelist` command do not exist in the results of the `routelist` command executed with the `-l` option specified.

b. Allow the host name (`CLIENT1`) to be resolved, and then delete the routing information.

```
$ sudo routedel -d CLIENT1 -g 172.16.2.1 eth2
KAQM05099-Q Do you want to delete the specified routing information?
(y/n) y
```

c. Add the routing information again.

```
$ sudo routeadd -t host -d CLIENT1 -g 172.16.2.1 eth2
```

Countermeasures for when deleted routing information is enabled:

When a host name is used to add routing information and then the IP address for the host name is changed, if the routing information is deleted, it is deleted from the settings file, but might remain enabled on a node.

To check if the deleted routing information is enabled

a. Compare the routing information set by the system administrator with that enabled on a node.

```
$ sudo routelist
Target          Netmask         Gateway         Method Type    MSS
Iface
```

```
$ sudo routelist -l
Target          Netmask         Gateway         Flags   MSS   Iface
172.16.3.109    255.255.255.255 172.16.2.1      UGH     -     eth2
172.16.2.0      255.255.255.0   0.0.0.0         U       -     eth2
10.0.0.0        255.255.255.0   0.0.0.0         U       -     hb0
192.168.0.0     255.255.255.0   0.0.0.0         U       -     pm0
10.213.88.0     255.255.252.0   0.0.0.0         U       -     mng0
```

In this example, the routing information added by the system administrator is not included in the results of the `routelist` command. When the `routelist` command is executed with the `-l` option specified the routing information is included in the results.

b. To delete the routing information that remains enabled on a node, execute the `routedel` command with the `--nochk` option specified.

Note: Do not delete the routing information automatically set by the OS.

```
$ sudo routedel -d 172.16.3.109 -g 172.16.2.1 --nochk eth2
KAQM05099-Q Do you want to delete the specified routing information?
(y/n) y
```

Make sure that the interface used to send packets and the gateway for the network segment of the communication-target host are correct.

Check the routing table to check from which network interface the packets of the communication-target host are sent and received. Check the routes displayed by the `routelist -l` command from the top to see whether there is a route that matches the IP address and netmask of the communication-target host. Confirm that the network interface set for the route can be communicated with the target host. If a gateway is set in the route, use the `nasping` command to confirm that you can communicate with the gateway.

If there are multiple routes that match the communication-target host, the first one from the top of the list is set for sending and receiving packets. If the HDI system receives packets from the route that is not set for receiving and sending packets, the HDI system discards the packets.

If multiple routes of the same segment are displayed by the `routelist -l` command, the settings for the routes might be wrong. Check the settings again.

Checking the negotiation mode

Make sure that the settings of the negotiation mode for the node data ports and the switch are the same. If the auto negotiation mode is set, you also need to check the communication status.

Node data ports

In the **List of Data Ports** page of the **Network & System Configuration** dialog box, make sure that the setting of the negotiation mode is the same as that for the switch. If the auto negotiation mode is set for the communication status with the switch, make sure that appropriate statuses are displayed for **Speed** and **Duplex** of **Connected status**.

Switch

Make sure that the setting of the negotiation mode for the port connected to the node data ports is the same as those for the nodes.

Depending on the switch type, the communication rate might become lower than expected or communication might become impossible even if the auto negotiation mode is set for both the nodes and switch. In this case, configure the fixed negotiation modes so that the settings of the nodes and switch are the same.

Examples of checking network communication

This section describes examples of checking the network communication.

Example of checking a network by using the nasping command

The following describes an example of checking a network by using the `nasping` command.

Successful example:

The following gives an example of command execution and an explanation when the communication is successful.

```
$ sudo nasping -c 3 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 56(84) bytes of data.
64 bytes from 192.168.0.20: icmp_seq=1 ttl=64 time=0.069 ms
64 bytes from 192.168.0.20: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 192.168.0.20: icmp_seq=3 ttl=64 time=0.058 ms

--- 192.168.0.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.058/0.061/0.069/0.010 ms
$ sudo nasping -c 3 -s 9000 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 9000(9028) bytes of data.
9008 bytes from 192.168.0.20: icmp_seq=1 ttl=64 time=5.74 ms
9008 bytes from 192.168.0.20: icmp_seq=2 ttl=64 time=0.981 ms
9008 bytes from 192.168.0.20: icmp_seq=3 ttl=64 time=1.18 ms

--- 192.168.0.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.981/2.636/5.742/2.198 ms
$
```

The first nasping command sent a 56-byte ICMP packet to the machine with the IP address of 192.168.0.20 for three times, and the machine received it three times. From the result, you can see that communication was performed correctly. The next nasping command sent a 9,000-byte ICMP packet to the same client, and the packet loss was 0%. The communication at this time was also performed correctly.

Failed example 1:

The following gives an execution example and explanation when the HDI system cannot communicate with a machine in the same network.

```
$ sudo nasping -c 3 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
From 192.168.0.10 icmp_seq=1 Destination Host Unreachable
From 192.168.0.10 icmp_seq=2 Destination Host Unreachable
From 192.168.0.10 icmp_seq=3 Destination Host Unreachable

--- 192.168.0.11 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time
2007ms, pipe 3
$
```

The nasping command sent a 56-byte ICMP packet to the machine with the IP address of 192.168.0.11 for three times, but the machine could not receive it even once. From the result, you can see the HDI system was not able to communicate with the machine that has the specified IP address. Check the settings for the IP address, netmask, and VLAN ID for the HDI system, switch, and client. If necessary, change the settings.

Failed example 2:

The following gives an execution example and explanation when the MTU value for the switch is not specified correctly.

The MTU value for the interface in the HDI system is 9,000. The following example shows the case when 9,000 is not specified for the MTU value for the switch.

```
$ sudo nasping -c 3 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 56(84) bytes of data.
64 bytes from 192.168.0.20: icmp_seq=1 ttl=64 time=0.074 ms
64 bytes from 192.168.0.20: icmp_seq=2 ttl=64 time=0.060 ms
64 bytes from 192.168.0.20: icmp_seq=3 ttl=64 time=0.070 ms

--- 192.168.0.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.060/0.068/0.074/0.005 ms
$ sudo nasping -c 3 -s 9000 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 9000(9028) bytes of data.

--- 192.168.0.20 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2015ms
$
```

The first nasping command sent a 56-byte ICMP packet to the machine with the IP address of 192.168.0.20 for three times, and the machine received it for three times. From the result, you can see that communication was performed correctly. The next nasping command sent a 9,000-byte ICMP packet to the same client, but the communication

failed with a packet loss of 100%. Check the settings for the MTU value for the HDI system, switch, and client. If necessary, change the settings.

Failed example 3:

The following gives an execution example and explanation when the HDI system cannot communicate with a machine in a different network. In the example, the gateway address of the different network is specified and the `nasping` command is executed.

```
$ sudo nasping -c 3 192.168.2.2
connect: Network is unreachable
$ sudo nasnetstat -rn
Kernel IP routing table
Destination     Gateway         Genmask          Flags   MSS Window  irtt
Iface
10.0.1.0        0.0.0.0         255.255.255.224 U         0 0          0
hb0
10.208.148.0    0.0.0.0         255.255.255.0   U         0 0          0
eth15-br
10.0.1.0        0.0.0.0         255.255.255.0   U         0 0          0
hb0-br
192.167.0.0     0.0.0.0         255.255.255.0   U         0 0          0
agr0-br
10.197.181.0    0.0.0.0         255.255.255.0   U         0 0          0
pm0
10.213.88.0     0.0.0.0         255.255.252.0   U         0 0          0
mng0-br
$
```

In this example, neither the target gateway for `192.168.2.2` nor the default route is specified. `Network is unreachable` is displayed because a route to the specified IP address has not been established. Check the routing setting for the HDI system, and if necessary, specify the setting again.

Example of checking communication by using the nastraceroute command

The following describes an example of checking a network by using the `nastraceroute` command.

Successful example:

The following gives an execution example and explanation when the communication route to a machine in a different network is set correctly.

```
$ sudo nastraceroute -n 10.213.76.124
traceroute to 10.213.76.124 (10.213.76.124), 30 hops max, 40 byte packets
 1  10.213.88.10  5.580 ms  5.588 ms  5.583 ms
 2  158.214.125.10  7.478 ms  9.683 ms  11.154 ms
 3  10.213.1.3  9.653 ms  9.667 ms  9.982 ms
 4  10.213.76.124  9.547 ms  9.560 ms  9.557 ms
$
```

In this example, the HDI system communicates with the machine with the IP address of `10.213.76.124` via the routers with the IP addresses of `10.213.88.10`, `158.214.125.10`, and `10.213.1.3`.

Failed example:

The following gives an execution example and explanation when an error occurs in the route between the router and the client.

```
$ sudo nastraceroute -n 10.10.10.10
traceroute to 10.10.10.10 (10.10.10.10), 30 hops max, 40 byte packets
 1  10.213.88.10  5.496 ms  5.490 ms  5.486 ms
 2  158.214.125.10  9.376 ms  9.403 ms  11.644 ms
 3  10.213.1.65  7.238 ms  7.258 ms  7.253 ms
 4  158.214.120.2  7.249 ms  9.324 ms  9.320 ms
 5  133.145.201.2  13.583 ms  15.147 ms  17.309 ms
 6  133.144.227.33  13.551 ms  11.658 ms  10.097 ms
 7  * * *
 8  * * *
...
29  * * *
30  * * *
$
```

From the execution result of the `nastraceroute` command, you can see that the communication to the gateway with the IP address of `133.144.227.33` was established, however, the communication beyond the gateway could not be established. Make sure that the settings for the router and other relay devices are correct, and the routing setting for the client is correct. If necessary, change the settings.

D

Troubleshooting Examples

This appendix provides troubleshooting examples.

- GUI-related troubleshooting examples
- HCP linkage troubleshooting examples
- Virus scan troubleshooting examples
- CIFS access troubleshooting examples

GUI-related troubleshooting examples

The following troubleshooting examples relate to problems that might occur during GUI operation.

Table D-1 GUI-related troubleshooting examples

Location of problem	Type of problem	Cause and action
Installation of Hitachi File Services Manager	The KAQM30001-E message is displayed during installation.	A user who does not have administrator permissions began the installation. Log in again to the management server as a user that has administrator permissions, and then retry the installation.
	The KAQM30002-E or KAQM30007-E message is displayed during installation.	Either the OS or the version of the OS on the management server on which Hitachi File Services Manager is to be installed is not supported. Prepare a management server that is running a supported version of a supported OS, and then retry the installation.
	The KAQM30053-E or KAQM30059-E message is displayed during installation.	The management server on which Hitachi File Services Manager is to be installed has insufficient free space. Increase the amount of free disk space on the management server, and then retry the installation.
	The KAQM30009-E message is displayed during installation.	The management server on which Hitachi File Services Manager is to be installed might not satisfy the requirements for installation. Make sure that the management server satisfies the requirements for installation, and then retry the installation.
Non-specific	Unable to display Hitachi File Services Manager in a Web browser.	Hitachi Command Suite Common Component is not started. Perform the following to start Hitachi Command Suite Common Component. For Windows 7 or earlier: Select **Start**, **Programs**, **Hitachi Command Suite**, **File Services Manager**, and then **Start - HFSM**. For Windows 8 or Windows Server 2012: From the list of applications in the Start window, select **Start - HFSM**.
		Hitachi Command Suite Common Component failed to start due to insufficient disk capacity on the management server. Increase the amount of free disk space on the management server, and then perform

Location of problem	Type of problem	Cause and action
		the following to start Hitachi Command Suite Common Component. For Windows 7 or earlier: Select **Start**, **Programs**, **Hitachi Command Suite**, **File Services Manager**, and then **Start - HFSM**. For Windows 8 or Windows Server 2012: From the list of applications in the Start window, select **Start - HFSM**.
	Two dialog boxes are opened by a single action (one screen is blank and the buttons do not work on the other screen).	This problem is related to the window controls of the Web browser, and is not due to a failure in the systems managed by Hitachi File Services Manager. Close the dialog boxes by clicking the close button in the top-right corner of each one, and then retry the operation that caused the dialog boxes to be opened.
	One of the following problems occurred on the displayed screen: • Part of the screen is not properly displayed. • Some buttons are not properly displayed. (When the cursor is moved over or away from a button.) • A JavaScript error occurred.	Different versions of the Hitachi File Services Manager screen information are cached in the Web browser's cache or in the proxy server's cache. This problem is likely to occur right after an upgrade installation of Hitachi File Services Manager. Clear the Web browser's cache, then retry the operation. If a proxy server is specified for the Web browser, refer to information about the environment settings for the management control in *Installation and Configuration Guide*, and then review the proxy settings.
	You attempted to display a subwindow by clicking a button, but "Page not found" is displayed in the window.	Check the following: • If there is a network connection problem between the client machine and the node. • Whether the node does not start. See If the File Services Manager GUI does not work correctly on page 1-7 for the troubleshooting procedures.
		Check the following: • If the OS of the management console does not meet the requirements for a management console. • If the OS of the management console might failed to verify an SSL certificate. Check the requirements for management consoles by seeing the explanation of environment settings for a management

Location of problem	Type of problem	Cause and action
		console in the *Installation and Configuration Guide*.
	A dialog box in which an operation is being executed does not change to a results dialog box for over half an hour.	This problem is related to the window controls of the Web browser, and is not due to a failure in the systems managed by Hitachi File Services Manager. Close the dialog box in which an operation is being executed by clicking the close button in the top-right corner. After that, execute refresh processing, and then check the latest information. If this problem occurs again when using Internet Explorer version 9.0 or later, select **Internet Options**, **Advanced**, and then apply **Use software rendering instead of GPU rendering**. If this does not fix the problem, or if the version of Internet Explorer you are using is older than version 9.0, select **Internet Options**, **Advanced**, and then reset the settings. After doing so, check the *Installation and Configuration Guide* and apply the settings for when Internet Explorer is used on the management console.
	The KAPM08201-E message is displayed during the operation of Hitachi File Services Manager.	An operation might have been attempted before the screen was completely displayed. Wait until the screen is completely displayed, and then retry the operation. If the problem cannot be corrected, acquire the maintenance server log data, and then contact maintenance personnel.
	The KAQM19114-E or KAQM19115-E message is displayed in the dialog box in which an operation is being performed.	This problem is related to the window controls of the Web browser, and is not due to a failure in the systems managed by Hitachi File Services Manager. Take action according to the displayed message.
	Logging in to Hitachi File Services Manager from Firefox and then clicking the **Close** button does not close the window.	This problem is related to the window controls in Firefox, and is not due to a failure in the systems managed by Hitachi File Services Manager. From the `about:config` page in Firefox, specify `true` for `dom.allow_scripts_to_close_windows`.
	When an operation terminated due to an error, a window was displayed. However, the user quickly closed the window, and could not check the information	Search the Hitachi File Services Manager log files for the message that was logged when the error occurred. Then, check the message ID and message text for the error details. For details about Hitachi File Services Manager log files, see Checking

Location of problem	Type of problem	Cause and action
	about the error that occurred.	the operating status of the management server on page 2-14.
	`500 Internal Server Error` appears on the screen.	The service either might have stopped or might currently be starting. Check the operating status of the service. If the service has stopped, restart it. If the service is currently starting, wait a while, and then log in to Hitachi File Services Manager again.
Login window	Failure to log in	Make sure the specified value is correct. If the value is correct, consult a system administrator who has administrator privileges to check whether your account is locked. If you are still unable to fix the problem, Hitachi File Services Manager might not be working properly because the management server time was changed while Hitachi Command Suite Common Component or Hitachi Command Suite products were starting. Restart the management server, and then log in to the system again.
Information displayed for the processing node status, physical node status, or hardware status	The status of the processing node is not `Online`.	The status of one of the physical nodes in the processing node is not `Online`. Take action according to the status of the physical node.
	`Unknown error` appears as the status of the physical node.	There is a problem with the network between the File Services management server and the node. Check the network by, for example, executing the `ping` command.
		The node has not started. Start the node.
		The Primary Server Base is inactive on the node side. Collect all log data, and contact maintenance personnel.
		While a processing node was being added, edited, or refreshed, an error was returned because of a cluster status transition (for example, the node being failed over). For details, check the status of the nodes and resource groups from the **Cluster Management** dialog box. Also, check whether error messages have been output to the **Check for Errors** dialog box.

Location of problem	Type of problem	Cause and action
		If a dialog box cannot be displayed, take action according to If the File Services Manager GUI does not work correctly on page 1-7, and then update the processing node. If this does not resolve the issue, collect all log data and contact maintenance personnel.
	`Credential error` appears as the status of the physical node.	The node password and Hitachi File Services Manager password do not match. Change the password on the node, and then refresh the processing node information (the same password must be set for both nodes in the cluster). Alternatively, in the **Edit Processing Node** dialog box, change the password on the Hitachi File Services Manager side.
	`Maintenance required` appears as the status of a physical node.	A user operation (for example, stopping the cluster, stopping a node, stopping a resource group, or disabling resource group monitoring) caused one of the following to occur: • A failover • Client services to be stopped • The cluster to not be configured Check the status of the node in the **Cluster Management** dialog box, and restart the services as necessary. If the cluster is not configured, configure it. After recovery, refresh the processing node information.
	`Transitional state` appears as the status of a physical node.	The status of the resource group is starting or stopping. If the node status does not change for a while, then an error might have occurred. Wait a while, and then refresh the processing node information to recover the status. If this does not cause the status to recover, retry refresh processing, and then wait until the status recovers. If the status has not recovered after a while, check the node status in the **Cluster Management** dialog box.
	`Ready for failback` appears as the status of a physical node.	The resource group scheduled to run on the physical node has been failed over. When this happens, the node services run on the other node. Check the node status in the **Cluster Management** dialog box.

Location of problem	Type of problem	Cause and action
		After removing the cause of the error, manually fail back the node.
	`Shutdown` appears as the status of a physical node.	The processing node status is stopping.
	`Starting` appears as the status of a physical node.	The processing node status is starting. Wait a while, and refresh the processing node information to recover the status. Confirm that the status of both nodes has recovered. If the status does not recover even after refreshing the processing node information several times, an error might have occurred while starting the OS. Check the status of the node in the **Cluster Management** dialog box for the physical node that is running. If neither physical node is running, contact maintenance personnel.
	The hardware status of the processing node is something other than `Normal`.	The hardware status of one of the physical nodes that make up the processing node is not `Normal`. The status of an element that makes up **Hardware Status** is not `Normal`. Confirm the status by using the **Health Monitor** button in the **Settings** tab. For details about statuses and causes of problems, see the explanation of how to view hardware information in the *Cluster Administrator's Guide*. For details about how to take recovery action, see Recovering hardware from a failure on page 4-41.
Information displayed for file system statuses	`Data corrupted` appears as the status of the file system.	The file system is offline due to an error in the OS. The mount status of the file system on the node side is `Fatal error`. For details about how to take recovery action, see Recovering from file system errors on page 4-15.
	`Device error` appears as the status of the file system.	The file system is offline due to an LU error (a multiple-drives error). The mount status of the file system on the node side is `Error`. For details about how to take recovery action, see Recovering from file system errors on page 4-15.

Location of problem	Type of problem	Cause and action
	`Expanding` appears as the status of the file system.	The file system is being expanded or an error occurred during expansion processing. Wait a while, and then refresh the processing node information. If the status does not change, an error might have occurred during processing. Acquire all the log data, and then inform maintenance personnel.
	`Reclaiming` appears as the status of the file system.	The unused capacity of the virtual LUs allocated to the file system is being released. Wait a while, and then refresh the processing node information. If the status does not change, an error might have occurred during processing. Acquire all the log data, and then inform maintenance personnel.
Information displayed for the System Software Installation Wizard	The KAQM20046-E message is displayed for a step in an update installation on the **Installation** page.	Possible causes are as follows: • A problem might exist with the network between the management server and the node. • Communication between the management server and node might not be set to go through `mng0` in the network configuration. If the OS is stopped, press the switch on the node to start the OS. If the dialog cannot be displayed after the OS starts, see If the File Services Manager GUI does not work correctly on page 1-7 and take the necessary actions. If you used the `routefilterctl` command to disable the reverse path filtering function, and if the communication between the management server and node is not set to go through `mng0` in the network configuration, check and revise the network configuration accordingly. After transferring the installation files, retry an update installation. If the error occurs repeatedly, acquire all log data, and contact maintenance personnel.
	The installation directory on the **Confirm** page displays the file path `C:\fakepath\install_files.tar.gz`, which was not specified.	The Web browser security functionality might have caused an attempt to acquire the file path to fail. Register the URL of the management server as a trusted site in the management client Web browser.

Location of problem	Type of problem	Cause and action
Edit HDvM Settings dialog box	The KAQM23020-E message is displayed.	There might be a problem with the communication processing because an HTTP request entity permitted by the Device Manager server exceeded a maximum. If necessary, ask the Device Manager administrator to expand the maximum length of HTTP request entities.
	The KAQM23028-E message is displayed.	Device Manager information might be incorrect. Check the values entered into the **Edit HDvM Settings** dialog box.
		The Device Manager server might not start. Check whether the Device Manager server has been started.
		There might be a temporary problem with the network. When Hitachi File Services Manager and Device Manager are on different servers, check for network problems by using the `tracert` and `telnet` commands. Confirm that there are no problems with the connection from Hitachi File Services Manager to Device Manager. [Example] `tracert` *`ip-address`* `telnet` *`ip-address`* `2001` (The Device Manager port number is 2001.)
		Access might be blocked by Windows firewall settings. Check the Windows firewall logs.
		Device Manager might be busy. If the error persists, change the notification time from the **Edit HDvM Settings** dialog box.
		There might be a problem with the Device Manager server. See the details of the message related to the problem in the Device Manager manuals.
HDvM Connection Management dialog box	Configuration information is not sent from Hitachi File Services Manager to Device Manager.	The management-target HDI system might be earlier than version 3.0.0. Check the version of the management-target HDI system.

Location of problem	Type of problem	Cause and action
Dialog boxes	The KAQM21100-E message is displayed.	The Hitachi File Services Manager information does not match the node information. You might not have refreshed the node after changing the configuration information in the Settings window, or a node operation might have been performed from another Hitachi File Services Manager instance or from the CLI. Click the **Refresh Processing Node** button to perform refresh processing.
Add Share dialog box and **Create and Share File System** dialog box	Local users and user names and group names set on an external server do not appear.	The Hitachi File Services Manager information does not match the node information. Click the **Refresh Users and Groups** button to perform refresh processing.
Create and Share File System dialog box	The KAQM23537-E message is displayed when a storage system is registered on the node.	A RAID group has been created, but there is not enough capacity on the disk to create an LU. Increase the disk capacity or reduce the size of the LU to be created, and then retry the operation.
Create and Share File System dialog box **Create File System** dialog box **Edit File System** dialog box	If **Yes** is selected for **Use namespace**, no values are displayed for **Tenant hard quota** or **Storage capacity used**, and the namespace cannot be used.	An error occurred during communication with the HCP system. Check the operating status of the HCP system. After that, in the Configuration Wizard, on the **6-3. HCP settings** page, click the **Test Connection** button. Confirm that a successful connection with the HCP system can be made, and then retry the operation.
Expand File System dialog box	When a file system that uses a namespace is being expanded, communication with the HCP system fails, and the KAQM26118-E message (HTTP return code: 100) is displayed.	An attempt to connect to the NIS server failed. Make sure that there are no problems with the NIS server settings or the network status. Resolve any problems, and then retry the operation.
Linking with Device Manager	An attempt to send configuration information from Hitachi File Services Manager to Device Manager fails (the KAQM23024-E, KAQM23025-E, or KAQM23026-E message is displayed).	See the causes of the KAQM23028-E message being displayed in the **Edit HDvM Settings** dialog box. See the action for the KAQM23028-E message in the Edit HDvM Settings dialog box.
	Unable to log in to the Device Manager GUI to use Hitachi File Services	If Hitachi File Services Manager and Device Manager are on different servers, the

Location of problem	Type of problem	Cause and action
	Manager (the KAQM23030-E message is displayed).	settings of the user account management server might be incorrect. If Hitachi File Services Manager and Device Manager are on different servers, make sure that the user account management server settings are correct. For details, see the *Installation and Configuration Guide*.
		A Device Manager administrator might not have administrator permissions for Hitachi File Services Manager. Give the the administrator permissions for Hitachi File Services Manager to the user who wants to log in to the Device Manager GUI to use Hitachi File Services Manager.
	The file system and mount information managed by Hitachi File Services Manager is not displayed in the Device Manager Management window.	The storage system used by the HDI system might not be registered in Device Manager. Register the storage system that LUN security is enabled for into Device Manager. For details, see the Device Manager manuals. After registering the storage system used by the HDI system into Device Manager, send the Hitachi File Services Manager configuration information again.
Configuration Wizard	On the **6-3. HCP settings** page, a connection test with the HCP system fails, and the KAQM26118-E message (HTTP return code: 100) is displayed.	An attempt to connect to the NIS server failed. Make sure that there are no problems with the NIS server settings or the network status. Resolve any problems, and then retry the operation.
	When the HCP system is being configured, on the **8. System settings** page, communication with the HCP system fails, and the KAQM26118-E message (HTTP return code: 100) is displayed.	

HCP linkage troubleshooting examples

The following troubleshooting examples relate to problems that might occur with HCP linkage.

Table D-2 HCP linkage troubleshooting examples

Problem	Cause and action
File systems cannot be created.	The tenant hard quota might be too small compared to the capacity of the namespace to be created. Ask the HCP administrator to revise the value for **Hard Quota**.
A migration or recall fails with the KAQM37037-E, KAQM37066-E, or KAQM37094-E message (HTTP return code: 400).	The user account for accessing tenants or namespaces might not have the necessary permissions for this operation. Ask the HCP administrator to revise the permissions.
A migration or recall fails with the KAQM37037-E, KAQM37066-E, or KAQM37094-E message (HTTP return code: 403).	• The user account information for accessing tenants or namespaces might be incorrect. Confirm the user name and password with the HCP administrator, and specify the correct information. • The user account for accessing tenants or namespaces might not have the necessary permissions for this operation. Ask the HCP administrator to revise the permissions. • The namespace might not exist. Check with the HCP administrator whether the namespace exists. • The settings might not allow custom metadata to be added to or deleted from namespace objects, or the settings might not allow you to overwrite metadata. Ask the HCP administrator to revise the namespace settings. • `Retention Class` might be set for the namespace. Use the HDI WORM functionality to set the retention period when the HCP and HDI systems are linked together. • The communication protocol (HTTP/HTTPS) settings for the HDI and HCP systems might not match. Revise the communication protocol settings by using the `arcsslctl` command. Ask the HCP administrator to revise the communication protocol settings.
A migration or recall fails with the KAQM37037-E, KAQM37066-E, or KAQM37094-E message (HTTP return code: 409).	• A conflict might have occurred with other HCP processing. Wait a while, and then try again. • Version management might not be enabled in the namespace settings. Ask the HCP administrator to enable version management.
A migration fails with the KAQM37037-E, KAQM37066-E, or KAQM37094-E message (HTTP return code: 413).	The capacity used by the HCP namespace might exceed the hard quota. Ask the HCP administrator to revise the value for **Hard Quota**.
A migration or recall fails with the KAQM37037-E, KAQM37066-E, or KAQM37094-E message (HTTP return code: 500 or 503).	An internal error might have occurred in HCP, or HCP might be temporarily unable to perform processing. Wait a while, and then try again.

Problem	Cause and action
A migration fails with the KAQM37038-E message.	Version management might not be enabled in the tenant settings. Ask the HCP administrator to enable version management.
One or more files that were migrated to the HCP system while the data was being imported from another file server have the `OFFLINE` attribute after the import finished.	If files are migrated to the HCP system while data is being imported from another file server, the files retain the OFFLINE attribute until another migration is performed after the import. Migrate the files again.
An HCP migration started while data was being imported from another file server, and now the data import is not making any progress.	If an HCP migration starts while data is being imported from another file server, the importing of all the files temporarily stops. The import resumes after the migration finishes.
A restoration is performed for migrated files, but some files are not restored.	Files are deleted synchronously from the HDI and HCP systems. If you delete files from the HDI system before restoration, the files are not restored to the HDI system. Restore deleted files from a previous version of the directory.
The HDI system cannot connect to the HCP system.	• The OS might not be restarted after the DNS server address set in the HDI system was changed. • The port for connecting to the HCP system might be blocked by some device used between the HCP and HDI systems. Verify that the communication ports for HTTP (80), HTTPS (443), and MAPI (9090) can be connected to.
Communication with the HCP system fails, and the KAQM26110-E message (HTTP return code: 302) is displayed.	The proxy server does not allow connection to the HCP system management port (9090). Change the proxy server settings to allow connection with port `9090`. Then, in the Configuration Wizard, on the **6-3. HCP settings** page, click the **Test Connection** button to confirm that a successful connection to the HCP system can be made.
Hard links cannot be created.	The creation of hard links for file systems whose data is migrated to the HCP system is disabled by default. Change the file system settings to create hard links. Note that hard link files cannot be restored from the HCP system.
Files with the OFFLINE attribute cannot be searched for.	Some clients do not search for files with the OFFLINE attribute. You can change the CIFS share settings so that the OFFLINE attribute is disabled. Note that some client operations might change (for example, timeouts will occur more frequently) if the OFFLINE attribute is disabled.
The migration of some files fails.	• Files whose file paths contain line feed codes are not migrated. Change the file name. • Timeout errors might occur if files are too large. Change the timeout value.

Problem	Cause and action
	• If a file is being updated at the moment the system checks whether the file can be migrated, the file is not migrated. The file is instead migrated the next time a migration is performed. Verify that no files are being updated during a migration. To forcibly migrate a file that is being updated at the moment the system checks whether the file can be migrated (by default, files that are being updated are not migrated), use the `arcconfedit` command to change the setting corresponding to the migrating of files that are being updated.
A migration or recall fails because a timeout occurs.	• If the files that failed are large, the timeout value for HCP communication might be too short. Change the timeout value. • An error might occur because the network bandwidth is low and the transfer speed to the HCP system reached the lower limit. Change the lower limit according to the network bandwidth. • The workload on the HCP system, HDI system, or network might be too high. Change the setting for the maximum number of threads. • A service might be running on the HCP system. Revise the migration schedule. • There might be some network problems. Revise the network.
The status of the migration task is `Last time interrupted`.	The migration task was stopped because migration did not finish before the preset duration elapsed. Because one or more files might not have been migrated to the HCP system, re-execute the task. If the task is placed in `Last time interrupted` status again, revise the duration.
User data cannot be used because the common key that is used to encrypt local data cannot be obtained from the HCP system.	An HCP system access failure occurred and a message in the range from KAQM05258-E to KAQM05264-E was output. Take appropriate action according to the message that was output. If the key displayed by the `encdisplaykey` command was saved to external media, and if correction of the failure takes a long time, you can use the `encrecoverkey` command to temporarily restore the common key that is used for encryption. However, even if the common key used for encryption is restored, you cannot use stub files until the HCP system access failure is corrected. To temporarily restore the common key that is used for encryption: 1. Use the `encrecoverkey` command to restore the common key that is used for encryption. 2. Use the `clstatus` command to check whether an error has occurred in the resource group. If an error has occurred, use the `rgstop` command to forcibly stop the resource group.

Problem	Cause and action
	3. Use the `clstatus` command to check the operating statuses of the cluster, node, and resource group. If the cluster or node has stopped, perform the following sequentially: a. If the cluster has stopped, start it by using the `clstart` command. b. If the node has stopped, start it by using the `ndstart` command. c. Start the resource group by using the `rgstart` command.

Virus scan troubleshooting examples

The following troubleshooting examples relate to problems that might occur when using the real-time scan function.

Table D-3 Virus scan troubleshooting examples

Problem	Cause and action
`Blocked (Access user info. is not registered)` is displayed for the **Server status** on the **List of Scanner Servers** page.	The user information for accessing the CIFS share is not registered on the scan server. On the scan server, check whether the target HDI host name exists in **Registered nodes** of the Hitachi Server Protect Agent Manager. If the target host name does not exist, use the Hitachi Server Protect Agent Manager to specify the node information, click **Add**, and then click **OK**. If the target host name exists, click the **OK** button in the Hitachi Server Protect Agent Manager. After specifying the settings on the scan server, use the HDI system to re-enable real-time scanning.
`Blocked (Time-out)` is displayed for the **Server status** on the **List of Scanner Servers** page.	There was no response from the scan server even after a certain period of time. Check whether a failure has occurred in the network or whether the scan server is heavily loaded. If you find a problem, take the appropriate action. In addition, if you are using scan software by Trend Micro and if you have selected an authentication method other than local authentication as the authentication method for CIFS users, check whether a failure occurred in the external authentication server. If a failure occurred, correct the failure.

CIFS access troubleshooting examples

The following troubleshooting examples relate to problems that might occur while accessing HDI from a CIFS client.

Table D-4 CIFS access troubleshooting examples

Location of problem	Type of problem	Cause and action
Non-specific	The added CIFS shares cannot be displayed on a client that is logging into the CIFS shares.	Automatic reloading of CIFS shares might have been disabled in a CIFS service-configuration definition. In the **Access Protocol Configuration** dialog box, on the **List of Services** page, restart the CIFS service or log in to the CIFS shares from the client again. For details on how to restart the CIFS service, see the *Cluster Administrator's Guide*.

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0)1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-90HDI029-12