Hitachi Data Ingestor

6.4.0

Single Node Troubleshooting Guide

This guide provides troubleshooting procedures for a Hitachi Data Ingestor (HDI) systems in single node configurations.

Contents

Hitachi Data Ingestor Single Node Troubleshooting Guide

Preface

This manual provides troubleshooting procedures for a Hitachi Data Ingestor (HDI) systems in single node configurations.

This preface includes the following information:

☐ Intended audience

☐ Product version

☐ Release notes

☐ Organization of HDI manuals

☐ Abbreviation conventions

☐ Document conventions

☐ Convention for storage capacity values

☐ Accessing product documentation

☐ Getting help

☐ Comments

Intended audience

This manual is intended for system administrators who operate and manage HDI systems in a single-node configuration.

Also, the user must have:

- 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 CIFS
- A basic knowledge of NFS
- A basic knowledge of Windows
- A basic knowledge of Web browsers

Product version

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

Release notes

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

Organization of HDI manuals

HDI manuals are organized as shown below.

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

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

Manual name	Description
Hitachi Data Ingestor Cluster Administrator's Guide, MK-90HDI038	This manual provides procedures for using HDI systems in a cluster configuration, as well as provides GUI references.
Hitachi Data Ingestor Cluster Troubleshooting Guide, MK-90HDI029	This manual provides troubleshooting information for HDI systems in a cluster configuration.
Hitachi Data Ingestor Single Node Getting Started Guide, MK-90HDI028	This manual explains how to set up an HDI system in a single-node configuration.
Hitachi Data Ingestor Single Node Administrator's Guide, MK-90HDI039	This manual explains the procedures for using HDI systems in a single-node configuration, as well as provides GUI references.
Hitachi Data Ingestor Single Node Troubleshooting Guide (This manual)	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.

Abbreviation conventions

This manual uses the following abbreviations for product names:

Abbreviation	Full name or meaning
Active Directory	Active Directory(R)
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
Internet Explorer	Windows(R) Internet Explorer(R)
Windows	Microsoft(R) Windows(R) Operating System

Abbreviation	Full name or meaning
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 • Microsoft(R) Windows(R) 8.1 32-bit • Microsoft(R) Windows(R) 8.1 64-bit • Microsoft(R) Windows(R) 8.1 Enterprise 32-bit • Microsoft(R) Windows(R) 8.1 Enterprise 64-bit • Microsoft(R) Windows(R) 8.1 Pro 32-bit • Microsoft(R) Windows(R) 8.1 Pro 64-bit
Windows Server 2012	A generic name for the following: • Microsoft(R) Windows Server(R) 2012 Datacenter • Microsoft(R) Windows Server(R) 2012 Essentials • Microsoft(R) Windows Server(R) 2012 Foundation • Microsoft(R) Windows Server(R) 2012 Standard

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click **OK**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `copy` *source-file target-file* *Note:* Angled brackets (< >) are also used to indicate variables.
`screen/code`	Indicates text that is displayed on screen or entered by the user. Example: `# pairdisplay -g oradb`
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `# pairdisplay -g <group>` *Note:* Italic font is also used to indicate variables.
[ ] square brackets	Indicates optional values. Example: `[a	b]` indicates that you can choose a, b, or nothing.

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 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 or1,000^2 bytes	1,024 KB or 1,024^2 bytes
1 GB	1,000 MB or1,000^3 bytes	1,024 MB or 1,024^3 bytes
1 TB	1,000 GB or1,000^4 bytes	1,024 GB or 1,024^4 bytes
1 PB	1,000 TB or1,000^5 bytes	1,024 TB or 1,024^5 bytes
1 EB	1,000 PB or1,000^6 bytes	1,024 PB or 1,024^6 bytes
1 block	-	512 bytes

Accessing product documentation

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

Getting help

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

Hitachi Vantara Community is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

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

Thank you!

1

General Procedure for Troubleshooting

This chapter explains how to identify the cause and location of an error that occurs in a Hitachi Data Ingestor (HDI) system.

☐ Overview of troubleshooting

☐ If a file system cannot be used

☐ If a Backup Restore functionality terminates with an error

☐ Viewing messages and related documents

Overview of troubleshooting

If an error occurs in the HDI system, first check whether you can access the HDI system. If you cannot access the HDI system when DHCP is in use, check whether the DHCP server and the HDI system can be connected, and then restart the HDI node. After you have become able to access the HDI system, disable the periodic saving of system configuration information. After that, refresh the GUI information, identify the cause of the error, and then perform error recovery.

Note that you need to set up an SSH environment before using commands. For details about how to set up an SSH environment, see the *Single Node Administrator's Guide*. For details about examples of errors that might occur during GUI or command operations, see Appendix C, Troubleshooting Examples on page C-1.

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.

Related items

- If a file system cannot be used on page 1-5
- If a Backup Restore functionality terminates with an error on page 1-7
- 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.

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.

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

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 4-8.

The flow chart below illustrates the steps to take when an HDI system cannot access an HCP system.
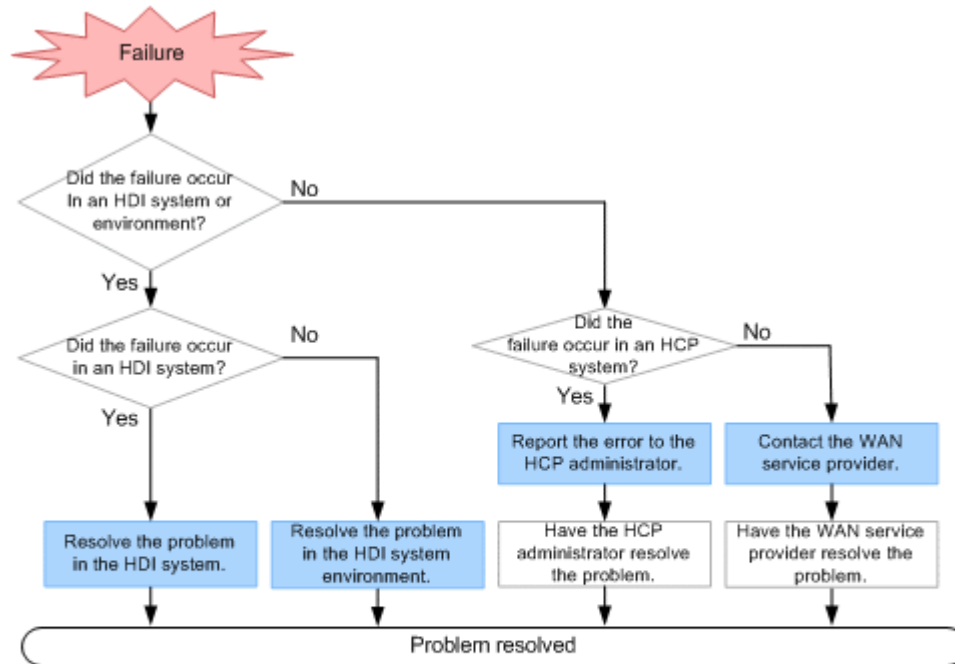
Figure 1-2 General troubleshooting procedure to follow when the HDI system fails to access the HCP system

If a file system cannot be used

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

If a file system cannot be created even though there is enough unused capacity, take action according to When files or directories cannot be created in a file system that does not support 64-bit inodes on page 4-4.

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

1. If an end user cannot access a file system, wait 20 minutes, and then ask the end user to access the file system again.

   If the end user can access the file system, no further action is necessary. If the end user cannot access the file system, go to the next step.

2. Check whether the file share used by the end user is an NFS share or a CIFS share.

   If an NFS share is stopped:

   > Check the IP address and shared directory name for the stopped service with the end user, to determine the file system or directory.

   If a CIFS share is stopped:

   > Check the shared path name for the stopped service (*name-of-host-on-node*#*CIFS-share-name**directory-path-used*) with the end user, to determine the 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.

   > #: You cannot specify, for the *name-of-host-on-node*, the alias registered in the CNAME record in the DNS.

3. Make sure that the node is turned on.

   If it is off, turn it 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.

4. Check the system messages on the node.

   If you cannot view system messages due to a system failure, take action according to Using a BMC to recover from a failure on page 4-31.

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

   Access from end users to the file system is temporarily suppressed during the following operations, and the file system is released from suppression when the operation terminates:

   ◦ Expanding the file system

   ◦ Configuration, expansion, and release of the temporary storage area for the Active File Migration function and Large File Transfer function

- Start and termination of data migration to HCP for file systems that use the Active File Migration function and Large File Transfer function

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

   In the **List of Services** page, check the operation status of the service used by the end user.

7. In the **File Systems** window, check the file system error information.

   If the service used by the end user is running and you cannot find an error in the service, the error might have occurred in the file system. See the File Systems window to check the status of the file system determined in step 1 above.

8. In the *file-system-name* window, check the settings of the file share.

   If the file system has been mounted normally, and you cannot find an error in the file system, see the *file-system-name* window to check the settings of the file share used by the end user.

   Check that the settings to enable resolution of host names are configured if the tab does not display an NFS share for which a host name or net group name has been specified. Check that DDNS is working correctly if DHCP is used. In addition, check the connection status of the following servers:

   - DNS server
   - NIS server
   - WINS server

   For details on how to check the connection status of the servers, see the *Single Node Administrator's Guide*. 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.

   If the file share is displayed but you are unable to find an error, check whether an error occurred in the operating environment of the network.

   Check the configuration and operating status of the network connecting the node and clients. For details about checking error information about network ports, see Using interface and network error information for error recovery on page 4-27.

   Also check the connection status of the node and the following servers:

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

   For details on how to check the connection status of the servers, see the *Single Node Administrator's Guide*. For details on the system

configuration and network configuration for an HDI system, see the *Single Node Getting Started 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 IP addresses of the node.

    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. Check whether a failure occurred in the HCP system.

    For details about how to check whether an access failure occurred in an HCP system, see Recovering from an HCP access failure on page 4-8.

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

If a Backup Restore functionality terminates with an error

If a Backup Restore functionality terminates with an error during execution, check whether an error message was output immediately before the termination to identify the site on which the error occurred and the cause of the error.

To identify the cause of the error, check the following items.

Table 1-1 Items to check when a Backup Restore functionality terminates with an error

Items to be checked	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
Resource error status on a node	Checking a resource error status on a node on page 2-4
File system error status	Checking the file system error status on page 2-6
Hardware status of a node	Checking the hardware status on page 2-10
Backup management software status and settings	Checking the backup management software status and settings on page 2-13

Viewing messages and related documents

The messages output by HDI and some of the related documents are used for both HDI cluster configurations and single-node configurations. As such, terms used in the messages and documents might differ from the terms used for HDI single-node configurations, and functionality not used by HDI systems in single-node configurations might be listed in the messages and documents.

- When reading messages, replace the following terminology with the corresponding terminology used in single-node configurations of HDI systems.

Table 1-2 Replacing the terminology used in cluster configurations of HDI systems

Terminology in messages	Terminology used in single-node configurations
Device file	LUs in the internal hard disk or storage system
Fixed IP address	IP address
System LU	System disk
User LU	User disk

- In explanations that refer to *clusters*, *nodes*, and *resource groups*, only the explanations pertaining to resource groups apply.
- Ignore any explanations regarding *virtual IP addresses*, *heartbeat ports*, *failovers*, and *failbacks*, because these terms are not used in single-node HDI systems.
- *Cluster management LU* refers to the drive capacity that has been allocated to store system settings information.

2

Identifying the Cause of an Error

This chapter explains how to check error information and 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 on identifying the cause of the error in this situation, see If a file system cannot be used on page 1-5.

☐ Checking error messages displayed in the GUI or standard error output

☐ Checking system messages on the node

☐ Checking a resource error status on a node

☐ Checking the file system error status

☐ Checking user mapping information

☐ Checking for a possible server connection problem

☐ Confirming that there are no problems with resolution of host names

☐ Checking the status of FC paths

☐ Checking the hardware status

☐ Checking the connection status with the HCP system

☐ Checking the communication of the network port

☐ Checking for a possible NTP time synchronization problem

Identifying the Cause of an Error

Checking error messages displayed in the GUI or standard error output

If a GUI operation causes an error, the GUI displays an error message. If a command operation causes an error, an error message is sent to the standard error output. Check the displayed error message to identify the cause of the problem.

For details on the error messages displayed, see the manual *Error Codes*.

If an error occurs during communication with the HCP system and the resulting error message displays a return value, report the return value to the HCP administrator and confirm the cause of the error and how to resolve it. If no return value is displayed, check whether there are any problems with the network or with the external servers. If no problems are found, ask the HCP administrator to check the status of the HCP system.

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:

$\text{KA}X^1X^2Y^1Y^2Y^3Y^4Y^5\text{-}Z$

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

Checking a resource error status on a node

You can use the `rgstatus` command to view the error status of resources on a node or to view the cause of the error. If the `rgstatus` command is executed, the resource status and the error information on a node are displayed in the following format:

resource-status/error-information

Checking a resource status

Check and identify the displayed resource status. The necessary action to take depends on the resource status.

Table 2-1 Resource statuses

Resource status	Description
Online	Running normally. Check the error information. For details on how to check error information, see Checking error information on page 2-4.
Online Pending	Starting.
Offline	Stopped.
Offline Pending	Stopping.
Partial Online	Some of the resources are blocked. A failure occurred on the hardware or an error occurred in the software. Take action according to Actions to take when `Partial Online` is displayed for the resource status: on page 2-5.

Checking error information

`No error` or `OS error` is displayed as the resource error information on the node. The cause of the error depends on the error information that is being displayed.

If `No error` is displayed:

The resources on the node are normal.

If `OS error` is displayed:

The one or more resources on the node have failed to start or stop. A hardware failure or a software error might be the cause of the problem. Check whether the system message KAQM35005-E, KAQM35007-E, or KAQM35008-E is output, and then take the appropriate action listed in the

Identifying the Cause of an Error

Hitachi Data Ingestor Single Node Troubleshooting Guide

Actions to take when `Partial Online` is displayed for the resource status:

If `Partial Online` is displayed for the resource status, take the following action:

1. Identify the resource that is being blocked by checking the message KAQM35001-E that is output directly before the system message KAQM35003-E.

   If the type of the blocked resource is `LVM_volume` or `Filesystem`, check the status of the file system in which the error occurred, and then take appropriate action.

   For details about checking the status of a file system, see Checking the file system error status on page 2-6.

2. Check the status of the node. If it is not `Online`, restart the node.

   For details about how to check the status of and restart the node, see the *Single Node Administrator's Guide*.

   If the system does not recover even after the node is restarted, acquire all log information, and then inform maintenance personnel.

Actions to take when `OS error` is displayed for the error information

Table 2-2 Messages to check and actions to take when error information displays "OS error"

Message	Directly preceding message	Two messages prior	Action
KAQM350 05-E	--	--	Acquire all the log files, and then inform maintenance personnel.
KAQM350 07-E	KAQM35009-E	--	Take the action for KAQM35009-E.
	KAQM35003-E	KAQM35001-E	Take the same action as for when `Partial Online` is displayed for the resource status. (For details, see Actions to take when `Partial Online` is displayed for the resource status: on page 2-5.)
			Check whether the KAQM05256-E system message, or a system message in the range from KAQM05258-E through KAQM05264-E was output, and take appropriate action for each message that was output.
		KAQM35002-E	Take the action for KAQM35002-E.

Message	Directly preceding message	Two messages prior	Action
	Any message other than the KAQM35*nnn* messages listed above	--	Acquire all the log files, and then inform maintenance personnel.
KAQM35008-E	KAQM35010-E	--	Take the action for KAQM35010-E.
	KAQM35004-E	--	Take the action for KAQM35004-E.
	KAQM35006-E	--	Acquire all the log files, and then inform maintenance personnel.
	Any message other than the KAQM35*nnn* messages listed above	--	Acquire all the log files, and then inform maintenance personnel.

Legend: --: Do not need to check

Checking the file system error status

If an error occurred in a file system, check the file system error status in the File Systems window, and then resolve the error.

The system administrator also needs to determine the cause of the error by checking the system messages displayed in the **List of RAS Information** page (for `List of messages`) of the Check for Errors dialog box around the time that the error occurred.

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:

- 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 node is 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 domains

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

- 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 you modify the user or group information managed by a domain controller (such as by re-creating a user or changing a user group), the system administrator restart the CIFS service or inform the end users to reconnect to the CIFS share after five minutes, in order for the information to be refreshed. If an end user is already connected to the CIFS share, they must disconnect and then reconnect the CIFS share.

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 the HDI system.

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 the HDI system, 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.

Using commands to 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.

Checking for a possible server connection problem

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

- DHCP server[#]
- DNS server[#]
- NIS server[#]

- NTP server[#]
- LDAP server
- CIFS client authentication server (domain controller)
- NFS client authentication server (KDC server)

The connection status between a node and non-DHCP servers can be checked in the **List of RAS Information** page (for `Server check`) in the **Check for Errors** dialog box. For details about how to check the connection status between a node and the servers, see Appendix A, Network Information on page A-1. Ask the network administrator to check the DHCP server.

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

Confirming that there are no problems with resolution of host names

If the system administrator can log in to the node, the system administrator needs to confirm that there are no problems with resolution of host names by using the `dig` command. In addition, check that DDNS is working correctly if DHCP is used.

To confirm that there are no problems with resolution of host names:

1. Log in to the target node by using the `ssh` command.

2. Confirm that there are no problems with resolution of host names 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 resolution of host names.

   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 problem still cannot be identified, take action according to Recovering from an HCP access failure on page 4-8.

Checking the status of FC paths

Use the fpstatus command to check whether any errors have occurred on an FC path. If an error occurs on an FC path, take appropriate action according to Recovering from FC path errors on page 4-24.

Checking the hardware status

Check whether there is a problem in the hardware. For details on how to check the hardware status from the GUI, see the *Single Node Administrator's Guide*. If you prefer to use commands to check the status, execute the hwstatus command. If the hardware status is not normal, take action according to Recovering hardware from a failure on page 4-31.

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 network port

If maintenance personnel ask you to check the communication of the network port, execute the `ping` command, specifying the network port.

Before starting the check procedure, prepare a worksheet as shown in Table 2-3 Worksheet for checking the communication of the network port on page 2-11. Use the worksheet to write down information acquired from the procedure.

Table 2-3 Worksheet for checking the communication of the network port

	Network port
IP address	
Check result	

To check the communication of the network port:

1. In the **List of Interfaces** page of the **Network & System Configuration** dialog box, check the IP address of the network port, and then write it down on the worksheet.

2. Execute the `ping` command by using the IP address 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 2-4 Example of a filled-out worksheet for checking the communication of the network port

	Network port
IP address	192.168.0.20
Check result	Failed

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:

o   Make sure that the node is properly connected with the NTP server.

o   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 on how to check the connection status between a node and the NTP server, see the *Single Node Administrator's Guide*. For details on 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.

Identifying the Cause of an Error

3

Collecting Data and Contacting Maintenance Personnel

This chapter describes how to collect log files.

System administrators must collect error information and send it to maintenance personnel if they cannot identify the error source or cause or cannot remedy an error. To analyze the cause of an HDI system error, the following log files are required:

- Node log files

- Node core files and dump files

To analyze and determine the cause of a network error, packet trace log files are required. To analyze and determine the cause of performance deterioration of the HDI system, performance statistics are required. Furthermore, to analyze the performance of the CIFS service, the CIFS-service performance analysis log files are required.

Note that, if a node stops because of an error in the output of a log file or a core file, garbled text might be output.

☐ Collecting node log files

☐ Collecting packet trace log files

☐ Collecting performance statistics

☐ Collecting the CIFS-service performance analysis log

Collecting node log files

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

As instructed by the message or maintenance personnel, download all log data, and then send the data to maintenance personnel.

To download system messages, system log data, and other log files in batch:

1. Click the **Action** menu in the top-left corner of the GUI, and choose **Download All Log Data**.
2. Click the **Download** button in the **Download All Log Data** dialog box.
3. In the Web browser download dialog box, specify where to download the files.
   The multiple log files are archived in tar format, compressed in gzip format, and then downloaded to the specified destination.
4. Click the **OK** button in the **Download All Log Data** dialog box.

If you want to download all the log files of a log group in one batch, follow the procedure below.

1. Display the Check for Errors dialog box by using either of the following methods:

   ○ Click the **Action** menu in the top-left corner of the GUI, choose **Launch**, and then **Check for Errors**.
   ○ In the **Settings** area of the *host-name* window, select **Check for Errors**.

2. In the **Info. type** drop-down list, select **Batch-download**, and then click the **Display** button.
3. Select the radio button for the log group you want to download in batch, and then click the **Download** button.
   Note: If you select a PSB log group, a dialog box asking you whether to perform a batch download is displayed before the download dialog box appears.
4. In the Web browser download dialog box, specify where to download the files.
   The log files that belong to the selected log group are archived in tar format, compressed in gzip format, and then downloaded to the specified destination.
5. Click the **Close** button in the download dialog box.

Some data might be missed if you perform a batch download to a disk with insufficient capacity for the temporary Internet files folder (in the case of Internet Explorer). Internet Explorer does not generate an error or message if this happens.

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 use the command, first see the *Single Node Administrator's Guide* to set up an SSH environment.

To collect the packet trace log files:

1. From a CIFS client or an NFS client, create an empty log file in any directory in a CIFS share or an NFS share that was created in HDI. When creating the log file, use a user account that has permission to create and delete log files.

   Create the empty log file in a file system that has at least 1 GB of free space. If the file system has less than 1 GB of free space, attempts to collect the packet trace log file might fail because of insufficient space. If you do not create an empty log file in advance, the collected packet trace log file will be created with root privileges and, as a result, you will not be able to delete the log file.

2. Log in to the target node by using SSH.

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. To specify an interface, add `-br` to the end of the interface name. For example, to collect information about the `eth1` interface, specify `eth1-br`. If you do not know the interface name or if you want to collect all the packet traces for all interfaces, specify `any`. You must specify this option. Note that, for interfaces for which a VLAN is set, specify the name in the following format:
   >
   > *port-name*.*VLAN-ID*`-br` (Example: `eth0.0010-br`)

   `-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 of the packet trace log file that was created in step 1. 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 is an example of executing the command to collect the packet trace log file (`/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.

```
$ sudo tcpdump -i eth1-br -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 unused space of the user disk 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.

4. Send the collected packet trace log file to the maintenance personnel.

5. From a CIFS client or an NFS client, delete the packet trace log file. When creating the log file, use a user account that has permission to create and delete log files.

Collecting performance statistics

To analyze and determine the cause of the performance deterioration of HDI system, ask the maintenance personnel for details about how to collect performance statistics, and then collect the log files. A log file output on 0:31 every day includes the performance statistics collected every minute from 0:00 to 23:59 of the previous day.

If the maintenance personnel ask you to collect performance statistics, use the following procedure.

1. Log in to the target node.
2. Use the `perfmonctl` command to view the current settings for performance statistics. If the performance statistics are not set to be collected, specify that they are to be collected. In addition, specify the directory to which performance statistics are to be transferred.

   You can collect log files from the day after you set the system to collect performance statistics.
3. Send the collected log data to the maintenance personnel.

   If you specified the transfer directory when you executed the command, access that directory and collect the log file with the following file name. You can collect log files from the day after you set the system to collect performance statistics.

   `perfdata_host-name_date-and-time-the-performance-statistics-were-collected` (format: `YYYY/MM/DD`)`.txt`

⚠️ **Note:**
- Do not modify the log file name.
- Do not create a file that has the same name as the log file.

   If you did not specify the transfer directory, or if the performance statistics could not be transfer to the directory (for example, due to insufficient memory), open the **Download All Log Data** dialog box, and then download all the log data. For details about how to download all the log data, see Collecting node log files on page 3-2.
4. After you send the log file, use the `perfmonctl` command to remove the setting of the destination directory for the performance statistics.
5. If you changed the setting in step 2 so that performance statistics are collected, change the setting by using the `perfmonctl` command so that performance statistics are no longer collected.

Collecting the CIFS-service performance analysis log

If the maintenance personnel ask you to collect the log file to analyze the CIFS service performance, use the following procedure.

1. Log in to the target node .
2. Use the `cifsinfogetctl` command to set the system to collect the CIFS-service performance analysis log.
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 and send all files in the subdirectories with names that begin with `cifsinfoget_` to the maintenance personnel.

⚠️ **Note:**
- Do not modify the log file name.
- Do not create a file that has the same name as the log file.

If you did not specify the log output directory, or if the performance analysis log could not be output to the directory (for example, due to insufficient memory), open the **Download All Log Data** dialog box, and then download all the log data. For details about how to download all the log data, see Collecting node log files on page 3-2.

4

Error Recovery

This chapter explains how to take recovery action.

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

If you (the system administrator) cannot fix the error, perform operation as instructed by the maintenance personnel.

If you manipulate a node or use a command when recovering the system from an error, you must refresh the view to update the information about the file systems displayed on the GUI.

☐ Checking and retrying any erroneous GUI operations

☐ Checking and retrying any erroneous command operations

☐ Checking system messages and recovering from an error

☐ Recovering from file system errors

☐ Recovering from an HCP access failure

☐ Recovering from failures that occur in the work space of the Active File Migration function and Large File Transfer function

☐ 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

Error Recovery

Hitachi Data Ingestor Single Node Troubleshooting Guide

Checking and retrying any erroneous GUI operations

If an error occurs due to an improper operation in the GUI, such as an incorrect setting or operational mistake, refresh the information displayed in the GUI, and then retry the operation as instructed by the message.

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.

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 might output messages and the message IDs, see Checking system messages on the node on page 2-3.

Recovering from file system errors

This subsection describes the actions that you need to take to recover from errors in a file system operated by an HDI system.

If an error occurs in a file system operated by HDI, see **Mount Status** in the GUI, or execute the `fslist` command to check the file system status, and then take appropriate action.

When the GUI displays `Data corrupted` in **Mount Status**, or when 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 insufficient capacity in a pool allocated to a volume group.

- ○ If you are using a storage system

  Check whether `KAQG90009-E` is displayed in the system messages on the node. If the error is displayed, take action according to When a file system is blocked due to insufficient capacity for a pool on page 4-7. If the error is not displayed, take action according to When the file system is blocked due to an error in the OS on page 4-5.

- ○ If you are not using a storage system

  The file system might be blocked due to an error in the OS. Take action according to When the file system is blocked due to an error in the OS on page 4-5.

When the GUI displays `Device error` in **Mount Status**, or when the `fslist` command displays `error` in `Device Status` and `fatal error` in `Mount Status`.

The file system is blocked due to an error in a disk allocated to a volume group. Take action according to When a file system is blocked due to an error in a disk allocated to a volume group on page 4-5.

In this case, an error might have occurred in a FC path at the same time as an error in a disk allocated to a volume group. After taking action for the blocked file system, use the **Hardware** window or the `fpstatus` command to check if any errors occurred in the FC path.

If an error occurs in an FC path, take action according to Recovering from FC path errors on page 4-24.

To restore a file system that does not synchronize data with any other HDI system via a linked HCP system, follow the appropriate procedures in Restoring a file system migrated to an HCP system on page 4-11 to recreate the file system and restore backup data. However, if a failure 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 4-13 to recover both from the error.

To restore a read-write-content-sharing file system, follow the appropriate procedures in Recovering a read-write-content-sharing file system on page 4-17 to restore data.

When files or directories cannot be created in a file system that does not support 64-bit inodes

In file systems that do not support 64-bit inodes, inode information is stored in an area that occupies the first 1 TB of the file system. File data is also stored in this inode area. When the capacity of the inode area becomes insufficient, files and directories cannot be created even if there is enough available capacity for file data in the file system. In order to address insufficient capacity in the inode area, apply one of the following measures. For details about how to use each command, see the *CLI Administrator's Guide*.

- Expanding the capacity of a file system

  When file system capacity is expanded by using the `fsexpand` command, the inode area is automatically reconfigured and file data of up to 10 GB is moved outside of the inode area if all of the following conditions are met:

  ○ The capacity of the file system after expansion is 1 TB or more.

  ○ The file system does not support 64-bit inodes

  Moving 10 GB of data takes up to about 50 minutes.

  The system message KAQM04288-I is output when reconfiguration of the inode area starts, and the system message KAQM04289-I is output when reconfiguration is complete. Use the `fslist` command to view system

information before and after reconfiguration of the inode area, and check that `I-node free` (the number of remaining inodes) has increased. Note that when the expanded size of the file system exceeds 10 GB, it might be possible to increase available capacity of the inode area further by executing the `fsinodespace` command as well.

- Reconfiguring the inode area

  When the inode area is reconfigured by using the `fsinodespace` command, file data is moved outside of the inode area if all of the following conditions are met:

  - The capacity of the file system is 1 TB or more
  - The file system does not support 64-bit inodes

  Moving 10 GB of data takes up to about 50 minutes. For details about the processing time required to move more than 10 GB of data, see the `CLI Administrator's Guide`.

  The system message KAQM04288-I is output when reconfiguration of the inode area starts, and the system message KAQM04289-I is output when reconfiguration is complete. Use the `fslist` command to view system information before and after reconfiguration of the inode area, and check that `I-node free` (the number of remaining inodes) has increased. If `I-node free` (the number of remaining inodes) does not increase even when the maximum volume of data to be moved is increased, consider expanding the file system.

- Change the setting to correspond to 64-bit inodes

  Use the `fsinodectl` command to change the file system settings to support 64-bit inodes. Note that this change is irreversible. For notes about supporting 64-bit inodes, see the *Installation and Configuration Guide*.

When the file system is blocked due to an error in the OS

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

1. Delete the blocked file system.
2. Restart the node.
3. Re-create the file system by using the `fscreate` command.
4. Mount the file system by using the `fsmount` command.
5. Restore the backup data to the re-created file system.
6. Re-create the file share.

   In the **Add Share** dialog box, you must select **Use existing directory as is**, because the file system has been restored from backed-up data.

When a file system is blocked due to an error in a disk allocated to a volume group

Use either of the following methods depending on the number of volume groups created.

When there is only one volume group

Delete the file system and the volume group. To restore a file system with help from maintenance personnel.

1. Ask maintenance personnel to remove the cause of the error, to re-install the OS on the node, and to initialize the user disks.

2. Restore the system configuration information and user data.

   - If data is migrated to the HCP system, the system configuration information and user data are restored from the HCP system at the same time. For details, see Batch restoration of system configuration information and user data on page 4-21.

   - If data is not migrated to the HCP system, take action as follows:

   a. Restore the system configuration information.

   b. Delete the blocked file system.

   c. Execute the `vgrdelete` command to delete the volume group.

   d. Execute the `vgrcreate` command to re-create the volume group.

   e. Create a new file system.

   f. Restore the backup data to the new file system.

When there are multiple volume groups

Check the status of the volume group in which the error occurred, and then take the necessary action according to the following procedure with help from maintenance personnel.

1. If an error occurred in a volume group in the storage system, replace the disk with help from maintenance personnel.

2. Use the `vgrlist` command to identify the volume group and disk in which the error occurred.

   The required procedure varies depending on the information displayed for `Total size(GB)`.

   To take corrective action if – is displayed for `Total size(GB)`:

   a. If the error occurred in a volume group in an internal hard disk, replace the disk with help from maintenance personnel.

   b. Use the `nasreboot` command to restart the node.

   c. Use the `rgstatus` command to check the status of the node.

      If `Online/No Error` is not displayed, execute the `rgstop` command with the `-f` option.

   d. Use the `vgrdelete` command to delete the volume group in which the error occurred.

   e. If you executed the `rgstop` command with the `-f` option specified, execute the `rgstart` command.

   f. Use the `vgrcreate` command to create a volume group.

To take corrective action if a capacity is displayed for `Total size(GB):`

a. Execute the `vgrrepair` command with the `--list` option.
   Record the failed file system.

b. Delete the file system displayed for `List of unavailable file systems:` when you executed the `vgrrepair` command with the `--list` option.

c. If an error occurred in a volume group in an internal hard disk, replace the disk with help from maintenance personnel.

d. Use the `nasreboot` command to restart the node.

e. Use the `vgrrepair` command to correct the volume group.

f. Use the `vgrexpand` command with additional LUs specified to expand the volume group.

3. If you deleted the file system, re-create the file system and file shares.

4. Use the `arcrestore` command to restore the user data from the HCP system.

⚠️ **Note:**

- When restoring a file system for which data is not synchronized with that of other HDI systems via the linked HCP system, if files or directories already exist in that file system, you cannot execute the `arcrestore` command. 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, and then re-execute the `arcrestore` command with the `--skip` option specified.

---

5. Review migration task setting, and please change setting as required.

When a file system is blocked due to insufficient capacity for a pool

To restore a file system that is blocked due to insufficient capacity for a pool with help from storage system administrator:

1. Ask the storage system administrator to provide sufficient capacity for the pool.

2. Restart the node.

A file system for which a work space is set is blocked

To restore a file system for which a work space is set is blocked, perform the following procedure.

1. Recover the file system from the error.
   See sections When files or directories cannot be created in a file system that does not support 64-bit inodes on page 4-4 to When a file system is

and recover from errors by taking action according to the procedure that corresponds to the cause of the error.

2. Delete the file system.

   Delete the blocked file system.

3. Re-create the file system.

A file system for which a work space is set is blocked due to insufficient pool capacity

To restore a file system for which a work space is set is blocked, perform the following procedure.

1. Ask the storage system administrator to resolve the problem with the insufficient pool capacity.

   If the pool is being formatted on 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. Delete the file system.

   Delete the blocked file system.

3. Restart the node.

4. Re-create the file system.

Recovering from an HCP access failure

If any of the following 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.

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.

   If you find a problem, contact maintenance personnel. If you do not find any problems, go to the next step.

5. Check the DNS server and the switch of the front-end LAN. Also, check the remote access environment, such as the NAT, VPN, or proxy server settings.

   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.

Recovering from failures that occur in the work space of the Active File Migration function and Large File Transfer function

This section describes the actions that you need to take to recover from errors in a work space.

An access failure has occurred in an internal hard disk or an LU in the storage system

If an access failure occurred in an internal hard disk or an LU in the storage system, use the following procedure to correct the failure.

To remedy an access failure in an internal hard disk or an LU in the storage system:

1. Check the status of the FC path.

   When the status of the FC path is normal

   > Check with the maintenance personnel whether an error occurred on the storage system. If an error occurred, take action as described in .

   > If no error occurs in the storage system, let the maintenance personnel know that the task is completed, and then proceed to step 2.

   When the status of the FC path is not normal

   > Take action by following the instructions in . After that, proceed to the next step.

2. Check the status of the work space.

   If the status of the work space is `Error`, perform the procedure described in .

If an error occurred on a storage system

Work with the maintenance personnel to perform the following procedure:

To correct the error:

1. Set the user LU assignment function to the maintenance mode by using the `lumapctl` command.
2. If the Large File Transfer function is enabled, disable it for the file system that contains the LU in which the failure occurred.
3. For the work space containing the failed LU, release the work space.
4. Ask the maintenance personnel to eliminate the error on the storage system.
5. Restart the OS.
6. Set up the work spaces again.
7. If the Large File Transfer function was disabled in step 2, enable the function again.
8. Set the user LU assignment function to the normal operation mode by using the `lumapctl` command.

Recovering from a work space error

To recover from a work space error, perform the following procedure:

1. If the Large File Transfer function is enabled, disable it for the file system that contains the work space in which the failure occurred.
2. Release the work space.
3. Restart the node.
4. Set up the work space again.
5. If the Large File Transfer function was disabled in step 1, enable the function again.

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 an 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.

If data was backed up to a tape device, after restoring the data of the HCP system, you must restore the data from the tape device. For details, see the *Single Node Administrator's Guide*.

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

1. If the Large File Transfer function is enabled, ask the HCP administrator to delete unnecessary data (objects whose names end with `.tmp`) in the HCP system.
2. Use the GUI to 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:

   - File system name
   - ACL type
   - How the HCP system is linked to (at the file system or share level)
   - How data is shared with other HDI systems via the linked HCP system
   - Whether the Active File Migration functionality is enabled
   - Whether the Large File Transfer functionality is enabled
   - Whether past versions of files are shown to clients
   - Whether the WORM function is enabled
   - If the WORM function is enabled, which mode of the autocommit function is to be used
   - Whether CIFS bypass traverse checking is enabled

Also, specify a mount point of the file system as the shared directory. If the directory is created directly under the mount point, you cannot restore the data of the HCP system.

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.

3. In the GUI, disable the migration schedule that was set for the file system.

   If the migration task is performed before executing the `arcrestore` command, you cannot restore the data from before the failure occurrence, because the data on the target file system is migrated to the HCP system.

4. If the mount point is not specified as the shared directory in the file system in which the failure occurred, delete the file share that was created in Step 1.

5. Restore the file system by using the `arcrestore` command.

⚠ **Note:**

- When restoring a file system for which data is not synchronized with that of other HDI systems via the linked HCP system, if files or directories already exist in that file system, you cannot execute the `arcrestore` command. If a file share has been created before executing the `arcrestore` command, data restoration from the HCP system might fail.

- To restore the data migrated to an HCP system into a WORM file system with autocommit enabled, execute the `arcrestore` command with the `--background` option specified. Any file that has not been turned into a WORM file at the time of migration is also not a WORM file at the restoration destination. Because the time that stub processing is applied to the file is the starting point of the autocommit period, it is necessary to restore all files as stub files in the background to change all restored files to WORM files as soon as possible.

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

- When a file system is restored, the reserved space used by the system will be set at 5% of the total capacity of the file system. Change the settings for the reserved space by using the `arcresvset` command as necessary.

---

6. Set a cache resident policy by using the `arcresidentpolicyset` command.

   Change the settings by using the `arcresidentpolicyset` command to stop files whose capacity is not less than the lower threshold of the file size for applying the Large File Transfer function from being turned into stub files.

7. Create a file share for the file system.

8. Review migration task setting, and please change setting as required.

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 both 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 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)
   - ○ How data is shared with other HDI systems via the linked HCP system
   - ○ Whether past versions of files are shown to clients
   - ○ Whether the WORM function is enabled
   - ○ If the WORM function is enabled, which mode of the autocommit function is to be used
   - ○ Whether CIFS bypass traverse checking is enabled

   Also, specify a mount point of the file system as the shared directory. If the directory is created directly under the mount point, you cannot restore the data of the HCP system.

   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. In the GUI, disable the migration schedule that was set for the file system.

   If the migration task is performed before executing the `arcrestore` command, you cannot restore the data from before the failure occurrence, because the data on the target file system is migrated to the HCP system.

5. If the mount point is not specified as the shared directory in the file system in which the failure occurred, delete the file share that was created in Step 3.

6. Restore the file system from the replica HCP system to the HDI system by using the `arcrestore` command. #

⚠️ **Note:**

- When restoring a file system for which data is not synchronized with that of other HDI systems via the linked HCP system, if files or directories already exist in that file system, you cannot execute the `arcrestore` command. If a file share has been created before executing the `arcrestore` command, data restoration from the HCP system might fail.

- To restore the data migrated to an HCP system into a WORM file system with autocommit enabled, execute the `arcrestore` command with the `--background` option specified. Any file that has not been turned into a WORM file at the time of migration is also not a WORM file at the restoration destination. Because the time that stub

processing is applied to the file is the starting point of the autocommit period, it is necessary to restore all files as stub files in the background to change all restored files to WORM files as soon as possible.

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

- When a file system is restored, the reserved space used by the system will be set at 5% of the total capacity of the file system. Change the settings for the reserved space by using the `arcresvset` command as necessary.

7. Create a file share for the file system.

8. Review migration task setting, and please change setting as required.

9. Start operation from the replica HCP system.

10. Recover the primary HCP system from the failure.

11. Perform a data recovery from the replica HCP system, and then copy the data on the replica HCP system to the primary HCP system.

12. Finish the data recovery between the primary HCP system and the replica HCP system.

13. Reset the host name of the primary HCP system for the HCP host name by using the `archcpset` command or the GUI.

14. 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 7. This will, however, cause the recovery of some past version directories to fail in Step 6, 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, immediately execute a migration.

Recovering a read-write-content-sharing file system

This section describes how to recover the integrity of a read-write-content-sharing file system with the HCP system, which would be lost if the integrity is recovered from a failure or if an HDI system is maintained.

The recovery method differs depending on the cause for integrity recovery.

If the file system or OS is recovered from a failure or if an HDI system is turned off

To recover the integrity with the HCP system, all files and directories in the share (except for the files and directories in the `.conflict` and `.conflict_longpath` directory) will be automatically re-synchronized when mounting the file system. Therefore, no user action is required.

However, if a failure occurs during communication with the HCP system for mounting the file system or if the node OS has not been restarted for over 10 days, the integrity with the HCP system will not be automatically recovered. If the file system does not have integrity with the HCP system, a directory operation or migration will result in an error, causing the KAQM37509-E message to be sent by an SNMP trap or email. In such a case, inform the end-users to stop accessing the share, and then take appropriate action according to the message and restart the resource by using `rgstop` and `rgstart` commands.

Note:

If an updated file exists that is not migrated to the HCP system when recovering the integrity with the HCP system, the file will be stored in the .conflict directory. Additionally, stub processing will be performed for all files in the file system, resulting in lower access performance.

If an HDI system is shut down as planned for maintenance

Use the following procedure:

1. Start the OS on nodes.
   Turn on the power to the node.
2. Check that the resource is running normally by using the `rgstatus` command.
3. Wait for 10 minutes or so for the migration task for the read-write-content-sharing file system to start, or execute the migration task immediately.
   To immediately execute the migration task, in the **Migration Tasks** dialog box, select the target file system, and then click the **Migrate Immediately** button.
4. Check that no KAQM37509-E message is output.
   If the KAQM37509-E message is output, take appropriate action according to the message.

5. On the *migration-task* page in the **Migration Tasks** dialog box, or with the `arctaskstatus` command, check the progress of the migration task.

When the task is complete, inform the end-users to restart accessing the share.

If the task fails, check whether the KAQM37507-E or KAQM37509-E message is output, and then take appropriate action according to the output message.

Restoring system configuration information

This subsection describes what actions to take when the system configuration information is invalid due to an error that occurred in the disk of the node. Work with maintenance personnel to resolve any problems. If data has been migrated to an HCP system and you want to restore only the system configuration information, see Restoring system configuration information from an HCP system on page 4-19. If data has been migrated to an HCP system and you want to restore both the system configuration information and the user data, see Batch restoration of system configuration information and user data on page 4-21.

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:

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 **System Configuration Wizard** or GUI **Service Configuration Wizard** after the maintenance personnel finish the initial setup.

   If you execute the GUI **System Configuration Wizard** or GUI **Service 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.

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

   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. If the data stored in an HCP system was encrypted, restore the common key for encryption by using the `hcprecoverkey` command.

6. 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.

7. Ask NFS clients to mount the file shares.

8. Delete the uploaded system configuration file.

9. If you were using the NDMP server, the password for the NDMP server will be initialized. To prevent unauthorized access, change the password.

Restoring system configuration information from an HCP system

This subsection explains what to do if the system configuration information becomes invalid because of an error occurring on the hard disk of a node in an environment where the system configuration information is saved in an HCP system. Use the system configuration information saved in the HCP system to perform 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, to execute commands, you will need the SSH secret key corresponding to the SSH public key that was registered on 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 has occurred on the hard disk of the node:

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 **System Configuration Wizard** or GUI **Service Configuration Wizard** after the maintenance personnel finish the initial setup.

If you execute the GUI **System Configuration Wizard** or GUI **Service 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 by using the `syslurestore` command.

   Specify the `--trans` and `--system-only` options, and then execute the `syslurestore` command to restore all system disks. 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 host when you saved the system configuration information.

   The public key that was registered before the error occurred will also be restored.

6. If maintenance personnel changed the network configuration in Step 1, restore the configuration.

7. Log in again to the node.

   Use the SSH secret key that corresponds to the public key that was restored in Step 5.

8. Check whether error messages related to the file system 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.

9. Ask NFS clients to mount the file shares.

10. If you were using the NDMP server, the password for the NDMP server will be initialized. To prevent unauthorized access, change the password.

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 autocommit 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 record file creation dates and times

- Configuration information regarding the initial mode for executing a migration task

- 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.

Batch restoration of system configuration information and user data

This subsection explains what to do if the system configuration information and user data becomes invalid due to an error occurring on the hard disk of the node in an environment where the system configuration information is saved to an HCP system and user data is migrated to the HCP system. 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 hard disk of the node:

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 **System Configuration Wizard** or GUI **Service Configuration Wizard** after the maintenance personnel finish the initial setup.

   > If you execute the GUI **System Configuration Wizard** or GUI **Service 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 host when you saved the system configuration information.

   The public key that was registered before the error occurred will also be restored.

6. If maintenance personnel changed the network configuration in Step 1, restore the configuration.

7. Log in again to the node.

Use the SSH secret key that corresponds to the public key that was restored in Step 5.

8. Check whether error messages related to the file system 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.

9. Ask NFS clients to mount the file shares.

10. If you were using the NDMP server, the password for the NDMP server will be initialized. To prevent unauthorized access, change the password.

Note that the following information cannot be restored:

- The configuration information for the file system that was not mounted when saving the information, including:

  o The minimum and maximum retention periods

  o The autocommit settings

  o Whether to send requests to delete files stored in an HCP system

  o Whether to issue warning messages regarding file system capacity shortages

  o Whether to record file creation dates and times

- Configuration information regarding the initial mode for executing a migration 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 an error might have occurred on an FC path while the storage system is being used, the system administrator uses the `fpstatus` command to check the status of the FC path, and then corrects the error.

When Error is displayed for one of the paths

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

(a) An error occurred in an FC path because of a disconnected FC cable.

(b) After an FC path was changed or deleted, the node was restarted.

(c) An FC path is not set up because no LUs are allocated to the storage system host group associated with the FC path.

When (a) or (b) is the cause of the error, take action as shown below. When (c) is the cause of the error, take action according to the procedure described in .

1. Check the status of the FC port on the node (`HostPort`) and the FC cable connected to the FC port on the storage system (`ArrayPort`).

   If an error occurred:
      Remove the cause of the error, and then put the FC path online by using the `fponline` command.

   If no error occurred:
      Restart the node.

2. Check the status of the FC path by using the `fpstatus` command.

When Online (LU Error) is displayed for both paths

If `Online (LU Error)` is displayed, a temporary failure might have occurred in the paths, or an error might have occurred in one or more of the LUs on the paths.

The following is the procedure for resolving the problem of `Online (LU Error)` being displayed because of a temporary path failure.

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. With maintenance personnel, recover the LUs in the storage system from the error.
2. Put the FC paths online by using the `fponline` command. Alternatively, execute the `fpstatus` command to check the status of the relevant FC paths.
3. Restart the node.
4. Check the status of the relevant FC paths by using the `fpstatus` command.

When Error is displayed for both paths

If `Error` is displayed for both paths, any of the following might have occurred or been performed:

(a) A failure occurred with all the LUs accessing the target FC paths, or an error occurred on the FC paths.

(b) After FC paths were changed or deleted, the node was not restarted.

(c) FC paths are not set up because no LUs are allocated to the storage system host groups associated with the FC paths.

For (a) or (b), take action as shown below. For (c), take action according to the procedure described in .

1. Check the status of the FC port on the node (`HostPort`) and and FC cable connected to the FC port on the storage system (`ArrayPort`).

   If an error occurred:
   > Remove the cause of the error, and then go to next step.

   If no error occurred:
   > Restart the node, and then confirm that the status of the FC paths is displayed correctly by using the `fpstatus` command.
2. Put the FC paths online by using the `fponline` command.
3. Check the status of the FC paths by using the `fpstatus` command.
   If the status of the FC paths is normal, then this is the last step for the error recovery procedure. If the FC paths are still in an error status or if a file system on the recovered FC path is blocked, go to the next step.
4. With maintenance personnel, recover the LUs in the storage system from the error.
5. Restart the node.
6. Check the status of the FC paths by using the `fpstatus` command.

When Configuration Mismatch is displayed for both paths

If `Configuration Mismatch` is displayed for both paths, the LU allocation to the host groups associated with one FC path might differ from the LU allocation to the host groups associated with an alternate path.

To recover from the error:

1. If no alternate path is set, ask maintenance personnel to set up one.
2. Check whether the same LUs are allocated to each host group set for the FC port (`ArrayPort`) on the storage system for the relevant path.

   If the settings differ, re-allocate the LUs so that the same settings are configured for each host group.
3. Restart the node.
4. Check the status of the relevant FC path.

When Unknown is displayed for both paths

If `Unknown` is displayed for both paths, the host port or array port might not be able to identified. If this happens or if FC paths are not set up because no LUs are allocated to the host groups associated with the FC paths, take actions as follows:

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

   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`) and the FC cable connected to the FC port on the storage system (`ArrayPort`).
4. Check the host security for the paths.
5. Allocate the same LUs to host groups set up for the FC port on the storage system (`ArrayPort`) for the paths.
6. Restart the node.
7. Check the status of the relevant FC paths.

When Partially Online is displayed for a specific FC path

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

To recover from the error:

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

When Configuration Mismatch is displayed for one of the paths

If `Configuration Mismatch` is displayed for one of the paths and if no information is displayed for the other path, an alternate path is not set. The path for which no information is displayed is assumed to be in the `Error` status. Take action according to <u>When Error is displayed for one of the paths on page 4-24</u>.

When FC path information is not displayed

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

To recover from the error:

1. Check the connections of the FC cable used by the path, and then remove the cause of the error.
2. Check the status of the FC path again.
3. Restart the node.

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.

Check the IP address for the network ports

> Check whether the IP addresses and netmasks are specified correctly. If the specified values are incorrect, specify the correct values.
>
> Specify the IP addresses and netmasks in the **Edit Interface** page.
>
> After specifying the correct values for the IP addresses and netmasks, 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 network ports

> Make sure that the negotiation mode setting of the network ports 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 network ports 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 network ports 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.

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:

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

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

Check the cable.

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

Check the switch.

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

If there is no problem with the cable or switch, there might be a problem with the 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 the HDI system. 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 4-28.

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 the **Change Active Port Status** button. `Active` is displayed in **Status** for **Active port**, and normal operation begins. If **Status** for **Active port** does not change to `Active`, contact 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 4-28.

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 the HDI system.

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

If there is no problem with the cable or switch, there might be a problem with the HDI system hardware. Contact the maintenance personnel to resolve the problem.

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 the HDI system. 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 the hardware status is abnormal, you must recover the hardware from the failure.

If you notice a failure in FC paths or Ethernet interfaces, take action according to <u>Recovering from FC path errors on page 4-24</u> or <u>Using interface and network error information for error recovery on page 4-27</u>.

For other hardware failures, contact maintenance personnel for recovery.

Using a BMC to recover from a failure

If you cannot view system messages due to a system failure, you can investigate the failure and recover from it by using a Windows computer connected to the BMC port on the node. This section explains how to use the BMC to recover from a failure. Note that when you use a Windows computer connected to the node, pressing **Ctrl**+**Alt**+**Del** will restart the OS of the node.

The procedure to recover from a failure by using a BMC differs depending on the used product. The name of the product used for the node can be acquired by using the `hwstatus` command.

When Compute Rack is used for the node

To use the BMC to recover from a failure when Compute Rack is used for the node:

1. Plug a Windows computer in and start it.
2. Make sure that the IP addresses of the BMC port and the Windows computer are part of the same network segment.
   The IP address of the BMC port is specified in the same network segment as the IP address of the port used for maintenance (`pm0`) (the host part is fixed to `40`). For example, if the IP address of `pm0` is `10.0.0.51`, the IP address of the BMC port is `10.0.0.40`.
   If the network segments are different, change the IP address of the Windows computer so that the IP addresses are both part of the same network segment.
3. Connect the Windows computer to the BMC port on the node with a LAN cable (a cross cable).
4. Execute the `ping` command from the command prompt of the Windows computer.
   If communication can be established, go to the next step. If communication cannot be established, contact maintenance personnel.
5. Open a web browser on the Windows computer and enter the following address in the address bar.
   `https://BMC-IP-address`

From the login window, enter `user01` for the user name and `pass01` for the password.

The Server Information window is displayed.

6. Click the **Server Settings** tab, and then click the **Remote KVM** button in the Language Settings window.

The Remote KVM Settings window is displayed.

7. Select the **RELATIVE Mode** radio box, and then click the **Modify** button.

8. Click the **Logout** button to log out.

9. Double click the Remote Console shortcut on the Windows PC's desktop.

The Remote Console window appears.

If there is no Remote Console shortcut, see the documentation for Remote Console provided with the hardware, and then install the application.

10. Configure the following specifications in the Remote Console window:

- **IP Address**: *BMC-IP-address*
- **User ID**: user01
- **Password**: pass01
- **Port Number**: 5001

Leave items other than the above items as their defaults.

11. Click the **Connect** button to check whether the login prompt is displayed.

If `Copy dump file start:` is displayed, wait 10 minutes, and then check whether the login prompt is displayed.

If the login prompt is displayed, execute the `ping` command to check the network status for the ports used for system management and data access, and resolve any problems. For details on how to recover from a failure, see Using error information on the data port for error recovery on page 4-30. If there are no network problems, go to step 14.

If there is no response, go to the next step.

12. Check the MAINTENANCE lamp of the node.

If something other than `00` is displayed, an error has occurred. Contact maintenance personnel. If `00` is displayed, go to the next step.

13. Press the RESET switch to restart the node.

The RESET switch is located between the SERVICE lamp switch and the BUZZER STOP switch. Use a thin object such as a paper clip to press the button.

It takes about 10 minutes to restart the node. After the node has restarted, the login prompt is displayed. If the node was successfully restarted, go to the next step. If restarting fails, contact maintenance personnel.

14. Check whether clients can access the file systems on the node.

If clients can access the file systems, the system has been successfully recovered. Ask maintenance personnel to collect dump information. If clients cannot access the file systems, contact maintenance personnel.

When PowerEdge is used for the node

To use the BMC to recover from a failure when PowerEdge is used for the node:

1. Plug a Windows computer in and start it.

2. Make sure that the IP addresses of the BMC port and the Windows computer are part of the same network segment.

   Use the LCD panel on the node to confirm the BMC port IP address. For details about how to check the IP address, see the hardware documentation.

   If the network segments are different, change the IP address of the Windows computer so that the IP addresses are both part of the same network segment.

3. Connect the Windows computer to the BMC port on the node with a LAN cable (a cross cable).

4. Execute the `ping` command from the command prompt of the Windows computer.

   If communication can be established, go to the next step. If communication cannot be established, contact maintenance personnel.

5. Open Remote Access Controller and log in.

   Open the web browser on the Windows computer and enter the following address in the address bar.

   `https://`*BMC-IP-address*

   From the login window, enter `root` for the user name, `calvin` for the password, and `This iDRAC` for the domain.

   The System Summary window is displayed.

6. Click the **Console/Media** tab to display the Virtual Console and Virtual Media window.

7. Click the **Launch Virtual Console** button to check whether the login prompt is displayed.

   If `Copy dump file start:` is displayed, wait 10 minutes, and then check whether the login prompt is displayed.

   If the login prompt is displayed, execute the `ping` command to check the network status for the ports used for system management and data access, and resolve any problems. For details on how to recover from a failure, see Using error information on the data port for error recovery on page 4-30. If there are no network problems, go to step 10.

   If there is no response, go to the next step.

8. Check the color of the LCD panel light.

   If the color is amber, contact maintenance personnel. If the color is not amber, go to the next step.

9. Press the NMI button to restart the node.

   The NMI button is located between the power indicator and the USB ports. Use a thin object such as a paper clip to press the button.

   It takes about 10 minutes to restart the node. You can check the progress from the window displayed in Step 7. After the node has restarted, the

login prompt is displayed. If the node was successfully restarted, go to the next step. If restarting fails, contact maintenance personnel.

10. Check whether clients can access the file systems on the node.

    If clients can access the file systems, the system has been successfully recovered. Ask maintenance personnel to collect dump information. If clients cannot access the file systems, contact maintenance personnel.

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

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

If communication with the import-source file server fails

If communication with the import-source file server fails, check the following items and correct the problem.

To check the status when communication with the import-source server fails:

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 the external servers such as the 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`) of the Check for Errors dialog box.

3. Check the operation status of the import-source file server, network settings, share settings (shared path settings), and I/O status. Use the **Test Connection** button in the **Import Files** dialog box or the `datamigrateaccesstest` command to check whether you can access the import-source file server with the current network and share settings. Also check the import status and I/O status from the file server console.

4. Check the host name, IP address, share name, account, and shared path that were specified when the import was performed. Use the **Import Files** dialog box or the `datamigrateconflist` command to check whether the settings are correct. Also, use the **Test Connection** button in the **Import Files** dialog box or the `datamigrateaccesstest` command to check whether you can access the import-source file server with the current settings.

If an I/O failure occurs in the HDI system

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

Table 4-1 Action to take according to the output message, if an I/O failure occurs in the HDI system during a data import from another file server

Message content	Action	See
Insufficient capacity in the file system	Delete unnecessary files or expand the file system to obtain enough capacity in the file system.	N/A
FC path failure	Follow the recovery procedure for FC path failures.	Recovering from FC path errors on page 4-24
File system failure	Follow the recovery procedure for when a file system is blocked.	Recovering from file system errors on page 4-3
Note: N/A = Not applicable.		

If the importing of some files fails

After a data import, use the **Import Files** window or specify the `--migfailedlist` option and then execute the `datamigratestatus` command to check the results of the import. If you notice that some files failed to be imported, resolve the problem by taking action according to the error message. After resolving the problem, start the import procedure again by using the **Import Files** window or executing the `datamigratestart` command. If some files fail 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 4-35 or If the account mapping is not set up on page 4-36:

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 (excluding `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. Use the **Import Files** window or the `datamigratestart` command to perform the import procedure again.

If the above steps do not work, execute the `arcconfedit` command with the `--migrate-replace-owner` option to set the account name to be assigned to the deleted accounts. Then perform the import procedure again by using the **Import Files** window or 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.

    ```
    [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. Use the **Import Files** window or the `datamigratestart` command to perform the import procedure again.

If the above steps do not work, execute the `arcconfedit` command with the `--migrate-replace-owner` option to set the account name to be assigned to the deleted accounts. Then perform the import procedure again by using the **Import Files** window or 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 import settings are deleted before an import finishes

If you use the GUI or the `datamigrateconfdel` command to delete the import settings before all files are imported, an access from a client to a file that was not imported causes an access error. If you need the file, perform the import procedure again. If you do not need the file, use the **Import Files** window to resume the importing of the target task, and then select **Change to On-Demand Import** to change the import method, and then delete the file. Alternatively, execute the `datamigrateconfadd` command, execute the `datamigratestart` command with the `--type on-demand` option, 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, use the **Import Files** window or the `datamigrateconflist` command to make sure that the mapping is correct. If the mapping is not set, use the **Import Files** window to edit the task settings or use the `datamigrateconfedit` command to set the mapping. After setting the mapping, continue the import procedure.

If multibyte characters are included in an account name

If the account name of the import source includes multibyte characters, change the import-target-account name (`DST_NAME`) of the target account to a name without multibyte characters, based on the information that was output from the mapping generation tool (`sidlist.exe`). After that, register the account to the HDI system or an external server. Then use the **Import Files** window to edit the task settings or use the `datamigrateconfedit` command to reset the mapping. After resetting the mapping, continue the import procedure.

Recovering from a Backup Restore functionality failure

This section describes what actions the system administrator takes when an error occurs while the Backup Restore functionality is being used. If you have identified what caused the error from the error messages, check the required recovery procedure, and then take appropriate action to remedy the error.

If the cause of an error can be identified by an error message, confirm what action is appropriate, and then remove the cause of the error.

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.

- Review the contents of the `/etc/hosts` file, and then correct the information set for the registered backup server.
- Check the NDMP server log (`/enas/log/ndmpserver.log`), and then take appropriate action according to the output messages.

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.

Recovering from a failure that occurred in an HDI system linked with an HCP system

If power to an HDI system is turned off or lost, the management information for the file system might become incomplete. After starting the HDI system, execute the arccorrection command to restore the management information.

In addition, if an HDI system shares data with other HDI systems via a linked HCP system, the file systems of the other HDI systems with which the data is shared might become incomplete. This problem occurs if power to an HDI system that is migrating data to the HCP system is turned off or lost, or if a failure occurs in the file system. After starting the HDI system or recovering the file system from the failure, execute the arcrestore command to restore the file systems on all the HDI systems that share the namespace of the same HCP system.

A

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

☐ The enas_routelist.log file

☐ The log_ifconfig file

☐ The log_interfaces_check 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
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 A-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.

```
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 A-2 Information that is output to the log_ifconfig file

Output item	Output contents
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 an IP address. One of the following values is output for *alias-number*: 0 This is output for an IP address on the node where log_ifconfig is output.
Link encap	Outputs the type of the link media.
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.

Output item	Output contents
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.

The log_interfaces_check file

The following table lists and describes the information that is output to the log_interfaces_check file.

Table A-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 A-4 Information that is output as the status of the connection with the DNS server on page A-6
Checking NIS configuration...	Outputs the status of the connection with the NIS server.	Table A-5 Information that is output as the status of the connection with the NIS server on page A-7
Checking NTP configuration...	Outputs the status of the connection with the NTP server.	Table A-6 Information that is output as the status of the connection with the NTP server on page A-7
Checking LDAP configuration (for user authentication)...	Outputs the status of the connection with the LDAP server used for user authentication.	Table A-7 Information that is output as the status of the connection with the LDAP server used for user authentication on page A-8
Checking authentication server configuration (for CIFS)...	Outputs the status of the connection with the authentication server for CIFS clients.	Table A-8 Information that is output as the status of the connection with the authentication server for CIFS clients on page A-9
Checking authentication	Outputs the status of the connection with the	Table A-9 Information that is output as the status of the

Messages	Description	See
`server configuration (for NFS)...`	authentication server for NFS clients.	connection with the authentication server for NFS clients on page A-10
`Checking LDAP configuration (for user mapping)...`	Outputs the status of the connection with the LDAP server used for user mapping.	Table A-10 Information that is output as the status of the connection with the LDAP server used for user mapping on page A-11

> ⚠️ **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 A-4 Information that is output as the status of the connection with the DNS server on page A-6 to Table A-10 Information that is output as the status of the connection with the LDAP server used for user mapping on page A-11).

Table A-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.
`unusing DNS`	A DNS server has not been specified.	To use the DNS server, specify DNS server information on the **DNS, NIS, LDAP Setup** page in the Network & System Configuration dialog box.
`Warning: DNS server does not respond.` `No respond servers:` *IP-address-of-DNS-server-specified-in-HDI*	The specified DNS server does not respond.	Make sure of the following: • Devices on the path between a node and the DNS server to be used are working normally. • The IP address of the specified DNS server is correct. • The DNS server is working normally.
`Error: cannot access DNS server.` *cause-of-error*	Another error has occurred.	Contact maintenance personnel.

Table A-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 on the **DNS, NIS, LDAP Setup** page in the Network & System Configuration dialog box.
Warning: NIS server does not respond. No respond servers: *name-or-IP-address-of-NIS-server-specified-in-HDI*[#]	The specified NIS server does not respond.	Make sure of the following: • Devices on the path between a node and the NIS server to be used are working normally. • The name or IP address of the specified NIS server is correct. • The NIS server is working normally.
Warning: The specified NIS server name cannot be resolved. NIS server name: *name-of-NIS-server-specified-in-HDI*	Resolving the name of the specified NIS server 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-NIS-server-specified-in-HDI*	The specified NIS domain name is incorrect.	Make sure that the NIS domain name is correctly specified on the **DNS, NIS, LDAP Setup** page in the Network & System Configuration dialog box.
Error: cannot access NIS server. *cause-of-error*	Another error has occurred.	Contact maintenance personnel.
#: When the broadcast is used, `Broadcast` is output.		

Table A-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 you want to use an NTP server, specify the NTP server settings on the **Time**

Output contents	Description	Action
		Setup page in the Network & System Configuration dialog box.
`Warning: NTP server does not respond.` `No respond servers:` *name-or-IP-address-of-NTP-server-specified-in-HDI*	The specified NTP server does not respond.	Make sure of the following: • Devices on the path between a node and the NTP server to be used are working normally. • The name or IP address of the specified NTP server is correct. • The NTP server is working normally.
`Warning: The specified NTP server name cannot be resolved.` `NTP server name:` *name-of-NTP-server-specified-in-HDI*	Resolution of the name of the specified NTP server failed.	Make sure that the name of the NTP server can be correctly resolved.
`Error: cannot access NTP server.` *cause-of-error*	Another error has occurred.	Contact maintenance personnel.

Table A-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 on the **DNS, NIS, LDAP Setup** in the Network & System Configuration dialog box.
`Error: LDAP server(`*IP-address-of-LDAP-server-specified-in-HDI*`:`*port-number*`) has not been connected.`	The specified LDAP server does not respond.	Make sure of the following: • Devices on the path between a node and the LDAP server to be used are working normally. • The name or IP address of the specified LDAP server is correct. • The LDAP server is working normally.

Output contents	Description	Action
`Warning: LDAP server(`*IP-address-of-LDAP-server-specified-in-HDI*`:`*port-number*`) has been connected, but the time limitation occurred.`	A timeout occurred while checking the connection between a node and the specified LDAP server.	On the **DNS, NIS, LDAP Setup** page in the Network & System Configuration dialog box, make sure that the LDAP server information is specified correctly.
`Warning: LDAP server(`*IP-address-of-LDAP-server-specified-in-HDI*`:`*port-number*`) has been connected, but the size limitation occurred.`	The number of entries that can be acquired from the specified LDAP server 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 on the **DNS, NIS, LDAP Setup** page of the Network & System Configuration dialog box. In addition, 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 specified LDAP server administrator is incorrect	Check whether the password of the LDAP server administrator has been specified correctly.
`Error: /etc/libnss-ldap.conf is not found.`	The configuration definition file for the LDAP server does not exist. There might be a problem with the node OS.	Contact maintenance personnel.

Table A-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`	Local authentication is used. NT domain authentication and Active Directory authentication are not used.	If you use NT domain authentication or Active Directory authentication, specify information about the server to be used on the **CIFS Service Management** page (**Setting Type**: `Basic`) in the Access Protocol Configuration dialog box.
`Error: rpc error.` `Server: `*name-of-authentication-server-specified-in-HDI*	The authentication server for specified CIFS clients does not respond.	Make sure of the following: • Devices on the path between a node and the authentication server for CIFS clients to be used are working normally.

Output contents	Description	Action
		• The name or IP address of the authentication server for specified CIFS clients is correct. • The authentication server for CIFS clients is working normally.
`Error: timeout. Server:` *name-of-authentication-server-specified-in-HDI*	A timeout occurred while checking the connection with the authentication server for specified CIFS clients.	Make sure of the following: • 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 specified CIFS clients is correct. • The authentication server for CIFS clients is working normally.
`Error: name resolution failure. Server:` *name-of-authentication-server-specified-in-HDI*	Resolution of the name of the authentication server for CIFS clients failed.	Make sure that the name of the CIFS server can be correctly resolved.
`Error:` *cause-of-error*. `Server:` *name-of-authentication-server-specified-in-HDI*	Another error has occurred.	Contact 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 A-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 about the KDC server to be used on the **NFS Service Management** page in the Access Protocol Configuration dialog box.

Output contents	Description	Action
Error: KDC error. Server: *name-of-KDC-server-specified-in-HDI*	The specified KDC server does not respond.	Make sure of the following: • Devices on the path between a node and the KDC server to be used are working normally. • The name or IP address of the specified KDC server is correct. • The KDC server is working normally.
Error: timeout. Server: *name-of-KDC-server-specified-in-HDI*	A timeout occurred while checking the connection with the specified KDC server.	Make sure of the following: • Devices on the path between the node and the KDC server to be used are working normally. • The name or IP address of the specified KDC server is correct. • The KDC server is working normally.
Error: name resolution failure. Server: *name-of-KDC-server-specified-in-HDI*	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-error* Server: *name-of-KDC-server-specified-in-HDI*	Another error has occurred.	Contact maintenance personnel.

Table A-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 LDAP user mapping, specify the information about the LDAP server on the **CIFS Service Management** page (**Setting Type**: User mapping) in the Access Protocol Configuration dialog box.
Error: LDAP search timeout.	The specified LDAP server does not respond.	Make sure of the following:

Output contents	Description	Action
		• Devices on the path between a node and the LDAP server to be used are working normally. • The name or IP address of the specified LDAP server is correct. • The LDAP server is working normally.
`Error: LDAP server name or LDAP server port number is invalid.`	The name or port number of the specified LDAP server is incorrect, or the LDAP server has been stopped.	Make sure of the following: • Devices on the path between a node and the LDAP server to be used are working normally. • The name or IP address of the specified LDAP server is correct. • The LDAP server is working normally.
`Error: LDAP suffix is not specified.`	The LDAP server root DN has not been specified in the HDI system.	Specify the LDAP server root DN on the **CIFS Service Management** page (**Setting Type**: `User mapping`) in the Access Protocol Configuration dialog box.
`Error: LDAP administrator DN is not specified.`	The LDAP server administrator DN has not been specified in the HDI system.	Specify the LDAP server administrator DN on the **CIFS Service Management** page (**Setting Type**: `User mapping`) in the Access Protocol Configuration dialog box.
`Error: LDAP administrator password is not specified.`	The LDAP server administrator password has not been specified in the HDI system.	Specify the LDAP server administrator password on the **CIFS Service Management** page (**Setting Type**: `User mapping`) in the Access Protocol Configuration dialog box.
`Error: LDAP user map DN or LDAP server root DN is invalid.`	Either of the following DNs specified in the HDI system is incorrect: • DN used to add a user mapping account • LDAP server root DN	Make sure that each DN is correctly specified on the **CIFS Service Management** page (**Setting Type**: `User mapping`) in the Access Protocol Configuration dialog box.

Output contents	Description	Action
`Error: LDAP administrator password is invalid.`	The LDAP server administrator password specified in the HDI system is incorrect.	Check the password specified in the LDAP server, and then change the password on the **CIFS Service Management** page (**Setting Type**: `User mapping`) in 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 the HDI system is incorrect.	Make sure that the LDAP server root DN, administrator DN, and administrator password are correctly specified on the **CIFS Service Management** page (**Setting Type**: `User mapping`) in 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.	Make sure that the following are satisfied, and then restart the CIFS service: • 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 on the **CIFS Service Management** page (**Setting Type**: `User mapping`) in the 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 on the **CIFS Service Management** page (**Setting Type**: `User mapping`) in the Access

Output contents	Description	Action
		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 node OS.	Contact maintenance personnel.
`Error: open cifs.conf failed.`	The `/enas/conf/cifs.conf` file could not be opened because of a problem in the node OS.	Contact maintenance personnel.
`Error: cannot access LDAP server.` *cause-of-error*	Another error has occurred.	Contact maintenance personnel.

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 the HDI system.

☐ Before checking network communication

☐ Performing checks for each network configuration

☐ Actions to be taken when communication cannot be established

☐ Examples of checking network communication

Before checking network communication

To make sure that no hardware or link failure occurred in the network, and identify any problems in the HDI 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.

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.
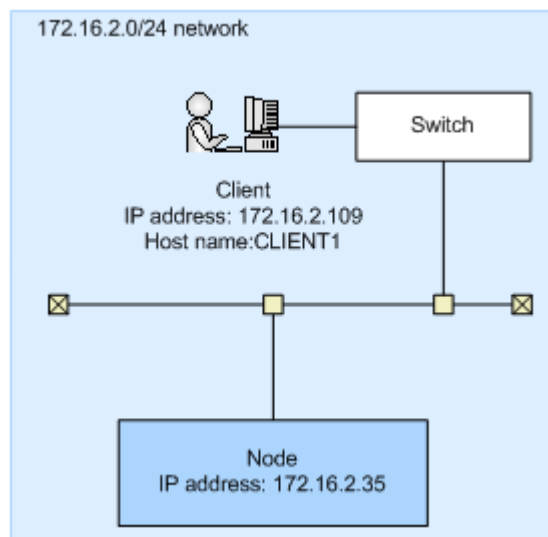
Figure B-1 Configuration example when the HDI system and the client belong to the same network

The following shows an example when the HDI system and the client belong to different networks.
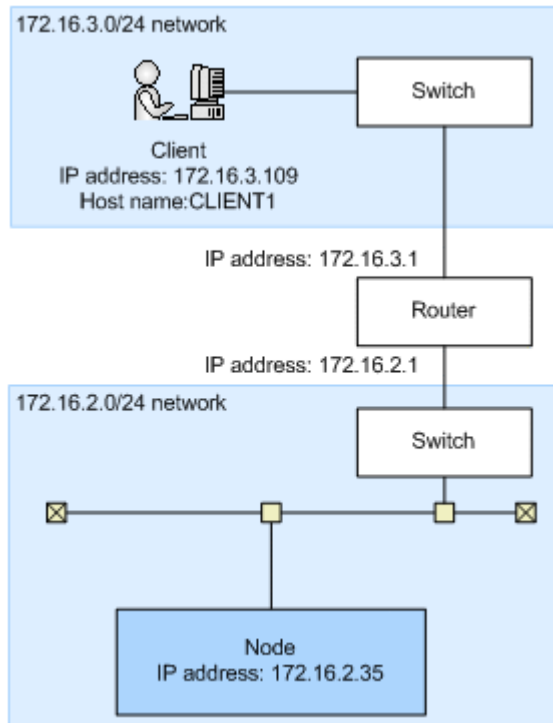
Figure B-2 Configuration example when the HDI system and the client belong to different networks

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. 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 B-4 and Checking the VLAN ID on page B-4.

2. 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 B-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 B-5.

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 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

How To Check Network Communication

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 node
- 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 .

```
$ sudo routelist
[IPv4]
Target          Netmask         Gateway         Method Type    MSS    Iface
CLIENT1         -               172.16.2.1      Allow  host    -      eth0
default         0.0.0.0         10.213.16.10    Allow  default -      mng0
```

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
[IPv4]
Target          Netmask         Gateway         Flags    MSS    Iface
172.16.3.109    255.255.255.255 172.16.2.1      UGH      -      eth0
172.16.2.0      255.255.255.0   0.0.0.0         U        -      eth0
10.0.0.0        255.255.255.0   0.0.0.0         U        -      pm0
10.213.16.0     255.255.255.0   0.0.0.0         U        -      mng0
default         0.0.0.0         10.213.16.10    UG       -      mng0

[IPv6]
Target                      Gateway             Flags Iface
::1/128                     ::                  Un    lo
fe80::210:18ff:fe75:5780/128 ::                 Un    lo
fe80::210:18ff:fe75:5780/128 ::                 Un    lo
fe80::862b:2bff:fe25:bcc7/128 ::                Un    lo
fe80::862b:2bff:fe25:bcc7/128 ::                Un    lo
fe80::/64                   ::                  U     mng0
fe80::/64                   ::                  U     mng0
fe80::/64                   ::                  U     eth0
fe80::/64                   ::                  U     eth0
ff00::/8                    ::                  U     mng0
ff00::/8                    ::                  U     mng0
ff00::/8                    ::                  U     eth0
ff00::/8                    ::                  U     eth0
::/0                        ::                  !n    lo
```

> ⚠️ **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 node is restarted while the host name cannot be resolved, the routing

How To Check Network Communication

Hitachi Data Ingestor Single Node Troubleshooting Guide

information specified by the system administrator might not be enabled on the 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
[IPv4]
Target          Netmask         Gateway         Method Type    MSS
Iface
CLIENT1         -               172.16.2.1      Allow  host    -
eth0
default         0.0.0.0         10.213.16.10    Allow  default -
mng0
```

```
$ sudo routelist -l
[IPv4]
Target          Netmask         Gateway         Flags    MSS    Iface
172.16.2.0      255.255.255.0   0.0.0.0         U        -      eth0
10.0.0.0        255.255.255.0   0.0.0.0         U        -      pm0
10.213.16.0     255.255.255.0   0.0.0.0         U        -      mng0
default         0.0.0.0         10.213.16.10    UG       -      mng0

[IPv6]
Target                   Gateway                 Flags Iface
::1/128                  ::                      Un    lo
fe80::210:18ff:fe75:5780/128 ::                     Un    lo
fe80::210:18ff:fe75:5780/128 ::                     Un    lo
fe80::862b:2bff:fe25:bcc7/128 ::                    Un    lo
fe80::862b:2bff:fe25:bcc7/128 ::                    Un    lo
fe80::/64                ::                      U     mng0
fe80::/64                ::                      U     mng0
fe80::/64                ::                      U     eth0
fe80::/64                ::                      U     eth0
ff00::/8                 ::                      U     mng0
ff00::/8                 ::                      U     mng0
ff00::/8                 ::                      U     eth0
ff00::/8                 ::                      U     eth0
::/0                     ::                      !n    lo
```

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 eth0
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 eth0
```

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
[IPv4]
Target          Netmask         Gateway         Method Type     MSS
Iface
default         0.0.0.0         10.213.16.10    Allow  default -
mng0
```

```
$ sudo routelist -l
[IPv4]
Target          Netmask         Gateway         Flags    MSS    Iface
172.16.3.109    255.255.255.255 172.16.2.1      UGH      -      eth0
172.16.2.0      255.255.255.0   0.0.0.0         U        -      eth0
10.0.0.0        255.255.255.0   0.0.0.0         U        -      pm0
10.213.16.0     255.255.255.0   0.0.0.0         U        -      mng0
default         0.0.0.0         10.213.16.10    UG       -      mng0

[IPv6]
Target                    Gateway               Flags Iface
::1/128                   ::                    Un    lo
fe80::210:18ff:fe75:5780/128 ::                 Un    lo
fe80::210:18ff:fe75:5780/128 ::                 Un    lo
fe80::862b:2bff:fe25:bcc7/128 ::                Un    lo
fe80::862b:2bff:fe25:bcc7/128 ::                Un    lo
fe80::/64                 ::                    U     mng0
fe80::/64                 ::                    U     mng0
fe80::/64                 ::                    U     eth0
fe80::/64                 ::                    U     eth0
ff00::/8                  ::                    U     mng0
ff00::/8                  ::                    U     mng0
ff00::/8                  ::                    U     eth0
ff00::/8                  ::                    U     eth0
::/0                      ::                    !n    lo
```

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 node OS.

```
$ sudo routedel -d 172.16.3.109 -g 172.16.2.1 --nochk eth0
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.

Action to be taken if there are multiple gateways connecting to external network segments:

The HDI system might be unable to respond to an ICMP redirect request from a gateway (request to change the route to another gateway). Therefore, the network must be designed so that no ICMP redirect occurs. Note that multiple gateways that connect to one or more external network segments can exist in a network segment connected to an HDI port. In such an environment, set the routing information so that an appropriate gateway is used for each of the external network addresses that the HDI system must communicate with. The following describes the corrective action:

a. Identify the gateway of the network to which the clients belong.

b. Add the gateway identified above to the routing information.

   An example of executing the command is shown below. This example assumes that the client target network is `172.16.3.0`, the gateway IP address of the network to which the clients belong is `172.16.2.1`, and the HDI interface that connects to the clients is `eth0`.

```
$ sudo routeadd -t net -d 172.16.3.0 -n 255.255.255.0 -g 172.16.2.1
eth0
```
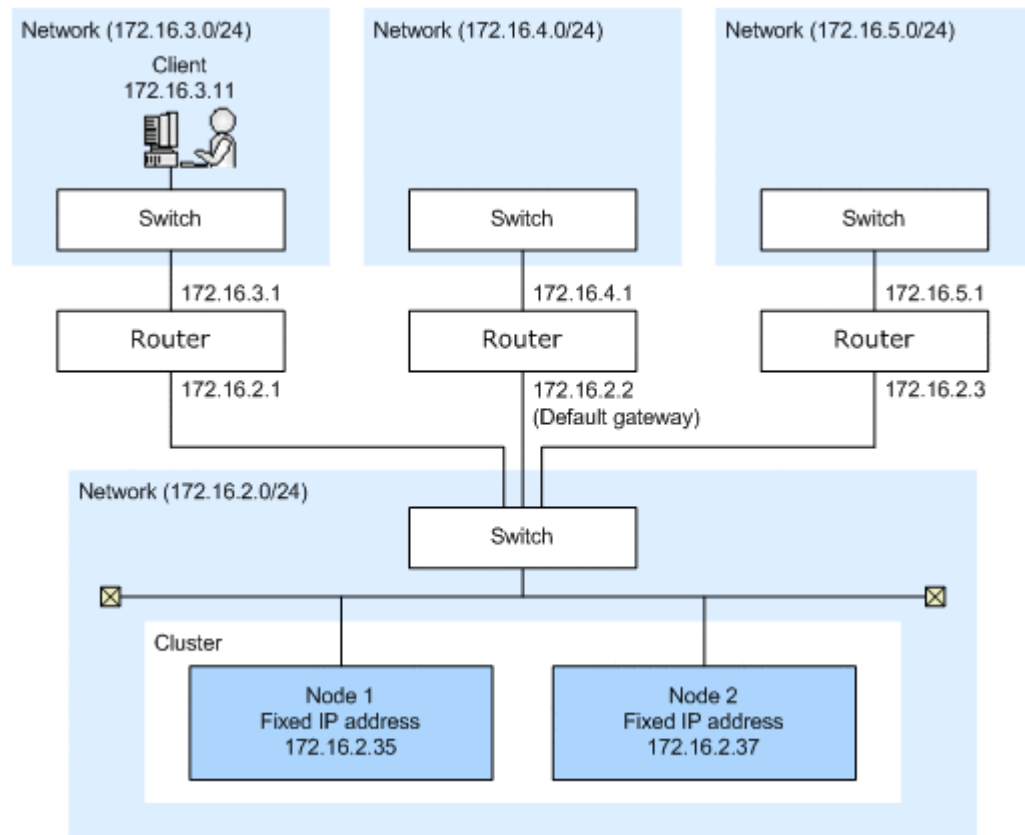
**Figure B-3 Configuration example when there are multiple
gateways connecting to external network segments**

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

How To Check Network Communication

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
10.0.0.0        0.0.0.0         255.255.255.0   U         0 0          0
pm0
192.168.0.0     0.0.0.0         255.255.255.0   U         0 0          0
eth0-br
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 output because the route to reach the specified IP address is not 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.

How To Check Network Communication

C

Troubleshooting Examples

This appendix provides troubleshooting examples.

☐ GUI-related troubleshooting examples

☐ Command-related troubleshooting examples

☐ HCP linkage troubleshooting examples

☐ Virus scan troubleshooting examples

☐ CIFS access troubleshooting examples

☐ SNMP troubleshooting examples

GUI-related troubleshooting examples

The following troubleshooting examples relate to problems that might occur during GUI operation.

Table C-1 GUI-related troubleshooting examples

Location of problem	Type of problem	Cause	Action
Non-specific	When logging into the GUI from Firefox, the window does not display correctly or login fails.	This problem is related to the window controls in Firefox, and is not due to a failure in the HDI system.	Use Internet Explorer instead, or type the IPv4 address or host name of the node in the Firefox address bar.
	Logging in to the GUI from Firefox and then clicking the **Cancel** button does not close the login window.	This problem is related to the window controls in Firefox, and is not due to a failure in the HDI system.	From the `about:config` page in Firefox, specify `true` for `dom.allow_scripts_to_close_windows`.
	The GUI is blurry.	This problem is related to the window refresh controls, and is not due to an error in the HDI system.	Close the window, and then log in to the GUI again.
	The operation cannot be performed because the GUI display does not change from the processing status.	This problem occurs for certain management console controls. The executed operation has not finished successfully because the processing request has not reach the node yet.	Log in to the GUI, and then retry the operation.
	You cannot use the GUI when you configure network information about nodes using DHCP.	Probable causes are: • The IP address has been changed because nodes were restarted or the `dhcpreload` command was executed. • No IP address has been set because a connection failure occurred with the DHCP server. • `mng0` and `eth`*number* or `xgbe`*number* might be connected to the same network.	• Specify the host name in your Web browser's address bar. • The node IP address might have been provisionally set to `169.254.1.100`, and the netmask might have been provisionally set to `255.255.0.0`. Connect the node to a computer that is configured to be able to connect to `169.254.1.100`, and then from that computer, check whether you can access the GUI by specifying the IP address

Location of problem	Type of problem	Cause	Action
			`169.254.1.100.` If you can access the GUI, the problem lies in the connection with the DHCP server. Ask the network administrator to address the problem. After the problem is resolved, restart the node. • Ask the network administrator to review and modify the network configuration. Restart the node after the network configuration is modified.
	The icon for HDI is not displayed in the network list of the management console when you use UPnP.	Probable causes are: • The HDI node is not powered on. • The management console is not configured to use UPnP. • A failure has occurred with the network where the node and the management console are connected.	Follow the procedure below to address the problem: 1. Make sure that the node is powered on. 2. Make sure that the management console is configured to use UPnP. For details about the management console settings required to use UPnP, see *Single Node Getting Started Guide*. 3. Check the operating environment of the network. Check that there is no problem with the operating environment and the configuration of the network where the node and the management console are connected. In addition, check the operating status and the connection status with the DHCP server. 4. Execute the `nasreboot` command to restart the node. If you cannot use the command, power off the node to shut down the OS, After that, power on the node again to start the OS. For details about how to start and forcibly shut down the OS, see

Location of problem	Type of problem	Cause	Action
			Single Node Administrator's Guide.
	You attempted to use UPnP, but the GUI did not start even though you clicked the HDI icon, or right-clicked the icon and then selected **View device web page**.	If the management console runs on Windows 8 or Windows Server 2012, a problem might occur if the https communication stops between the HDI node and the management console.	Click the address displayed in **Device webpage** in the properties dialog box for the HDI icon.
System Configuration Wizard	After the System Configuration Wizard is executed, the screen is not displayed again for a long time.	An error might have occurred when the IP address used for system management was being changed.	Log in again by using the IP address before the change, check the entered values, and then retry the operation. If the screen is not displayed when you use the IP address before the change, contact maintenance personnel.
	The System Configuration Wizard is executed and you log in again, but the settings are not applied.	An error might have occurred when the System Configuration Wizard was being executed.	Check the entered values, and then retry the operation.

Command-related troubleshooting examples

The following troubleshooting examples relate to problems that might occur during command operations.

Table C-2 Command-related troubleshooting examples

Problem	Cause	Action
You cannot log in to the node when the network information about the node is configured using DHCP.	Probable causes are: • The IP address has been changed because nodes were restarted or the `dhcpreload` command was executed. • No IP address has been set because a connection failure occurred with the DHCP server.	• Specify the host name to log in to the node. • The node IP address might have been provisionally set to `169.254.1.100`, and the netmask might have been provisionally set to `255.255.0.0`. Connect the node to a computer that is configured to be able to connect to `169.254.1.100`,

Problem	Cause	Action
	• `mng0` and `eth`*number* or `xgbe`*number* might be connected to the same network.	and then from that computer, check whether you can log in to the node using the IP address `169.254.1.100`. If you can log in, the problem lies in the connection with the DHCP server. Ask the network administrator to address the problem. After the problem is resolved, restart the node. • Ask the network administrator to review and modify the network configuration. Restart the node after the network configuration is modified.

HCP linkage troubleshooting examples

The following troubleshooting examples relate to problems that might occur with HCP linkage.

Table C-3 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. • The namespace might not exist. Check with the HCP administrator whether the namespace exists.
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

Problem	Cause and action
	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.
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 and the importing of the files is changed to on-demand mode. The importing of the files 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 the past version 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.

Problem	Cause and action
	• 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 **Service Configuration Wizard**, on the **2. 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. • If a file is updated during an attempt to migrate it, the migration of the file will fail unless the Active File Migration function is used. The file will be migrated the next time a migration occurs. Check whether your file was updated during an attempt to migrate it. If you want to migrate files that are updated during attempts to migrate them, you must use the `arcactmigctl` command to enable use of the Active File Migration function.
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.

Problem	Cause and action
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.

Virus scan troubleshooting examples

The following troubleshooting examples relate to problems that might occur when using the real-time scan function.

Table C-4 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 setup on the scan server finishes, enable the real-time scan again in the HDI system and restart the CIFS service.
`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 C-5 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 *Single Node Administrator's Guide*.
	A timeout often occurs during CIFS client authentication due to processing that establishes a connection from HDI to domain controllers.	CIFS client authentication processing might be delayed because a domain controller in the domain cannot communicate with HDI. On the **List of RAS Information** page (displaying **List of other log files**), examine `/var/log/cifs/log.winbindd` and check whether any domain controller in the domain cannot communicate with HDI. For details about messages that are output to log.winbindd and actions to be taken, see the *File System Protocols (CIFS/NFS) Administrator's Guide*. If this does not resolve the problem, check the host names (in FQDN format) of domain controllers output to `cifstrustinfo.log` (between `Find DNS domain server` and `ENDofTrustDomainInfo`), and then confirm that those domain controllers are able to communicate with HDI. You can obtain the `cifstrustinfo.log` data by downloading the log file of the OS log group on the **List of RAS Information** page (displaying **Batch-download**), and then unzipping `cifslog.tar.gz`. If a domain controller that cannot communicate is found, obtain the IP address corresponding to the FQDN host name of that domain controller by using, for example, the nasping

Location of problem	Type of problem	Cause and action
		command. Then, use the `cifsoptset` command to suppress communication to that domain controller.

SNMP troubleshooting examples

The following troubleshooting examples relate to problems that might occur when SNMP is used.

Table C-6 SNMP troubleshooting examples

Problem	Measures
Traps for reporting failures are not sent to the SNMP manager.	In the **Check for Errors** dialog box, on the **List of RAS Information** page (for `List of other log files`), check whether the message shown in Table C-7 Content output to the SNMP agent log (/var/log/snmpd.log) on page C-10 was output, and then perform the necessary actions.
	If the message shown in Table C-7 Content output to the SNMP agent log (/var/log/snmpd.log) on page C-10 has not been output, check the following regarding the settings of the `snmpd.conf` file and the SNMP manager:
	• If `trap2sink` is specified in the trap notification settings, make sure the community name specified in `trap2sink` matches the community name specified on the SNMP manager.
	• If `trapsess` is specified in the trap notification settings, make sure the user name, authentication type, authentication password, encryption type, and encryption password that were specified in `trapsess` match the values specified on the SNMP manager.
	• In the firewall setting of the SNMP manager, the access from the HDI node has not been blocked.

Table C-7 Content output to the SNMP agent log (/var/log/snmpd.log)

Message	Cause	Measures
`trap2sink syntax error` *`maintenance-information.`* `line=`*`line-number-where-errors-were-detected-in-snmpd.conf`*	There is a syntax error in the line corresponding to the `trap2sink` setting as indicated by *line-number-where-errors-were-detected-in-snmpd.conf*.	Refer to the description about the `trap2sink` setting in the *Single Node Administrator's Guide* and then revise the setting.
	Verify the following:	
	• Make sure there is no excess or deficiency in the `trap2sink` settings.	
	• Make sure the specified community name, SNMP manager host name or	

Message	Cause	Measures
	IP address , and port number are correct.	
`trapsess syntax error` *`maintenance-information.`* `line=`*`line-number-where-errors-were-detected-in-snmpd.conf`*	There is a syntax error in the line corresponding to the `trapsess` setting as indicated by *line-number-where-errors-were-detected-in-snmpd.conf*. Verify the following: • Make sure there is no excess or deficiency in the `trapsess` settings. • Make sure the specified user name, SNMP manager host name or IP address, and port number are correct.	Refer to the description about the `trapsess` setting in the *Single Node Administrator's Guide* and then revise the setting.
`Error: passphrase chosen is below the length requirements of the USM`	In the line corresponding to the `trapsess` or `createUser` setting, the value set for the authentication password or encryption password consists of 7 or fewer characters.	For `trapsess` or `createUser`, specify values for the authentication password and encryption password that consist of 8 or more characters.
`/etc/snmp/snmpd.conf:` `line` *`line-number-where-errors-were-detected-in-snmpd.conf`*`: Error:` *`item-for-which-errors-were-detected`*	There is a syntax error in the line corresponding to the `rouser`, `rwuser`, or `createUser` setting as indicated by *line-number-where-errors-were-detected-in-snmpd.conf*. Verify the following: • Make sure the user name, security level, and OID specified for `rouser` or `rwuser` are correct. • Make sure the user name, authentication type, authentication password, encryption type, and encryption password specified for `createUser` are correct.	Refer to the descriptions about the `rouser`, `rwuser`, and `createUser` settings in the *Single Node Administrator's Guide* and then revise the settings.
`fail to send Trap`	In the line corresponding to the `trap2sink` or `trapsess` setting, there might be an error in the value specified for the SNMP manager host name or IP address.	Make sure the SNMP manager host name or IP address that was specified for `trap2sink` or `trapsess` is correct. If it is correct, verify the following:

Message	Cause	Measures
		• If the host name is specified, make sure there are no problems related to name resolution. • Make sure there are no problems in the connection between the node and the SNMP manager.

`get error EngineID`
 	
`invalid Trap type TYPE=XX`
 	
`too few arguments`
	An internal error occurred.	Obtain all log data and then contact maintenance personnel.

Hitachi Vantara