HITACHI
Inspire the Next

Hitachi Data Ingestor

6.2

Remote Server Administrator Guide (Locally Managed HDI RS)

This guide is for Hitachi Data Ingestor (HDI) administrators who are responsible for managing HDI remote servers (RS) locally. This guide describes all the information administrators should know in order to install, set up, administrer, troubleshoot, and replace a locally managed HDI RS.

MK-90HDI054-02
October 2017

Contents

Preface

Hitachi, Ltd. owns the copyrights of this guide. No part of this guide may be reused or reproduced without permission of Hitachi, Ltd.
HDI Remote Server falls into HDI-RS LM (Locally Managed HDI Remote Server) that does not cooperate with HCP Anywhere and HDI-RS CM (Centrally Managed HDI Remote Server) that cooperate with HCP Anywhere.
When managing the Locally Managed HDI Remote Server system, read this guide carefully, and fully understand the operation procedure and instructions before starting the work.

HDI Remote Server described in this guide

This guide describes the HDI-RS LM (Locally Managed HDI Remote Server).
To clarify whether the system is HDI-RS LM, use "prsstatus" command that display "Locally Managed" as the result.
For the detail of "prsstatus" command, refer to Chapter12 "Command to distinguish the operation form (prsstatus)".
If prsstatus command display "Centrally Managed", the system is HDI-RS CM. The system is managed by HCP Anywhere Administrator and this guide does not describe the management about it.

Role and job description in this guide

Role names and each job description shown in this document are as follows.

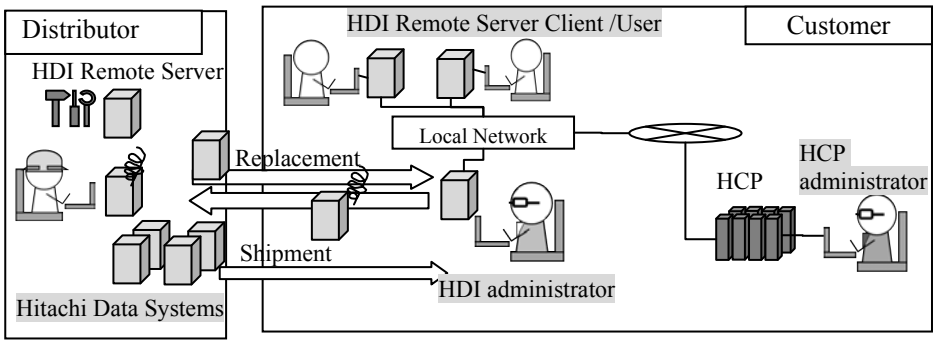


Figure 1. Image of each administrator

Table 1. Job Description of Each Person in Figure 1

#	Role name	Description
1	Hitachi Data Systems	Distributor who assembles and ships HDI Remote Server.
2	HDI administrator	Administrator who refers to this guide. Administrates Locally HDI Remote Server. They manage the HDI Remote Server information. To execute the initial settings, the troubleshoot, the replacement of HDI Remote Server LM. They also manage the network server in the client/user environment if required.
3	HCP administrator	They manage the HCP totally.
4	HDI Remote Server Client/User	HDI Remote Server user who reside in each location.

Chapter 1. *Flow of introducing HDI Remote Server*

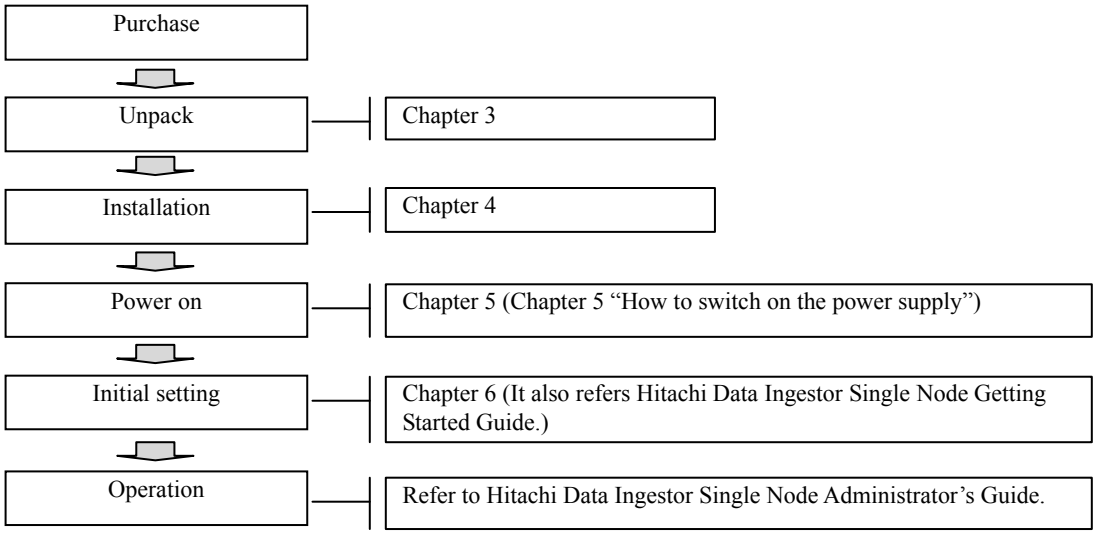


Figure 1-1. Flow of Introduction

Chapter 2. *Information for your safety and comfort*

Precautions for Using the HDI Remote Server

- For this product, use a set of power supply cords included in this product. Do not use a set of power supply cords included in this product for other products. Otherwise, unexpected failures or accidents may be caused.
- If you take notice of unusual smell, abnormal heat generation, or smoke emission, shut off the power feed to the equipment and inform the maintenance engineer of it. Leaving such conditions unattended will cause an electric shock or fire.
- Do not give any shock to the equipment and parts by dropping or hitting them against something, otherwise it will cause an electric shock, fire, an injury, or failure.
- Do not get on the equipment instead of a footstool. Avoid using the equipment for any use other than its original purpose.

  Otherwise, an injury or failure will be caused.
- Putting a heavy material on the equipment will result in an injury or failure due to falling.

  Do not put any heavy material on the equipment. Further, the HDI Remote Server may not operate normally.
- Do not put a vessel with water or a tiny metallic article such as a paper clip on the HDI Remote Server. If the water or the article falls into the HDI Remote Server and the HDI Remote Server is used leaving it as it is, an electric shock, an emission of smoke, or a fire can be caused.
- Route cables so that they do not catch your feet.

  If your feet are caught by cables and you fall over, this can cause personal injury.
- Do not put any heavy material on cable. Do not put cables near any apparatus that generates heat. The cable coating will break, resulting in an electric shock, fire, or failure.
- Do not use the HDI Remote Server in a moist or dusty place. An electric shock or a fire may be caused because the insulation will be deteriorated.
- Make sure that no foreign particles are stuck on the power plug and then insert it securely to its root.

  Remove such foreign particles if they are found because they will cause a fire. Improper insertion will cause an unexpected plug slip-out, resulting in a loss of important data.
- Cool air is taken in from the air vent on the front of the HDI Remote Server and exhaust air is expelled from the vent on the rear to prevent the temperature from rising inside the HDI Remote Server. If the vents are blocked by placing any object in front of or against the vents, the temperature will rise inside the HDI Remote Server, resulting in an electric shock or fire.
- Do not put any metallic material such as clip or any combustible material such as paper into the equipment from the air vent. It will cause an electric shock or fire.
- When a failure occurs in the HDI Remote Server, take action according to this guide so as to prevent personal injury. If the trouble does not correspond to any corrective measure written in this guide, inform the provider of it.
- This product is designed and produced aimed at general office work use. In the high reliability system to influence life and property remarkably, this product cannot be used and is not guaranteed. The example of the high reliability system that is inappropriate to use this product is chemical plant control, medical equipment control, and the urgency communication control.

Chapter 3. *Package Contents and Getting to Start*

When the HDI Remote Server arrived at the HDI administrator`s site, open the box and start to introduce and set the system referring to Hitachi Data Ingestor Single Node Getting Started Guide.

Chapter 4. *Installation*

Installation place

Regarding the conditions for installation environment, refer to the section Chapter12 “Conditions for installation environment” to install HDI Remote Server. After the installation, proceed to the Chapter4 “For connecting cable”.

For connecting cable

Connecting cable - Basic Configuration

The system configuration in this document is described based on using the HCP, AD / DC servers, UPnP control point, DHCP server and DNS server. Build the environment referring to the figure shown below.

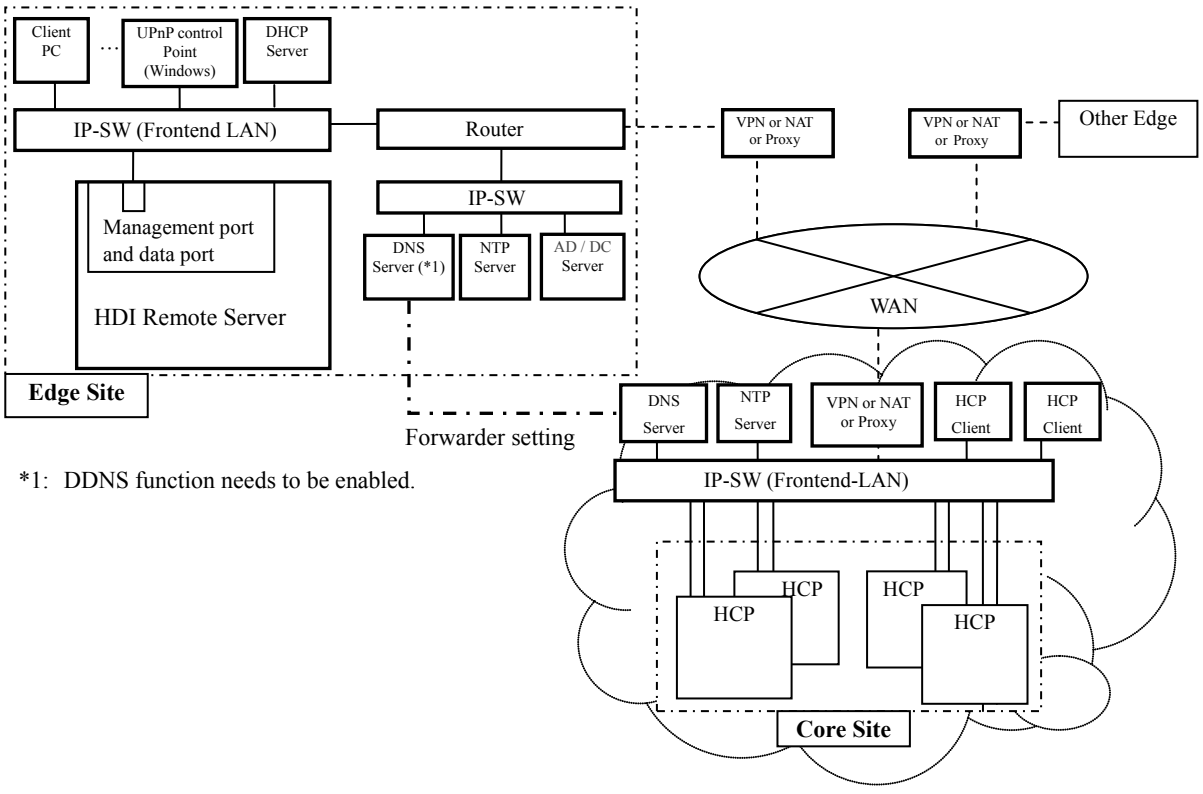
Note that the Edge Site and Core Site are linked through WAN.

DNS server, AD/DC server and NTP server can also be built in one machine. In this case, install the servers in a place reachable from HDI Remote Server. Also, the DNS server should enable the DDNS function.

Set the NTP server to synchronize the clocks of all devices at the both Edge Site and the Core Site.

For the DNS server at the Edge Site, the forwarder setting is required for the DNS server at the Core Site. By setting the forwarder, communication to HCP is resumed even HDI Remote Server address was changed dynamically or a node of HCP has failed over due to the failure, as soon as the DNS server is updated.

Tag VLAN cannot be set for IP-SW (Frontend LAN) though, a port VLAN can be set.



*1: DDNS function needs to be enabled.

Figure 4-1 Example of Network Configuration

Connecting cable - Connecting each cable

For the connecting location, refer to the rear view of Hitachi Data Ingestor Single Node Getting Started Guide.

(1) Connect between HDI Remote Server and the power cable.

(2) Connect IP-SW and HDI Remote Server using a LAN cable.

Connecting cable - LAN Interface specifications

Before the setting of IP address, choose either setting through DHCP or setting unchanging IP address in advance. For the negotiation mode and MTU, see below.

Correct settings between devices which connect to the HDI Remote Server are required. For the settings of IP-SW to be connected, refer to the table shown below.

Table 4-2 LAN Interface Setting

Port	IP address		Negotiation mode	MTU
	IPv4	IPv6		
Management port and data port	ヽ (mandatory)	ヽ	Auto Negotiation	1500
ヽ=Supported, (LinkAggregation and Link Alternation are not supported.)				

【Notes on changing IP address setting】

Note the followings when setting the IP address, subnet mask, and default gateway:

(i) In case of IPv4, set IP addresses that do not begin with 0, 127, or 255. 0.xxx.xxx.xxx, 127.xxx.xxx.xxx, 255.xxx.xxx.xxx cannot be set.

(ii) By the IPv6 address of the Management port, the link local unicast address (fe80::/10) and the multicast address (ff00::/8) cannot be set.

Connecting cable - Port to be used

The following services are running to provide various types of services.
Setting the following port numbers so that HDI Remote Server and HCP can communicate each other is required.

Table 4-3 Ports Used by a Node (1/2)

Port number	Protocol	Service name	Description	Direction of transmitting and receiving data. ("RS→" means HDI Remote Server transmit a request. "→RS" means HDI Remote Server receives a request.)		
				HDI RS and HCP	HDI RS and peripheral server (AD/DC/DNS/NTP, etc. (Core Site side))	HDI RS and User`s PC
20	tcp	ftp	ftp-data port		→RS	
21	tcp	ftp	Used for ftp		→RS	
22	tcp	ssh	Used for ssh		→RS	
22	tcp	sshd	Used for sftp. Also used as a data port.		→RS	
25	tcp	SMTP	Use for E-mail Alert. (This number is default, and cam be set any value)		RS→	
53	udp	DNS	Used for DNS		RS→	
68	udp	DHCP	Used for DHCP		RS→ →RS	
69	udp	tftp	Used for tftp.		→RS	
80	tcp	HCP	Data migration to HCP	RS→		
88	udp/tcp	kdc	Used for user authentication in an Active Directory environment		RS→	
111	udp/tcp	portmap	Used to manage the port numbers used by NFS-related services, and respond to inquiry from clients about port numbers		RS→	→RS
123	udp	ntp	Used for NTP		RS→	
137	udp	NetBIOS Name Service	Used for the CIFS service via NetBIOS over TCP/IP		RS→ →RS	
138	udp	NetBIOS Datagram Service	Used for the CIFS service via NetBIOS over TCP/IP		RS→ →RS	
139	tcp	NetBIOS Session Service	Used for the CIFS service (Used for the communication with domain controller.) via NetBIOS over TCP/IP.		RS→ →RS	→RS
161	udp	SNMP	Used for SNMP		→RS	
162	udp	SNMP trap	Used for SNMP (This number is default, and cam be set any value)		RS→	
199	tcp	SNMP Unix Multiplexer	Used for SNMP		RS→	
389	tcp	LDAP	Used for the following 2 services. - User mapping through the external LDAP. - LDAP authentication *: in case of using a port number other than the default setting (389), a port number can be specified from the management GUI.		RS→	
389	udp	connectionless ldap	Used to check whether the DC server is alive or acquire DC information		RS→	
443	tcp	https	Used for connection between the management server and the management console	RS→		→RS
443	tcp	HCP	Data migration to HCP	RS→		

Table 4-3 Ports Used by a Node (2/2)

Port number	Protocol	Service name	Description	Direction of transmitting and receiving data. ("RS→" means HDI Remote Server transmit a request. "→RS" means HDI Remote Server receives a request.)		
				HDI RS and HCP	HDI RS and peripheral server (AD/DC/DNS/NTP, etc. (Core Site side))	HDI RS and User`s PC
445	tcp	Direct Hosting of SMB	Used for the CIFS service via Direct Hosting of SMB		RS→ →RS	→RS
464	udp/tcp	kpasswd	Used to join in a domain or change the user password in an Active Directory environment		RS→	
514	udp	syslog	Used when SYSLOG is sent to other server.		RS→	
750	tcp	kerberos4	Used for user authentication in an Active Directory environment		RS→	
600～1023	tcp	NIS	Used for NIS		RS→	
1900	udp	UPnP	Used for UPnP		RS→	RS→ →RS
2049	udp	nfsd	Used for file shares by NFS			→RS
4045	udp/tcp	lockd	Used for region locks on file shares by NFS			→RS
665～1023, 32768～61000	udp/tcp	lockd	Used for region lock shared by NFS, at the time of the NFS port dynamic allocation.			→RS
1024～65534	tcp	ftp	ftp-data port (in the case of passive mode)		→RS	
1024～65535	tcp	nasavd, smbd	Used for communication with virus scan server. (The default valued of the port depends on the scan server.)		RS→	
9090	tcp	Management API	Receiving port for Management API	→RS		
9090	tcp	HCP	Used for MAPI access to HCP	RS→		
10000	tcp	ndmp	Used for NDMP		RS→	
20048	udp/tcp	rpc.mountd	Used for file shared by NFS, at the time of the NFS port is fixed.			→RS
20997	udp/tcp	rpc.statd	Used for region lock shared by NFS, at the NFS port is fixed.			→RS
22550	tcp	hfrrdmn	Used for Hitachi File Remote Replicator			RS→
32768～61000	udp/tcp	mountd	Used for file shared by NFS, at the time of the NFS port dynamic allocation.			→RS
32768～61000	udp/tcp	statd	Used for region lock shared by NFS, at the time of the NFS port dynamic allocation.			→RS

Table 4-4 Ports Used by the administrative terminal (Web browser)

Port number	Protocol	Service name	Description	Direction of transmitting and receiving data ("RS→" means HDI Remote Server transmit a request. "→RS" means HDI Remote Server receives a request.)		
				HDI RS and HCP	HDI RS and peripheral server (AD/DC/DNS/NTP, etc. (CoreSite side))	HDI RS and User`s PC
443	tcp	https	Used to connect to HDI Remote Server.			→RS
1900	udp	UPnP	Used for UPnP			
20265	tcp	Manager Agent	Used for authentication by using the account/password generated by the temporary-account login function during access to the GUI			→RS

Chapter 5. *Operation of Power Supply*

・How to switch on the power supply

・How to switch off the power supply

・How to switch off the power forcibly

How to switch on the power supply

(1) Check that the power cable is connected.

(2) Check the location of the power switch referring to Hitachi Data Ingestor Single Node Getting Started Guide.

(3) After confirming that power of each server is switched on referring to the Chapter 6 “Confirmation points before initial setting” of this document, press the power switch.

(4) Confirm that the power LED is on.

 **Tip:** If the power is not turned on, see FAQ.

How to switch off the power

(1) Press the power switch.

(2) Confirm that the power LED is off.

 **Tip:** If the power is not turned off, try to switch off the power forcibly.

How to switch off the power forcibly

Press and hold the power switch to turn off.

Confirm that the power LED is off.

Chapter 6. *Initial Setting*

To perform the initial setting, take the following procedure.

・Confirmation points before initial setting.

・Executing the initial settings

・Updating software

Confirmation points before initial setting

- In case of using the DHCP server, confirm that the DHCP server is booted and the settings have also been completed.
- In case of using the DHCP server, confirm that the DNS server is booted and the settings have also been completed.
- In case of using the DHCP server, an administrative terminal which is corresponding to UPnP is required. Confirm that the administrative terminal is corresponding to UPnP as well as the function is enabled.
- Confirm to the HCP administrator that the power of HCP which manage the data of using HDI Remote Server is switched on.
- Confirm that the network environment of HDI Remote Server and HCP which manages the data of HDI Remote Server is prepared to connect.
- Confirm that you get the license DVD at hand. If the management PC does not have DVD drive, prepare the external DVD drive.

Performing initial setting

For the initial setting, refer to Hitachi Data Ingestor Single Node Getting Started Guide.

At the time of the initial installation and after the node replacement, HDI administrator performs the settings that include license settings using System Configuration Wizard and Service Configuration Wizard.

Initial IP address and netmask of the node is “169.254.1.100”, and “255.255.0.0” in the case that user does not use DHCP or the node could not access to DHCP server.

After the initial setting, HDI administrator should determine whether software update is necessary. If necessary, update the software.

Updating software

HDI administrator logs into management GUI and select “Software Update” from [Resources] tub to update the software (-> see the Chapter 10 “Updating software according to the request from a distributor”).

Chapter 7. *Overview and Basic Functions of HDI Remote Server*

General overview

General overview - Data flow (Read/Write processing of client)

File read/write is performed for the internal HDD by the read/write requests from the client to the node.

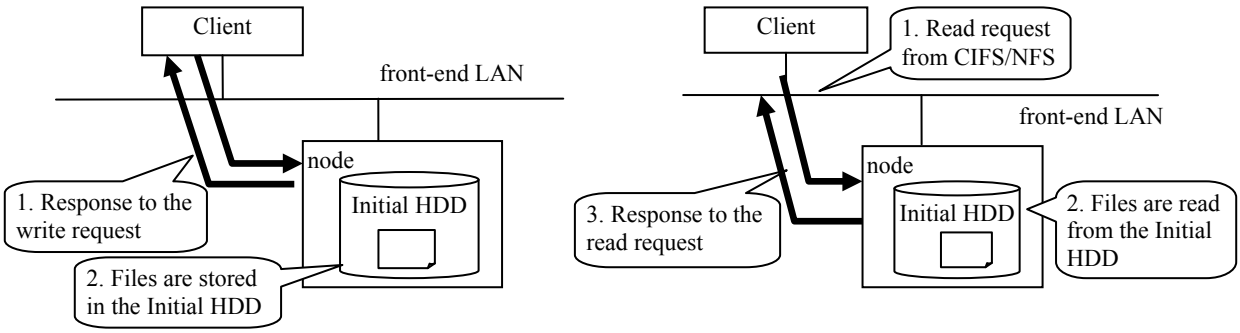


Figure 7.1-1 Flow of Write (left) / Read (right) Processing

General overview - RAID configuration

Automatically determines the number of HDDs and configure RAID. In case of the 2 HDDs, RAID configuration will be RAID1, and in case of the 4 HDDs, RAID configuration will be RAID5.

An image of the LU configurations is as follows.

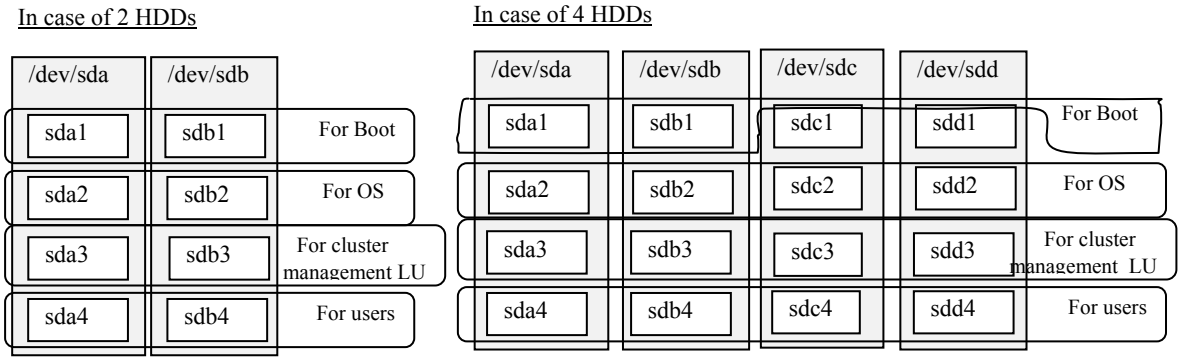


Figure 7.1-2 Image of RAID Configuration

General overview - Resource group

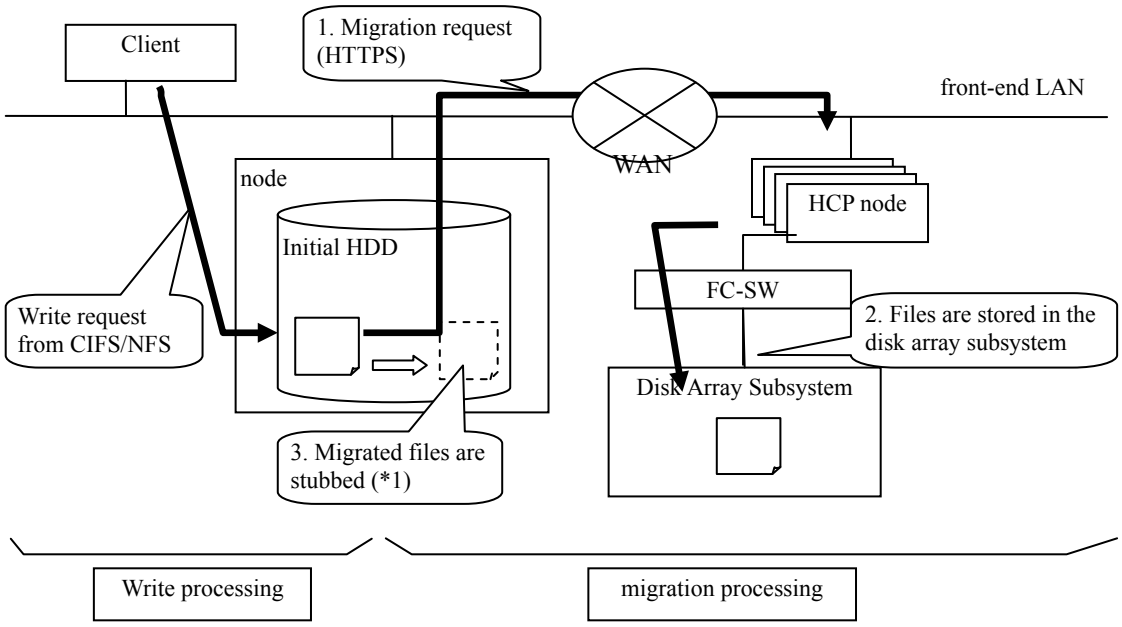
Resource group is booted when OS is booted and a resource group is stopped when OS is stopped. If OS has a failure, a service will keep stopping until the failure is recovered.

(1) HCP function

The Hitachi Content Platform (HCP) is a networking storage system which is suitable for the long storage of stored data without any modifications.
To ensure the integrity of stored data, the HCP uses Write Once Read Many (WORM) storage technology, protection policies, storage policies, and various metadata. In addition to easily accessing an archive when adding or retrieving data, the HCP can delete the saved data if permitted by the access right and policy.
The inside of HCP is divided into “tenant” and its lower place called “namespace”, which are logically partitioned and controlled.
Because objects stored in a namespace cannot be referenced from other namespaces, data saved for a different application, a business unit, or a customer can be separated.
When the HDI is linked with the HCP, files stored on an HDI file system using the NFS/CIFS protocol can be migrated automatically to the HCP according to a migration policy.
The migrated files are regularly stubbed by HDI, the clients can still read/write files while the HDI can reduce the capacity used in the file system.
When HDI start stubbing files regularly, if the free space of the file system is lower than set value (Default : 10%), HDI select WORM files and the files that update time is old, and stub them.
If HDI fails and the stub files are lost, the stub files can be restored from the data stored in the HCP.

(2) Migration processing

The read/write processing includes migration and recall processing between HDI and HCP in addition of read/write from a client to HDI.
The migration processing is performed according to the migration policy specified in GUI.



*1: When HDI start stubbing files regularly, if the free space of the file system is lower than set value (Default: 10%), the files are stubbed in chronological order of the last update dates and time

Figure 7.1-3 Migration Processing

(3) Recall processing

Recall processing is executed when a migrated stub file is accessed by a client. The recall processing when reading the stub file is as follows.

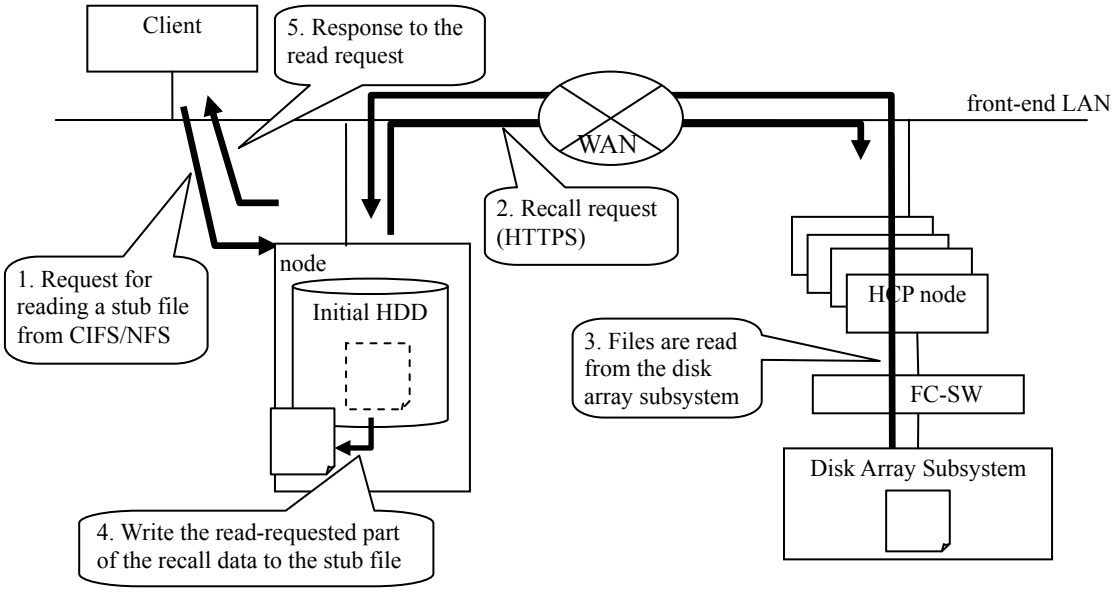


Figure 7.1-4 Recall Processing

(4) Considerations in the normal operation

Before the HDI resource group is started, HCP must have been started. Before HCP is stopped, the HDI resource group must have been stopped.
If the HDI resource group is started when HCP has stopped, the migration or recall processing fails.
Figures 7.1-5 and 7.1-6 show the schematic figures of the failures.

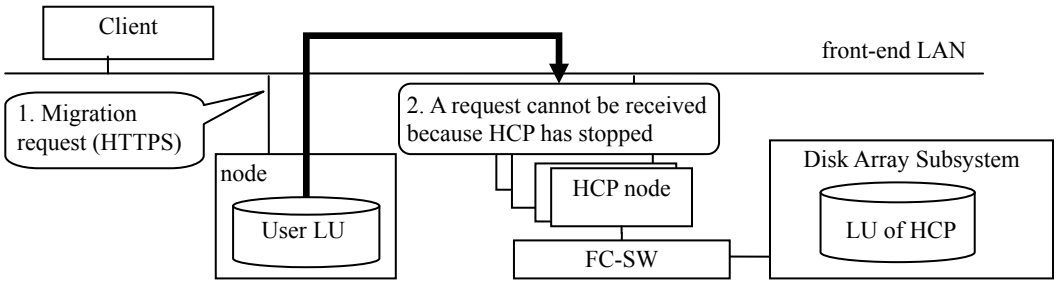


Figure 7.1-5 Migration Processing When HCP Stopped

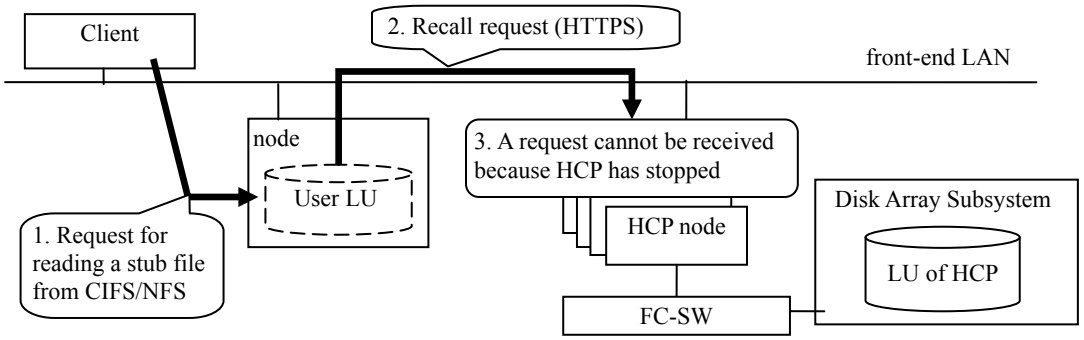


Figure 7.1-6 Recall Processing When HCP Stopped

(5) Communication failure with HCP

The Read/Write request from a client could fail because the communication is disconnected in a way of communication between HDI and HCP via WAN.

- It responds I/O error for the client.

Figure 7.1-7 shows the recall operation when the WAN failure occurs as an example.

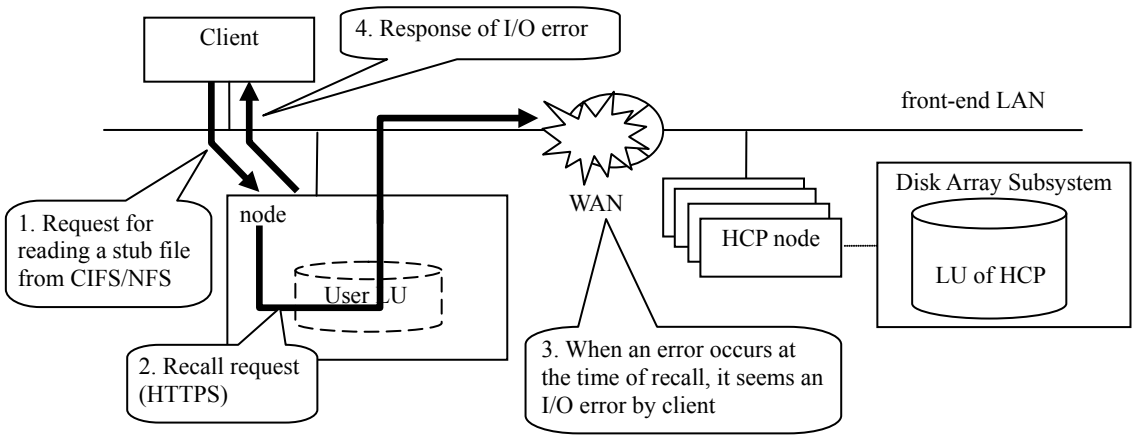


Figure 7.1-7 Operation When WAN Failure Occurs (Recall)

If Read/Write from the client fails due to an I/O error, the client retries after 20 minutes or more elapses after the I/O error occurrence, and checks whether Read/Write is possible.
In the case where the node of HCP failed, the communication may be resumed by retrying from the client. However, in the case where the communication pathway fails, the communication may not be resumed by retrying.
After an I/O error occurred by Read/Write from the client, even if you retry after 20 minutes or more elapsed but an I/O error still occurs, network, hardware or software failure may occur. In this case, determine a failure by following the procedure shown in Chapter8 “Troubleshooting”.

Basic functions of HDI Remote Server

Basic function of HDI Remote Server - Starting Management GUI

(1) In case of using the DHCP server, open the network of an administrative terminal (control point) and click the HDI Remote Server icon shown in the **Other Device**.
If the unchanging IP address is used, type the URL into the address bar of the Web browser in the following style.

URL style when using the unchanging IP address: https://<IP address of the node or host name>/admin/

(2) When the login window is displayed, enter the user ID and password. Then click [Login].
Main window is displayed.

Note: When logging into GUI for the first time, the password change window is displayed. To prevent the unauthorized access, be sure to change the password at the time of the first login.

User ID: admin
Password: chang3me!

Tip: If GUI is not displayed.

See the Chapter 8 “Troubleshooting”.

Basic function of HDI Remote Server – Failure report

HDI Remote Server reports a failure of the node using SNMP(Simple Network Management Protocol) to the customer’s monitoring computer in which the SNMP manager program is installed. By this, the HDI administrator can detect a failure occurred in the node.

HDI Remote Server also reports a failure to the e-mail account defined by HDI administrator.

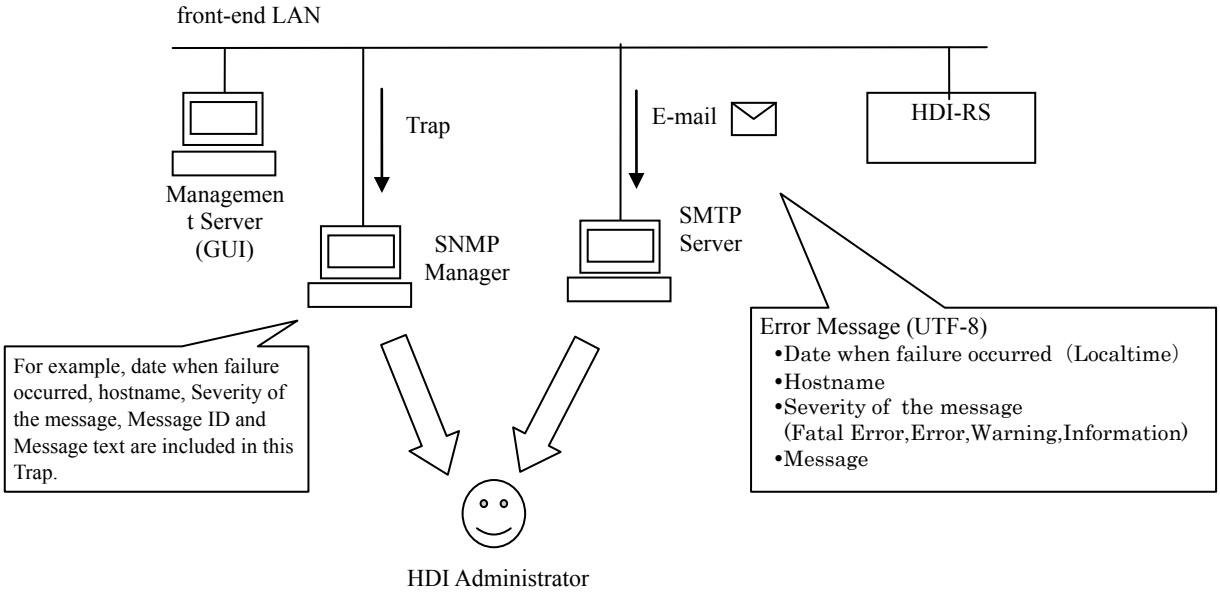


Figure 7.1-8 The flow of that the customer notices the failure occurred.

The system administrator checks message IDs and the messages from the E-mail. The maintenance personnel obtain E-mail that is reporting the message ID from the system administrator.

The following example show example of the failure notice which is sent by E-mail

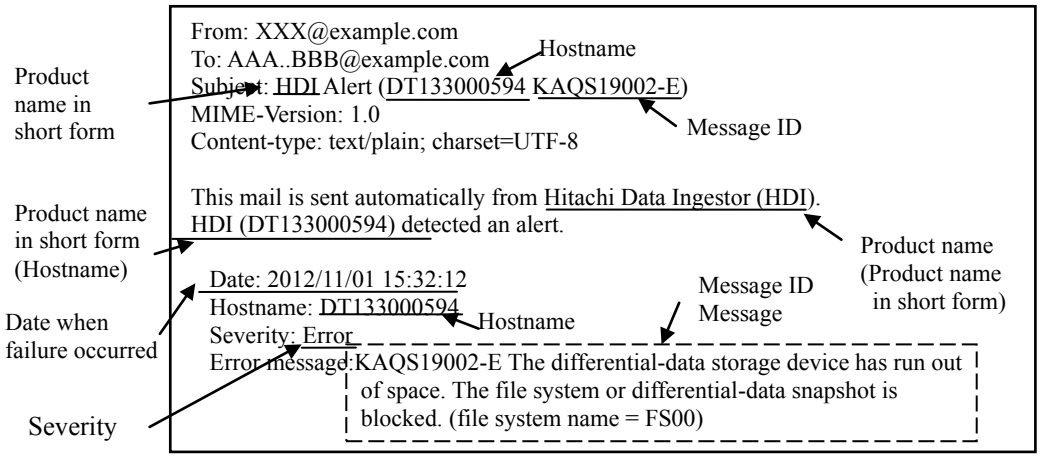


Figure 7.1-9 Display examples of failure notice by E-mail

Chapter 8. *Troubleshooting*

This chapter describes the failure determination procedure. This failure determination procedure varies depending on the failure occurrence status. If a failure occurred during an operation, follow the failure determination procedure after the Chapter 8 “Finding a failure by users” of this document orderly to determine a failure and recover.

If a failure occurred at the time of installing HDI Remote Server at the initial stage, see FAQ (FAQ for the time of initial installation) for the failure determination procedure. If a failure has occurred during the initial installation and notified by message, take an appropriate action referring to the message confirmation table in the Chapter 8 “Confirming Message ID”.

Table 8-1 Structure of Chapter8

#	Title
1.	Finding a failure by users
2.	Checking FAQ (User FAQ)
3.	Confirming Message ID
4.	Checking network environment
5.	Checking management port of HDI Remote Server
6.	Confirming HCP status
7.	Checking FAQ (AD server)
8.	Rebooting HDI Remote Server
9.	When a problem is not solved
10.	All Log collection procedure
11.	Appendix A-When finding the invalid data in Consistency Check

Overview of the failure determination procedure is shown below.

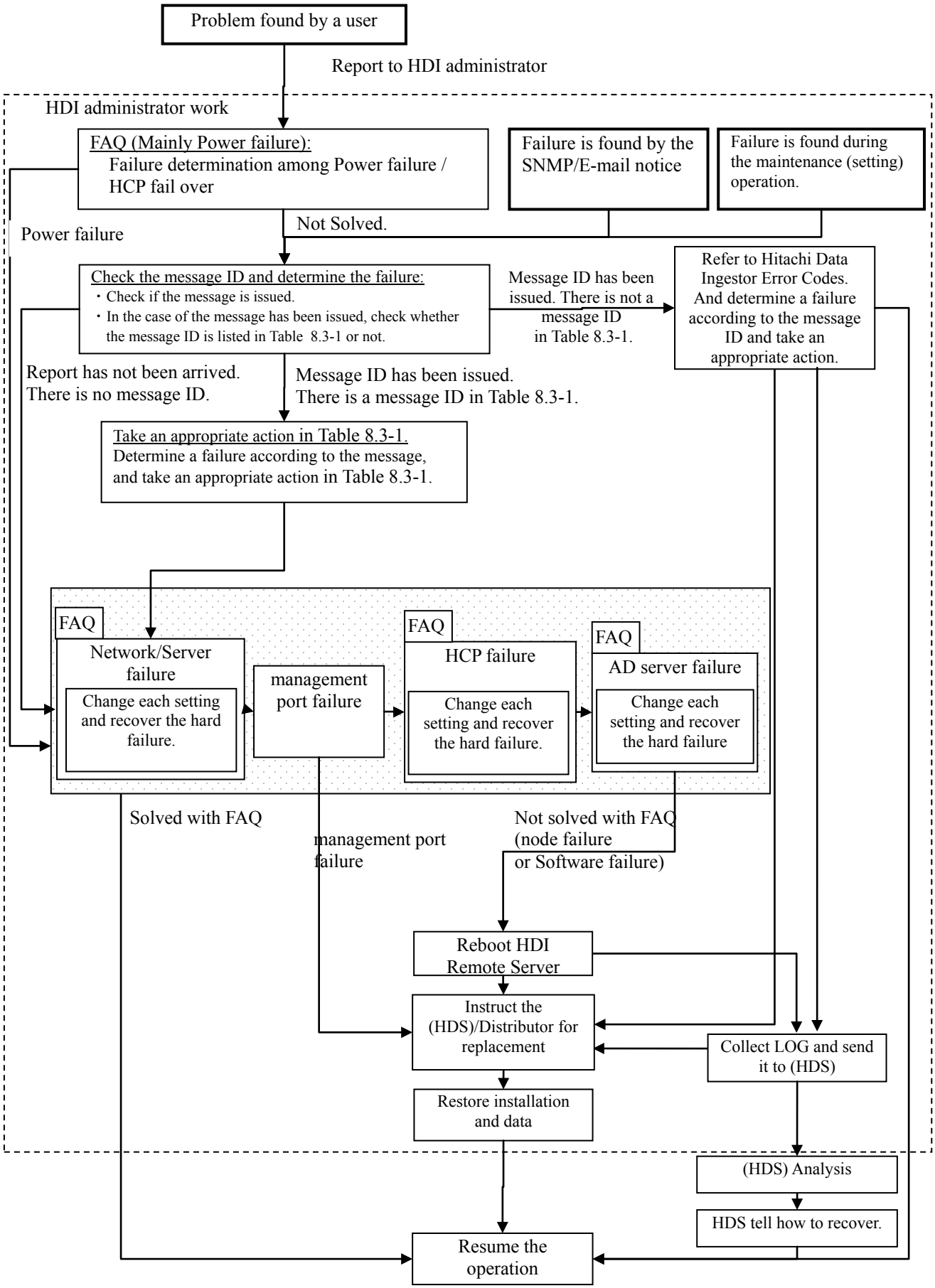


Figure 8-1 Overview of Failure Determination

Finding a failure by users

When a failure occurred during the HDI Remote Server operation, a user contacts a HDI administrator and HDI administrator starts the failure determination.

If any beep (memory error) or abnormal tone (hardware error) sounds, HDI administrator replaces the node.

If I/O error has occurred, follow the failure determination procedure stated after the Chapter 8 “Checking FAQ” of this document.

Finding a failure by SNMP/E-mail

When a failure occurred during the HDI operation , the SNMP trap/E-mail that store the failure information is sent to HDI administrator. When HDI administrator receive the SNMP tarp/E-mail, Chapter 8 “Confirming Message ID” should be referred.
If the message ID is found in the Table 8.3-1, perform the action.
If the message ID is not found in the Table 8.3-1, refer the description and the action in “Hitachi Data Ingestor Error Codes”, and perform the failure isolation and recovery.

Checking FAQ (User FAQ)

(1) HDI administrator should ask a user to retry the system 20 minutes after the failure phenomenon occurred. By waiting, the following temporary trouble may be restored.
- I/O has not been executed due to the failover of HCP which manages the data of HDI Remote Server.
- Windows client IP address caching problem

If a problem is not resolved after the retry, follow the below procedure.

(2) If the IP address of the HDI Remote Server has been set via the DHCP server and the reservation function of the IP address is not used on the DHCP server, IP address is changed due to the reboot operation etc. and I/O may not be executed as a consequence.
In this case, instruct a user to execute the following operations.
- For the client using the CIFS sharing, particular operation is not required.
  (System will be recovered followed by the retry performed 20 minutes after the failure phenomenon occurred stated in (1) shown above)
- For the client using the NFS sharing, execute the mounting again.

(3) Check that the power LED of the HDI Remote Server is switched on. If the power LED has been switched off, push the power switch.

If the power LED is ON, proceed to the Chapter 8 “Confirming Message ID”.

If the power LED is still OFF even if the power switch is pushed, check with FAQ (Power FAQ) whether any problem occurs in the power supply system. After checking FAQ (Power FAQ), confirm whether there is a problem with the items shown in the following table.

If no problem is found, write “ﾚ” in the Check column.

If all columns are filled with “ﾚ” to determine that no problem has occurred in the power supply system and proceed to the Chapter 8 “Confirming Message ID”.

If a problem is not resolved yet even after checking FAQ (Power FAQ), it may be a hardware problem. Execute the node replacement based upon the Chapter 9 “Replacement”.

Table 8.2-1 Confirmation Table for Power Supply System

#	Confirmation Item	Check column
1	No problem with connection of power cable.	
2	Conducting to the HDI Remote Server connecting port.	
3	Power failure has not been occurred.	

Confirming Message ID

In the case that SNMP trap or E-mail had been received, refer the Table 8.3-1 and check if the message ID is found in the Table 8.3-1 or not.
If the message ID is found in the Table 8.3-1, perform the action.
If the message ID is not found in the Table 8.3-1, refer the description and the action in “Hitachi Data Ingestor Error Codes”, and perform the failure isolation and recovery.

NOTE: Contact to (HDS), if the message ID's action in the “Hitachi Data Ingestor Error Codes” is “contact maintenance personnel”.

In the case there is no message, the failure of network or server setting may have occurred. Proceed to the Chapter 8 “Checking network environment”.

If a few messages are output, start to take an action corresponding to an oldest unconfirmed message. When a few messages are output at the same time, start to take an action corresponding to largest code number.

Table 8.3-1 Failure Recovery from Notification Message (1/2)

#	Message ID	対処
1.	KAQM06138-E	1・.If any message ID as followed is displayed, take the action that the message indicates. (KAQG90001-E(blocked), KAQG90006-E(blocked), KAQG41004-E(HDD failure), KAQG41010-E (Consistency Check error), KAQG41011-E (FAN failure), KAQG41013-E (Consistency Check error)) 2. Switch off the power first and then switch on the power again. 3. If the problem has not been solved yet, collect logs and replace a node (-> Chapter 9 “Replacement”).
2.	KAQM35003-E	
3.	KAQM35007-E	
4.	KAQM35004-E	1. Switch off the power first and then switch on the power again. 2. If the problem has not been solved yet, collect logs and replace a node (-> Chapter 9 “Replacement”).
5.	KAQM35008-E	
6.	KAQM35017-E	
7.	KAQG41011-E	Replace a node. (-> Chapter 9 “Replacement”)
8.	KAQG46531-E	
9.	KAQG46533-E	Replace a node. (-> Chapter 9 “Replacement”) The node could lead to the temperature rise. Please stop using the node immediately and to power off the HDI Remote Server until replacement.
10.	KAQG41010-E	Refer to the Chapter8 “When finding the invalid data in Consistency Check”. Error occurred in the Consistency Check.
11.	KAQG41013-E	
12.	KAQG41004-E	Replace HDD or node (see the Chapter 9 “HDD Replace procedure” at the start).
13.	KAQG90001-E	1. Switch off the power first and then switch on the power again. 2. If the problem has not been solved yet, replace a node (-> Chapter 9 “Replacement”).
14.	KAQG90006-E	

Table 8.3-1 Failure Recovery from Notification Message (2/2)

#	Message ID	対処
15.	KAQG20902-E	1. If the message KAQG90001-E(File system is blocked) or KAQG90006-E(File system is blocked) has been output, take an appropriate its action. 2. Switch off the power first and then switch on the power again. If the problem has not been solved yet, collect logs and replace a node (-> Chapter 9 “Replacement”).
16.	KAQG41008-E	
17.	KAQG41009-E	
18.	KAQG41012-E	
19.	KAQG52900-E	
20.	KAQG90006-E	
21.	KAQG90008-W	
22.	KAQG90010-E	
23.	KAQM04247-E	
24.	KAQM05156-E	
25.	KAQM06137-E	
26.	KAQM06139-E	
27.	KAQM14129-E	
28.	KAQM37021-E	
29.	KAQM37025-E	
30.	KAQM37036-E	
31.	KAQM37101-E	
32.	KAQM37140-E	
33.	KAQM50900-E	
34.	KAQM50901-E	
35.	KAQM50902-E	
36.	KAQM50903-E	
37.	KAQM50904-E	
38.	KAQM50905-E	
39.	KAQM50906-E	
40.	KAQM50921-E	
41.	KAQM50922-E	
42.	KAQM50923-E	
43.	KAQM50924-E	
44.	KAQM50925-E	
45.	KAQM50926-E	
46.	KAQM50927-E	
47.	KAQM50928-E	
48.	KAQM50930-E	
49.	KAQM50941-E	
50.	KAQM50942-E	
51.	KAQM50943-E	
52.	KAQM50944-E	
53.	KAQM50945-E	
54.	KAQM50946-E	
55.	KAQM50947-E	
56.	KAQM50948-E	
57.	KAQM50949-E	
58.	KAQM50950-E	

Checking network environment

Check the following confirmation items. If no problem is found , write "ㅅ" in the check column and when all columns are filled with "ㅅ", determine that there is no problem with the network environment and proceed to the Chapter 8 "Checking management port of HDI Remote Server".

If the check columns are not filled with "ㅅ", check the FAQ (Network FAQ) and confirm whether no mistake with the items set to the server.

Table 8.4-1 Checking Network Environment

#	Environment	Confirmation Item	Check Column
1.	Connecting to HDI Remote Server	DNS server is operated normally.	
2.		DNS server has been set to be able to use the DDNS function.	
3.		HDI Remote Server is registered on the DDNS server.	
4.		DHCP server is operated normally.	
5.		HDI Remote Server is registered on the DHCP server.	
6.		Active Directory is operated normally.	
7.		HDI Remote Server is registered in Active Directory.	
8.		IP-SW, Router, WAN and NAT are operated normally.	
9.		NTP server is operated normally.	
10.		HDI Remote Serve is synchronized with NTP server.	
11.	Connecting to HCP which manages the data of HAD Remote Server.	DNS server is operated normally.	
12.		HCP is registered on the DNS server.	
13.		Host name of HCP is resolved on the DNS server.	
14.		IP-SW, Router, WAN and NAT are operated normally.	
15.		NTP server is operated normally.	
16.		HCP is synchronized with the NTP server.	

Checking management port of HDI Remote Server

(1) Try to access to the management GUI.
(Refer to Chapter 7 “Basic function of HDI Remote Server - Starting Management GUI”.)
If the management GUI login window is not displayed, proceed to step (2).

(2) Switch off the node. (Refer to Chapter 5 “How to switch off the power ".)

(3) Unplug the power cable and wait for 1 minute.

(4) Connect the power cable.

(5) Connect management PC directly to HDI Remote Server referring “Hitachi Data Ingestor Single Node Getting Started Guide”.

In case of operating DHCP, set the IP address of the management PC to the value that can access to ”169.254.1.100”.The netmask is ” 255.255.0.0”.

[Example] IP address: 169.254.1.99, Netmask: 255.255.0.0, Gateway: (None)

(6) Switch on the node and wait for 5 minutes after the power LED is lit.
(Refer to Chapter 5 “How to switch on the power".)

(7) Try to access to the management GUI.
(Refer to Chapter 7 “Basic function of HDI Remote Server - Starting Management GUI”.)

If the management GUI login window is not displayed, the management port or the OS failed. Perform the node replacement.

If the management GUI login window is displayed, it is cleared that the management port of the HDI Remote Server did not fail. Reconnect the cable of the HDI Remote Server which disconnected in step (5). Then, switch off the node, and switch on the node 1 minute after again. And, proceed to Chapter 8 “Confirming HCP status”.

Confirming HCP status

Confirm to HCP administrator that any failure or failover has not been occurred by seeing GUI of HCP which manages the data of HDI Remote Server.

If a failure occurs, take an appropriate action according to the below table.

Table 8.5-1 Failure Confirmation Procedure When an Error Occurs in HCP

#	Confirmation Item	Status	Action
1	Confirm that HCP is accessible	- When HCP is accessible	-> Proceed to #2.
		- When HCP is not accessible	-> Contact the center where HCP is located to ask whether a failure occurs.
2	Confirm that a HCP node has not failed over in one hour since the fail over occurred.	・When fail over occurs	-> Perform I/O again 20 minutes later. If the problem has not been solved yet, proceed to #3.
		・When fail over does not occur	-> Proceed to #3.
3	Confirm the HCP status (Confirm whether service is still given)	・When the status is normal.	-> Proceed to the Chapter8 “Checking FAQ (AD server)”.
		・ When the status is not normal.	-> Contact the center where HCP is located to ask whether a failure occurs.

Checking FAQ (AD server)

Check that Active Directory has been operated and set normally.

If I/O by a user cannot be recovered, proceed to the Chapter 8 “Rebooting HDI Remote Server”.

Rebooting HDI Remote Server

Since the problem may be solved, reboot HDI Remote Server. Try to reboot for twice (if the problem has not been solved 1st reboot.) by following procedure.

(1st reboot)

(1) Switch off the HDI Remote Server. (-> see the Chapter 5 “How to switch off the power”)

(2) Unplug the power cable and wait for 1 minute.

(3) Connect the power cable and switch on the HDI Remote Server. And then wait for 5 minutes after the power LED is lit...
(-> see the Chapter 5 “How to switch on the power”)

(4) Try to access to the management GUI.
(-> see the Chapter 7 “Basic function of HDI Remote Server - Starting Management GUI”)

(5) If the management GUI login window is not displayed, try to execute the 2nd reboot.

(2nd reboot)

(1) Switch off the HDI Remote Server.
(-> see the Chapter 5 “How to switch off the power”)

(2) Switch on the HDI Remote Server. And then wait for 5 minutes after the power LED is lit...
(-> see the Chapter 5 “How to switch on the power”)

(3) Try to access to the management GUI.
(-> see the Chapter 7 “Basic function of HDI Remote Server - Starting Management GUI”)

If the problem has not been solved yet, proceed to the Chapter 8 “When a problem is not solved”

When a problem is not solved

HDI administrator should collect logs. Then contact the distributor / (HDS) to send the alternative device to the environment where an HDI Remote Server failure has occurred.

For the log collection method, see the Chapter 8 “All Log collection procedure” and for the node replacement and replacement procedure, refer to the Chapter 9 “Replacement”.

All Log collection procedure

Collect a log and contact the distributor/ (HDS) with the collected log as necessary.

●Log acceptance at the distributor site

[TUF server] The account will be provided from Hitachi Data Systems.

Note that a few log files are archived with “tar” and downloaded in the zipped format (gzip).

Using management GUI, collect the “Alllog” referring “Hitachi Data Ingestor Single Node Troubleshooting Guide”.

Appendix A - When finding the invalid data in Consistency Check

This section describes the countermeasures when a HDI administrator finds the invalid data

Messages of invalid data

- “KAQG41010-E”
- “KAQG41013-E”

When finding an invalid data - Concept

When the invalid data message is output, replace a node.

An HDI administrator should arrange for a new node immediately, and ask a user to check the file visually to confirm whether any corrupted file exists until the new hardware arrives at the HDI administrator side.

If a corrupted file is found, ask a user to overwrite the corrupted file with the “Normal file”. The Consistency Check is executed on every Tuesday and Friday and nothing notified if there was no problem. Therefore, overwriting of a corrupted data with the data migrated before last Tuesday or Friday has a higher possibility of restoring the “Normal data”. However, the migrated data has been performing versioning for default 7 days. If 8 days have passed, “Normal data” may disappear.

Table 8.10-1 Countermeasures

#	Countermeasure (*1)	Status after taking countermeasure
1	Execute the node replacement	Invalid data is resolved.
2	Execute the overwrite of the migrated data	An error is output to Report continuously as the failure is remained. (If the failure part is [OS/Boot area], it may be panic / hung. If the failure part is [User data area], it may be resolved, but it seldom happens).

*1: Data to be restored after the node replacement is the data migrated before the node replacement (last node replacement). Note that corrupted data might have been migrated depending on the timing of the migration.

For the procedure when invalid data is found and practical examples are shown below.

When finding an invalid data - Execution procedure

(1) Check whether KAQG41010-E and KAQG41013-E are output in the daily Report.

(2) If a report of KAQG41010-E or KAQG41013-E is confirmed, an HDI administrator should arrange for a node change.
Ask a user to overwrite the corrupted file with the past migrated “Normal data” before the execution of the node replacement.

Ask a user to check whether the corrupted file is found which updated after the latest Consistency Check day. Moreover, if the data corrupted file is found, ask a user to check the migrated data in the past and overwrite a corrupted data with the “Normal data”. The most suitable for the data to overwrite a corrupted file is the file of the previous date than the last Consistency Check.

However, a corrupted file may not be found as the invalid data file does not necessarily exist in the user data area and the invalid data file exists in OS / Boot area instead.

(3) After taking the above countermeasure (2), HDI administrator should continue to monitor a Report.
Invalid data message will not be issued if a node was replaced.
If the overwrite of the past migrated data was executed, confirm that“KAQG41013-E.” is not output in Report until the node replacement is executed. In case that a message is output, execute the above procedure (2) again.

(4) When a new hardware has arrived at the HDI administrator side, HDI administrator replaces a node.

Note: After checking the user data, leave a whole day (to wait until the normal data is migrated) and HDI administrator replace the node.

Inform users that data will be restored to the last migrated data after the node replacement.

When finding an invalid data - Execution example

The below table shows the recovery procedure when occurring the invalid data in chronological order.

[Assumed scenario] (Migration Schedule: once a day. Consistency Check: Twice a week (Tuesday and Friday), Retention period of the migrated data in the past: 7 days)

An error is found in the Consistency Check executed on 5/8 (Fri) and arranged for HDI Remote Server for replacement. However, it takes over 7 days until delivered to an HDI administrator. Since the normal migrated data in the past may be disappeared, instructed a user to check the file in visual and overwrite with a normal file and migrate.

Table 8.10-2 Example of Recovery Procedure when Occurring Invalid Data

(Abbreviation in the HDI Remote Server event: C.C.= Consistency Check, M(data_*mmdd*)=Migration (data_backup-date))

#	Date	Time	HDI Remote Server event	Notification/Action by HDI administrator	Action by users	Operation
1.	5/ 5 (Tue)	1:00	M(data_0505)			Continue
2.		2:00	C.C. start			↓
3.		14:00	C.C. end	(For the normal termination)		↓
4.	5/ 6 (Wed)	1:00	M(data_0506)			↓
5.	5/ 7 (Thu)	1:00	M(data_0507)			↓
6.	5/ 8 (Fri)	1:00	M(data_0508)			↓
7.		2:00	C.C. start			↓
8.		14:00	C.C. end	Report: Output of KAQG41010-E is confirmed. Report to a user if this message is output. Start to arrange for HDI Remote Server for replacement.		↓
9.	5/ 9 (Sat)	1:00	M(data_0509)			↓
10	5/10 (Sun)	1:00	M(data_0510)			↓
11	5/11 (Mon)	1:00	M(data_0511)			↓
12		9:00 - 17:00			Check the file. If a corrupted file is found, find the normal file from data_0505 and over write.*1	↓
13	5/12 (Tue)	1:00	M(data_0512)	(Normal data as a user data is migrated (assumption))		↓
14		2:00	C.C. start			↓
15		14:00	C.C. end	Report: Confirm that “KAQG41013-E.” is output. Report to a user if the message is output.		↓
16	5/13 (Wed)	1:00	M(data_0513)			↓
17		9:00 - 17:00			Check the file. If a corrupted file is found, find the normal file from data_0512 and over write.	↓
18	5/14 (Thu)	1:00	M(data_0514)	(Normal data as a user data is migrated (assumption))		↓
19	…(HDI administrator should keep monitoring error messages until an HDI Remote Server for replacement is arrived at the HDI administrator side. If “KAQG41013-E.” was output in failure notification, execute the step #17 in the procedure. If “KAQG41013-E.” was not output, no operation is required.)…					↓
20	5/21 (Thu)	1:00	M(data_0521)	(Repeat the overwrite and normal data is migrated)		↓
21		9:00 -			HDI Remote Server is arrived. Notify to HDI administrator.	Stop/Replace
22					Replace a node (+ “data_0521” is restored)	↓
23						Resume

*1: Sometimes data which was migrated on the specified date may not be found depending on the timing of file creation. In that case, find a normal file from the files which was migrated on the date closer to the normal completion of the Consistency Check.

Chapter 9. *Replacement*

The replaceable unit of HDI Remote Server includes the node and the HDD. According to the part to be replaced, proceed to the appropriate section.

Procedure of a node replacement is required

If a node replacement is required according to the failure determination process, HDI administrator should ask the distributor/(HDS) to ship and recall a node.

When replacing a node, follow the below procedures.

- Disconnect an older node from the environment
- Operation for node replacement

If the failed HDI Remote Server is still within the warranty period, the distributor sends the product to Hitachi Data Systems as soon as the HDI Remote Server arrives, and receives a substitute. If the failed HDI Remote Server is out of the warranty period, no substitute is available.

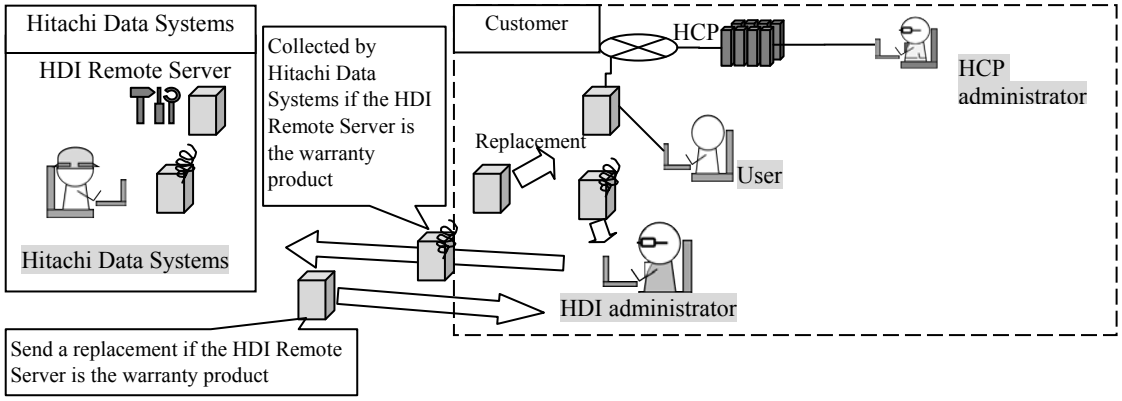


Figure 9.1-1 Flow of Replacement

Node replacement - Disconnecting older HDI Remote Server from the environment

(1) Switch off the power if Power LED is on.

(2) After confirming that the power is off by Power LED turning off the light, pull out each connecting cable.

(3) Send the replaceable HDI Remote Server to the distributor/(HDS).

Note: If the node to be replaced is using the fixed IP address, HDI administrator needs to set the IP address. Before the replacement check the node IP address used in the node to be replaced.

(1) When HDI Remote Server arrived at the HDI administrator`s site, HDI administrator confirm a label and serial number and make sure that they are same as the ones the HDI administrator is understanding.

(2) Connect new HDI Remote Server to the network environment referring Hitachi Data Ingestor Single Node Getting Started Guide.

In case of operating DHCP, the following items need to reregister and make well known.

- If the IP address is fixed with the IP address reservation function of the DHCP server, MAC address which has been registered on DHCP server for the reservation of the IP address needs to be reregistered in the MAC address on HDI Remote Server.

(3) HDI administrator restores the system setting information and the user data referring “Hitachi Data Ingestor Single Node Troubleshooting Guide”.

(4) HDI administrator executes the OS update installation if necessary (-> see the Chapter10 “Updating software according to the request from a distributor”).

(5) HDI administrator should confirm with a user that I/O was executed successfully.

Note:
- Client which is using the shared NFS needs to stop the access and unmount the mount with the old host name, and mount again by using the new host name.
- Also, in case of using the shared CIFS and DHCP, let users know the host name of the destination access of the replaced node.

If I/O was not recovered, proceed to the Chapter 8 “All Log collection procedure” to collect All Log and send.

HDD replacement procedure

If a HDD failure message was output, HDI administrator should replace HDD after checking the OS status. For the detailed procedure, see below.

Note:
- Even if 2 HDD are failed, sometimes it seems to be 1 HDD failure. 2nd HDD failure may be found while replacing and rebuilding a first HDD. Note that a node needs to be replaced in this case.
- When replacing HDD, confirm that the HDI Remote Server is powered on. If not, rebuilding is not executed.
- Do not reinstall the same HDD which has been removed.

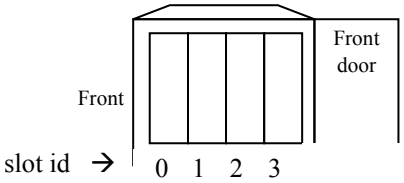
(1) HDI administrator confirm that the OS status is up (determine it whether the login window of the management GUI is displayed.) and that the following message ID which indicate HDD failure in the report is output.

In the following cases, a node needs to be replaced. (-> See the Chapter 9 “Node replacement - Operation for node replacement”)
- When the failure message (KAQG41004-E) is output for two or more HDDs (slot).
- A failure message (KAQG41004-E) is output and OS goes down as well.
- An automatic recovery failure message (KAQG41011-E) is output.

(2) HDI administrator contact (HDS) to send HDD.

(3) HDI administrator specifies which HDD has a failure according to the message.

KAQG41004-E An error was detected in the device I/O. (state = faulty, RAID-LU = < RAID-LU name >, slot = < slot id >, device = < device name >)



* In the 2 HDDs configuration, HDD is not installed in the slot ID 2 and 3.
Slot ID is always numbered from the left side as 0,1・・・.

Figure 9.2-1 HDD Installation Example

(4) HDI administrator should confirm that a status of failed HDD is [removed] in GUI. If the status [removed] is confirmed, HDI administrator replaces HDD.

Note: When replacing HDD, wait more than 1 minute from the time pulled HDD until installing another HDD.

If over 1 minute has passed after the removal of HDD, “nodevice” is output. If the time is shortly after the HDD installation, “setup” is output. If the time is after the recognition of HDD installation until the recovery of data is completed, “rebuild” is output.

Note:
- Sometimes the HDD status may be [setup] after installing HDD. If this status [setup] does not change to [rebuild] even after a few hours, either a node or HDD has a failure.
- I/O performance is degraded while rebuilding. Time takes for rebuilding is varied depending on the I/O load.

(5) HDI administrator should confirm GUI and make sure that the HDD status is “normal”. If the status “failed” included, “Rebuild” has been failed. In that case, replace a node.

Chapter 10. *Updating software according to the request from a distributor*

Sometimes a distributor may ask the HDI administrator for the software update.

HDI administrator should ask HCP administrator to store the OS image which requires the update in HCP, and execute the installation.
Software is give from a distributor to HDI administrator through HTTP.

Note: To execute the update for a huge volume of HDI Remote Server from one HCP at the same time, load on the network increases. Therefore, this update needs to execute in a systematic manner.

(1) (HCP) administrator stores the installation image on HCP.
The procedures shown below need to be performed by (HCP) administrator.

(a) Provide a name space called “system-install” to each tenant cooperated with HDI Remote Server. Set “Hash Algorithm” to “MD5” when creating a name space.

For the name space of “system-install”, set the data account for the system (HDI administrator sets this account.). Add the authorization of “Browse”, “Read” “Write” and “Delete” for the name space of **system-install**.

(b) Provide an account for the image registration (not the data account for the system). For “Role” of the account for the image registration, assign the same Role as the one assigned to the data account for the system. Then, execute the procedures from the step (c) using the account for the image registration.

(c) Provide the system directory in the name space of **system-install**.

(d) Provide the directory titled the product name (“HDI”) in the system directory created in the above step (c).

(e) Extract **install_files.tar.gz** from the distributed DVD and store the directory created in the above step (d).

Note: Image needs to be stored in each tenant cooperated with HDI Remote Server.

(f) On the file browser screen of HCP, compare the Hash value (MD5) and the value of install_files.tar.gz.md5 stored in the distributed DVD and confirm that MD5 has been stored correctly.

(g) From the environment such as Linux server where is accessible to HCP, register the custom metadata of the installation image using the **curl** command for the installation image on HCP. The custom metadata to be registered is the version management file (version.xml) which is included in the installation media.

(Execution example: curl -k -b hcp-ns-auth=<*user-name (base64)*>:<*password (MD5 hash)*> -iT version.xml https://system-install.<*tenant-name*>.<*hostname(hostname.hitachi.com)*>/rest/system/HDI/ install_files.tar.gz?**type=custom-metadata**

Value of < *user-name (base64)*>:
Enter the value which was base64 encoded account name created in the above procedure (b).
(Generally available base64 encoding tool is also usable)

Example: A method to encode a user name (user1) in base64.

```
$ echo -n user1 > username.txt
$ base64 username.txt
dXNlcjE=xxxxxxxxxxxxxxxxxxxxxxxxxx
```

Value of <*password (MD5 hash)*>:
Enter the MD5 hashed value of the account password which was created in the above procedure (b).
(Generally available MD5 hashed tool is also usable)

Example: A method to generate MD5 hash value of the password (pass1).

```
$ echo -n pass1 > password.txt
$ md5sum password.txt
a722c63db8ec8625af6cf71cb8c2d939 password.txt
```

(2) HDI administrator should execute the update installation referring ”Hitachi Data Ingestor Single Node Administrator’s Guide”.

(3) HDI administrator should check the “System Version” in GUI and confirm that the OS version is updated.

Chapter 11. *Quality Assurance System and New OS Distribution Path*

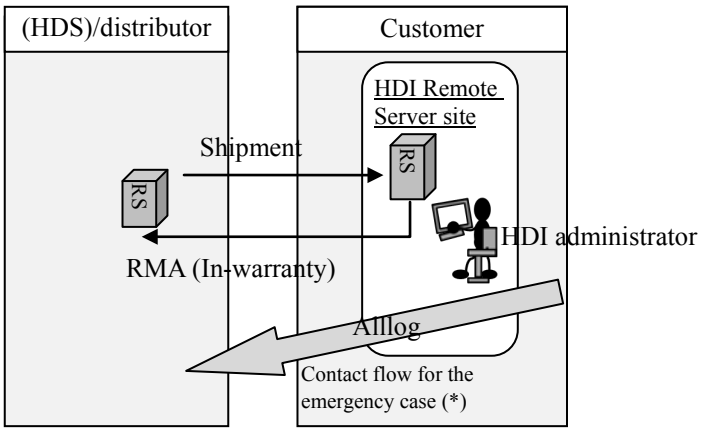
Since the warranty period is varied depending on the time of delivery, check the specifications or any other documents come with the HDI Remote Server.

If any problem has occurred, contact the local distributor.

If the local distributor cannot resolve the problem, send the log to the distribution source.

Local distributor should consider taking measures such as providing an alternative HDI Remote Server to HDI administrator.

If an HDI Remote Server is the product out of warranty, an HDI administrator should purchase a new HDI Remote Server. Note that continuous use of the out of warranty HDI Remote Server is not covered.



* Not recoverable case even though all I/O have failed and a node was replaced.

Figure 12-1 Escalation Route

Chapter 12. *Miscellaneous*

Command to distinguish the operation form (prsstatus)

This command display whether the HDI-RS on that this command is performed coordinate with HCP Anywhere or not.

Login to the node using 'ssh' referring to Hitachi Data Ingestor CLI Administrator's Guide, and then use this command.

Synopsis

prsstatus
prsstatus –h

Displayed Information

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

Table 12-1 Information displayed when executing the prsstatus command

Displayed Information	Description
Centrally Managed	Displayed in the case the HDI-RS coordinate with HCP Anywhere.
Locally Managed	Displayed in the case the HDI-RS does not coordinate with HCP Anywhere.

Example

When the command is performed on the node which coordinate with HCP Anywhere:

```
$sudo prsstatus
Locally Managed
```

図12-1 Execution Example of the prsstatus command

Return values

Table 12-2 Return values and Messages of the prsstatus command

Message	Description	Action
KAQM14136-I	Normal termination (Specify "-h" option)	-
KAQM14134-E	An error occurred in the shared processing of commands	1. Switch off the node, then switch on the node again. 2. If the problem has not been solved yet, collect logs and replace a node (-> Chapter 9 "Replacement").

*: If any other massage is displayed, refer to Hitachi Data Ingestor Error Codes.

Conditions for installation environment

HDI Remote Server installation environment is as follows.

Table 13-1 Environment Conditions

No	Item		Quality standard/Specification
1	Ambient temperature	In operation	Please confirm it to Hitachi Data Systems.
2	Ambient humidity	In operation	
3	Power requirement		

Glossary

Table 13-2 Definition of Terms

#	Term	Meaning
1	HCP	Abbreviation of Hitachi Content Platform. The HCP is a system for long-term data storage and management. The data of the file system created by HDI is migrated to HCP.
2	HCP-AW	Abbreviation of Hitachi Content Platform Anywhere It is a system which is shared by accessing to data from various locations. If a user adds data to HCP AW, that data is saved in HCP and the data is shared through user terminals (computer, smart phone, tablet computer etc.).
3	Centrally Managed HDI Remote Server	The HDI-RS that is managed by HCP Anywhere administrator and that coordinate with HCP Anywhere. It is abbreviated as HDI-RS CM.
4	Locally Managed HDI Remote Server	The HDI-RS that is managed by HDI administrator and that does not coordinate with HCP Anywhere. It is abbreviated as HDI-RS LM.
5	Namespace	A namespace that can be created in HCP. The namespace is a logical group, and an object stored in one namespace cannot be referred to from another namespaces. It specifies one namespace per file system of a node.
6	Tenant	One grouped a namespace that can be created in HCP. One tenant can own multiple namespaces. One tenant is allocated to one node for migration.
7	Migration	A function to copy the file data on a node to HCP.
8	Recall	A function to read the substantial data of the file from HCP in response to the HDI client access that a node client Read/Write the stub file.
9	Stub file	A file that file property is remained, but that data on a node moved to HCP. About the file on a node the data of the file are duplicated to HCP by Migration, but after that the file on a node become unsubstantial because a node stub data and remained only property. If a client require to Read /Write stub file, a node respond it using Recall function that read out the substantial data of the file from HCP.
10	Management GUI	Management GUI is a user interface used by the HDI administrator to manage a node.
11	UPnP Control Point	A client which received the UPnP service.
12	node	It indicates HDI Remote Server. A server to receive the request of Read/Write using CIFS/NFS. Data is stored in the internal HDDs within the server.
13	front-end LAN	LAN which the client uses for accessing data.

Hitachi Vantara

Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 95050-2639 USA
www.HitachiVantara.com
community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com