HITACHI
Inspire the Next

HDI Remote Server Administrator Guide

Hitachi Data Systems

MK-90HDI040-00

Contents

Preface

This preface includes the following information:

- Intended audience
- Release notes
- Document revision level
- Changes in this revision
- Document organization
- Safety information
- Referenced documents
- Getting help
- Comments

Intended audience

This document is intended for system administrators, Hitachi Data Systems representatives, and Authorized Service Providers who install, configure, and operate the HDI Remote Server.

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.

Document revision level

Revision	Date	Description
MK-90HDI040-00	December 2013	Initial Release

Changes in this revision

None. Initial release.

Document organization

The following table provides an overview of the contents and organization of this document. Click the chapter title in the left column to go to that chapter. The first page of each chapter provides links to the sections in that chapter.

Chapter	Description
Chapter 1: Introduction	This chapter provides an overview of the role names and job descriptions used with the HDI Remote Server.
Chapter 2: Installation	This chapter describes the installation procedure.
Chapter 3: Power supply operation	This chapter describes how to turn on and off the power supply.
Chapter 4: Initial setting	This chapter describes how to perform the initial settings.
Chapter 5: Overview and basic functions of HDI Remote Server	This chapter explains the basic functions of the HDI Remote Server.
Chapter 6: Troubleshooting	This chapter describes how to troubleshoot the HDI Remote Server.
Chapter 7: Replacement	This chapter contains information about replacement procedures.

Chapter	Description
Chapter 8: Updating software according to the request from a distributor	This chapter describes how to update software according to a distributor request.
Chapter 9: Procedure to use HDI Remote Server on another site	This chapter describes the procedure to use HDI Remote Server on another site.
Chapter 10: Quality assurance system and new OS distribution path	This chapter describes the quality assurance and new OS distribution path.
Chapter 11: Miscellaneous	This chapter contains miscellaneous information about the HDI Remote Server.

Safety information

Before performing unit replacements, read the Safety Guidelines in this document.

Referenced documents

The Hitachi Compute Blade system user documentation is available on the Hitachi Data Systems Portal: https://portal.HDS.com. Please check this site for the latest documentation, including important updates that may have been made after the release of the product.

Getting help

When you contact http://support.hds.com, provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The exact content of any messages displayed on the system(s).

For technical support, visit the portal site at https://portal.HDS.com.

Comments

Please send us your comments on this document, if any, by e-mail to: doc.comments@hds.com. Make sure that the e-mail includes the document title and number, revision, and section(s) and paragraph(s) whenever possible.

Thank you! (All comments become the property of Hitachi, Ltd.)

Safety guidelines

This section contains warnings and important safety guidelines for using the HDI Remote Server. Read and understand the information in this section before removing, replacing and installing system components.

This section includes the following key topics:

- Precautions for using the HDI Remote Server

Precautions for using the HDI Remote Server

- 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 might occur.
- If you notice unusual smells, abnormal heat generation, or smoke emission, shut off the power feed to the equipment and inform the maintenance engineer. Leaving such conditions unattended might 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 might cause an electric shock, fire, 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 might occur.
- Putting heavy material on the equipment might result in an injury or failure due to falling.
- Do not put any heavy material on the equipment. The HDI Remote Server might not operate normally.
- Do not put a vessel with water or a tiny metallic item such as a paper clip on the HDI Remote Server. If the water or the item falls into the HDI Remote Server and the HDI Remote Server is running, an electric shock, smoke, or fire might occur.
- Route cables so that they do not catch your feet.
- Getting your feet caught by cables can cause personal injury.
- Do not put any heavy material on the cables. 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 might occur because the insulation will be deteriorated.
- Make sure that no foreign particles are stuck on the power plug and then insert it securely into the power socket.
- Remove such foreign particles if they are found because since they can cause a fire. Improper insertion will cause an unexpected plug slip-out, resulting in the 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 objects 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 a clip or any combustible material such as paper into the equipment from the air vent. It might cause an electric shock or fire.
- When a failure occurs in the HDI Remote Server, take action according to this guide in order 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 a high reliability system heavily influencing life and property, this product cannot be used and is not guaranteed. Examples of high reliability systems that are inappropriate for using this product include chemical plant control, medical equipment control, and urgency communication control.

1

Introduction

This chapter provides an overview of the role names and job descriptions used with the HDI Remote Server, and also a flowchart to guide you through installation and setup.

This chapter covers the following key topics:

- ☐ Roles and job descriptions

Roles and job descriptions in this guide

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

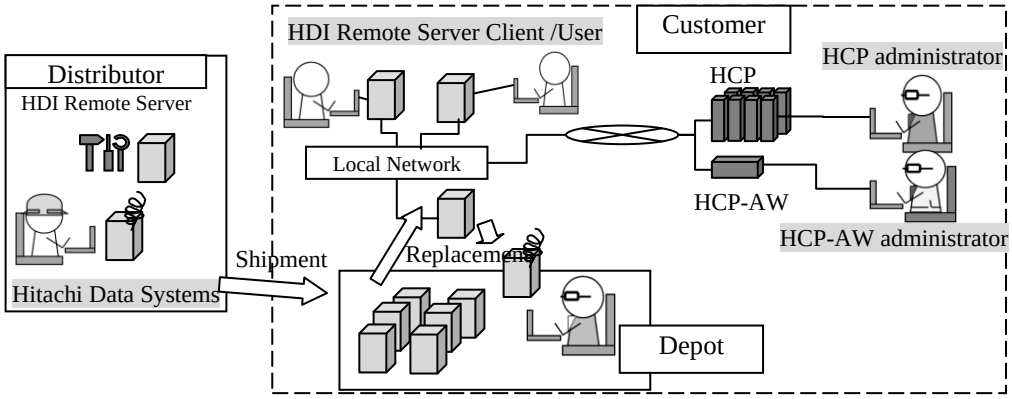


Figure 1-1: Image of each administrator

Table 1-1: Job description of each person in Figure 1-1

#	Role name	Description
1	Hitachi Data Systems	Distributor who assembles and ships HDI Remote Server.
2	Depot administrator	Administrator who ships HDI Remote Server for replacement.
3	HCP-AW administrator	Administrator who refers to this guide. Administrates HCP Anywhere (HCP-AW hereinafter). They manage the HCP-AW and HDI Remote Server information. They also manage the network server in the client/user environment if required.
4	HCP administrator	They manage the HCP totally.
5	HDI Remote Server Client/User	HDI Remote Server user who reside in each location.

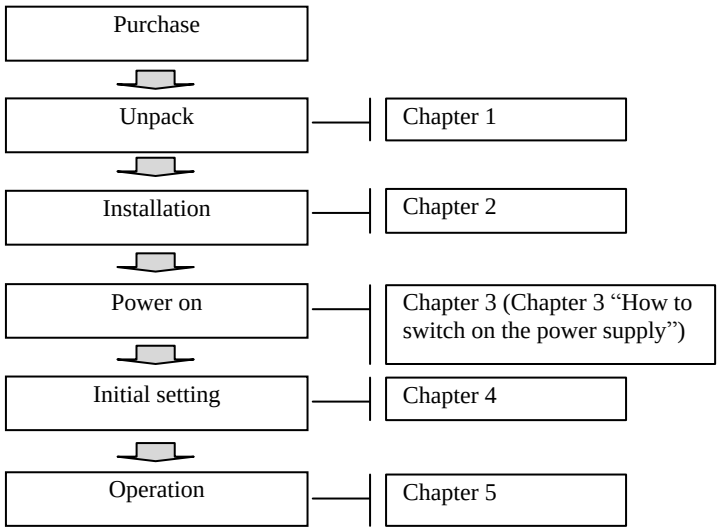


Figure 1-2: Introduction flowchart

2

Installation

The installation procedure is described in this chapter. When the HDI Remote Server arrives at the site, open the box and begin installing the system according to the instructions in the Quick Reference Card.

This chapter covers the following key topics:

- ☐ Installation location
- ☐ Connecting cables

Installation location

The HDI Remote Server should be installed in a controlled environment where heat and humidity are maintained at a constant level.

Connecting cables

Basic Configuration

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

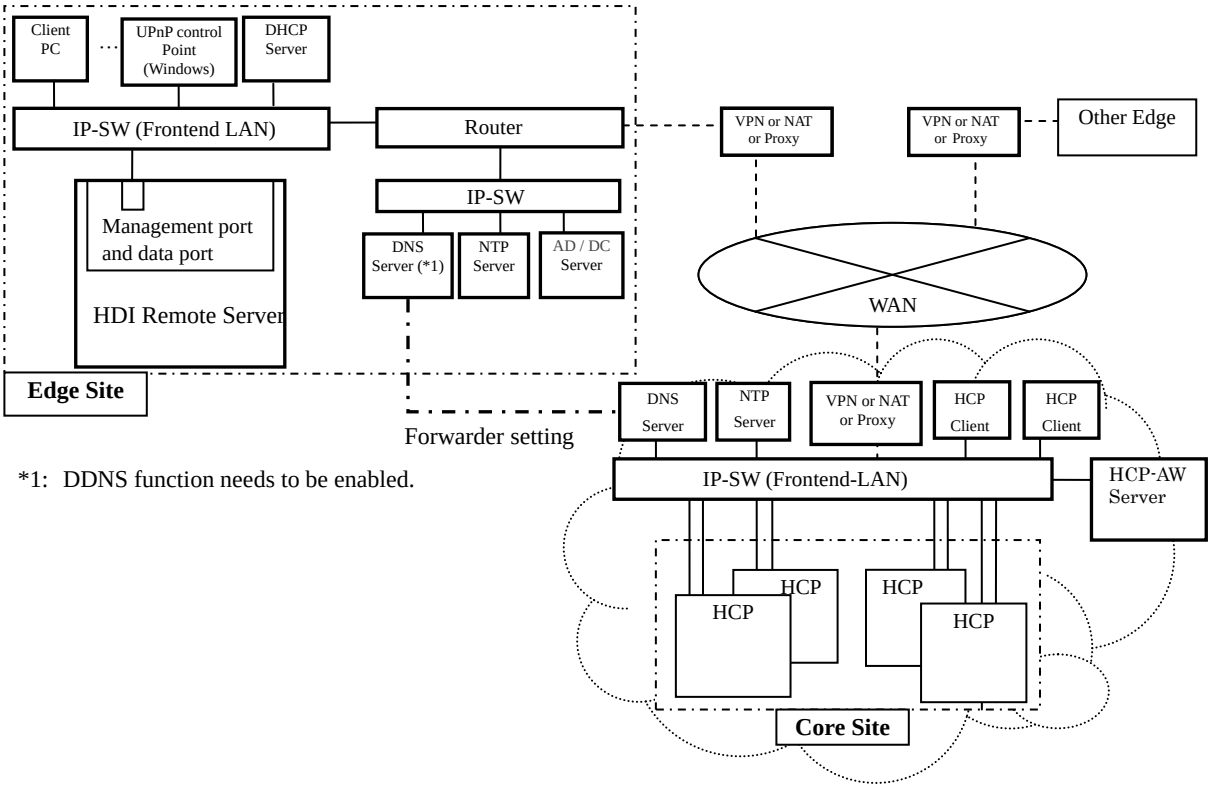
Note that the Edge Site and Core Site are linked through WAN.

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 both the 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 if the 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 2-1: Example of network configuration

During the initialization/setup process, HDI RS communicates with HCP Anywhere (HCP AW). HCP AW is the central management point for all HDI RSs. HCP AW also acts as a central reporting and monitoring platform for HDI RS. Once HDI RS setup is completed it starts communicating with HCP and replicates the data stored locally.

Connect each cable

For the cable connections, refer to the rear view of the Quick Reference Card.

(1) Connect the power cable to the HDI Remote Server.

(2) Connect the HDI Remote Server to the LAN via the LAN cable.

LAN interface specifications

Before setting the IP address, choose either setting through DHCP or setting fixed IP address in advance. If you use a fixed IP address, set it prior to the Provisioning. For the negotiation mode and MTU, see below.

Correct settings between devices which connect to the node are required. For the connection settings of IP-SW, refer to the table shown below.

Table 2-2: LAN interface setting

Port	IP address		Negotiation mode	MTU
	IPv4	IPv6		
Management port and data port	Y (mandatory)	-	Auto Negotiation	1500
Y=Supported, -= Non 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.

Port to be used

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

Table 2-3: Ports used by a node

Port number	Protocol	Service name	Description	Direction of transmitting and receiving data ("Transmit a request from "RS→"=HDI Remote Server, and receive a request from "→RS"="HDI Remote Server.			
				HDI RS and HCP-AW	HDI RS and HCP	HDI RS and peripheral server (AD/DC/DNS/NTP, etc. (CoreSite side))	HDI RS and User`s PC
22	tcp	ssh	Used for ssh				
53	udp	DNS	Used for DNS			RS→	
67	udp	DHCP	Used for DHCP			RS→	
68						→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→	
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	Connection-less 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→		
445	tcp	Direct Hosting of SMB	Used for the CIFS service via Direct Hosting of SMB			RS→	→RS
464	udp/tcp	kpasswd	Used to join in a domain or change the user password in an Active Directory environment			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				
2049	udp	nfsd	Used for file shares by NFS				→RS
4045	udp/tcp	lockd	Used for region locks on file shares by NFS				→RS
600 ~ 1023	udp/tcp	rquota	Used for file shared by NFS				→RS
8005	tcp	tomcat	Used for Tomcat shutdown				
8443	tcp	tomcat	Used for communication with Tomcat by HTTPS				
15000~ 15019, 19012	udp/tcp	Data Management	Used for Replication management port 0				
32768 ~ 61000	udp/tcp	mountd	Used for file shared by NFS				→RS
32768 ~ 61000	udp/tcp	statd	Used for region lock shared by NFS				→RS

Table 2-4: Ports used by the administrative terminal (web browser)

Port number	Protocol	Service name	Description	Direction of transmitting and receiving data ("Transmit a request from HDI Remote Server ="RS→", and receive a request from HDI Remote Server="→RS".			
				HDI RS and HCP-AW	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				

3

Power supply operation

This chapter describes how to switch on and off the power supply. The following key topics are covered:

- ☐ 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

Perform the following steps to switch on the power supply.

1. Confirm that the power cable is connected.
2. Check the location of the power switch referring to the Quick Reference Card.
3. After confirming that power to each server is switched on, referring to the Chapter 4 section, *Confirmation points before initial setting* of this document, press the power switch.
4. Confirm that the power LED is on.

If power is not turned on, see FAQ.

How to switch off the power supply

Perform the following steps to switch off the power supply.

1. Press the power switch.
2. Confirm that the power LED is off.

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

How to switch off the power forcibly

Press and hold the power switch for 3 to 4 seconds to turn the system off. Confirm that the power LED is off.

4

Initial setting

This chapter describes how to perform the initial setting. The following key topics are covered:

- ☐ Confirmation points before initial setting
- ☐ Perform initial setting
- ☐ Confirming report notification
- ☐ Updating software

Confirm the following before initial setting

- When using the DHCP server, confirm that the DHCP server is booted and that the settings have also been completed.
- When using the DHCP server, confirm that the DNS server is booted and that the settings have also been completed.
- When using the DHCP server, an administrative terminal, which is corresponding to UPnP, is required. Confirm that the administrative terminal is corresponding to UPnP and that the function is enabled.
- Confirm that power to the HCP and HCP-AW, which manages the data of the HDI Remote Server, is switched on.
- Confirm that the HDI Remote Server is connected to the environment in which HCP and HCP-AW, which manages the HDI Remote Server data, is used.
- Confirm whether a user can check the HCP-AW account information (credentials which entered into Provisioning Wizard).
- Confirm that the items to be set to HDI Remote Server have been registered in HCP-AW.

Perform initial setting

For the initial setting, use the Provisioning function.

At the time of the initial installation and after the node replacement, perform the settings using the Provisioning function under the instruction of a HCP-AW administrator.

The HCP-AW administrator determines whether a software update is necessary after using the Provisioning function. Execute the installation if necessary.

When not using the DHCP server, use the Provisioning function after setting the fixed IP address.

When using the DHCP server, follow procedure (1). When using the fixed IP address, follow procedure (2).

1. When using DHCP

   a) Confirm that the HDI Remote Server, HCP-AW and DNS server, etc., are running.

b) Open the network of the administrative terminal (Control Point) and start the HDI Remote Server icon shown in the Other Devices.

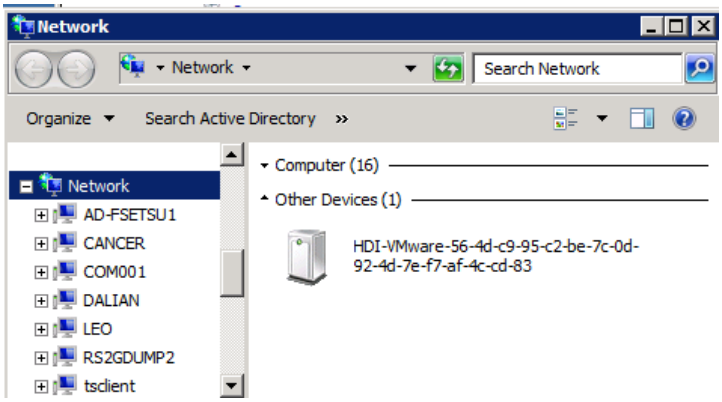


Figure 4-1: Booting GUI on HDI Remote Server

Tip

If the HDI Remote Server icon is not found in the administrative terminal.

Resolve the problem referring to FAQ (Network FAQ).

If the retrieval of the address on the DHCP server has failed, the default IP address might have been set. To change to the configuration using the fixed IP address, directly connect the administrative terminal with the HDI Remote Server through the network and follow the procedure (2) to configure from the fixed IP address.

(go to 2, or see network FAQ)

---

c) Refer to the Quick Reference Card to log into the management GUI. When logging into the management GUI, the HDI Remote Server GUI password change dialog will open (first time only).

d) When the change of the initial password has completed, the Provisioning Wizard will start.

e) When the introduction window is displayed for the first time, read the description, and click [Next].

f) When the Provisioning Settings window is displayed, input the URL of HCP-AW server and password, which should have been provided in advance by the HCP AW administrator. Execute the setting of the Proxy server if necessary.

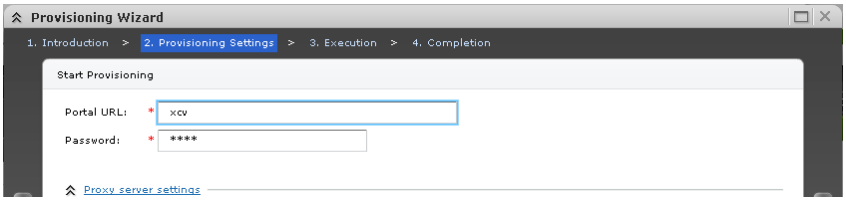


Figure 4-2: Provisioning Wizard window 1

Then press the [Next] button.

g) When the confirmation window is displayed, confirm the setting of Portal URL and press the [Next] button. The HDI Remote Server will retrieve the configuration information from the HCP-AW server.
h) A progress window is displayed. When each process reaches 100% and "Completed" appears, then the configuration is complete.
i) When the setting has completed, go to the Chapter 6 section, *Confirming report*.

2. When using the fixed IP address.

If the DHCP server is not used, execute the setup referring to the following procedure. The HCP-AW administrator should execute the following procedure from (a) to (i) before distributing a node. Then execute the rest of the procedure following (i) after distributing a node on the spot.

a) Confirm that the HDI Remote Server is running.
b) Link the administrative terminal (Control Point) and HDI Remote Server directly. Set the segment of the administrative terminal to be able to connect to "169.254.1.100", and then the netmask set to 255.255.0.0.
   For example, Assign IP address: 169.254.1.99, Netmask: 255.255.0.0, Gateway: (None)
c) Access to HDI Remote Server with the default IP address (169.254.1.100) in the Web browser.
   For example, URL: https://169.254.1.100/admin/

   User ID: admin

   Password: chang3me!
d) The HDI Remote Server login window is started. Log into the management GUI. When logging into the management GUI, the HDI Remote Server GUI password change dialog will open (first time only). Make a note of the changed password.
e) Introduction window and Information are displayed. Read the description, and press [Next].

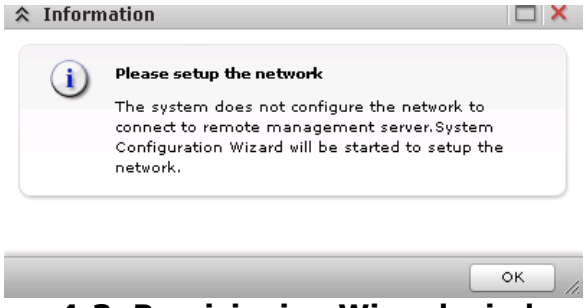


Figure 4-3: Provisioning Wizard window 1

g) Select [Setup Network], shown on the lower side of “Provisioning Settings” window.

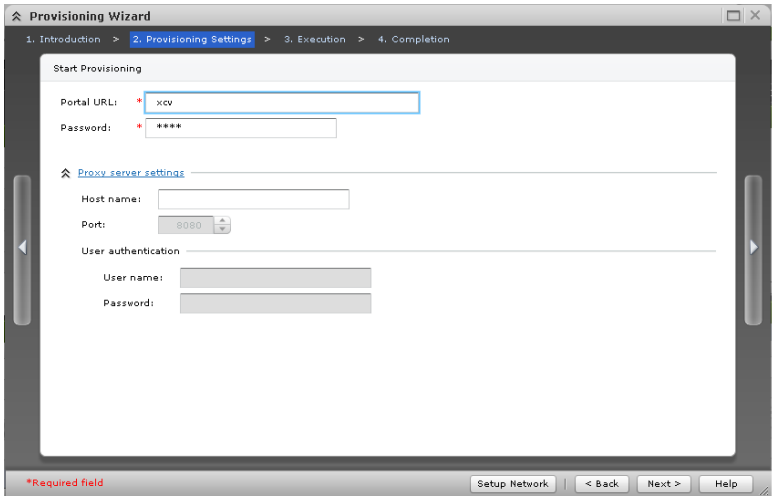


Figure 4-4: Provisioning Wizard window 2

h) Uncheck the checkbox “Yes” next to “Use DHCP” and enter the fixed IP address, netmask, default gateway, DNS server address and NTP server address. Then press [Next].

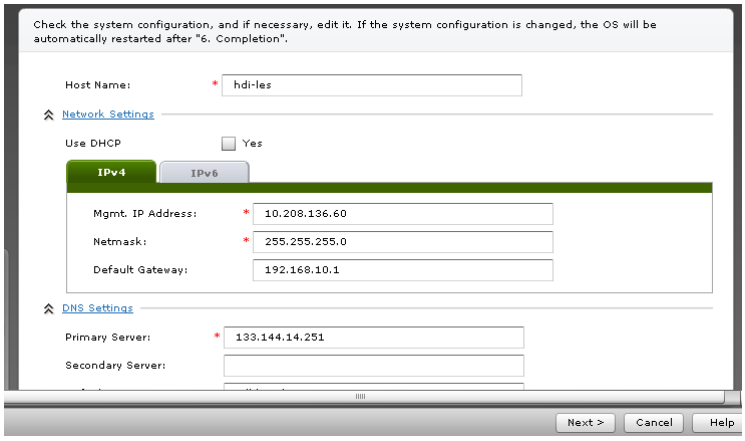


Figure 4-5: System Configuration Wizard window 1

i) When the confirmation window appears, confirm the contents and place a check in the checkbox shown on the lower side of the window. Then press the [Apply] button. The system reboots automatically after the progress window shows the completion of the network configuration.

Execute the following procedure after distributing a node.

j) Connect the HDI Remote Server to the network in the operation environment.
k) Set the segment of the administrative terminal (Control Point) to be able to connect to the HDI Remote Server, and connect the administrative terminal to the HDI Remote Server.

l) Enter the IP address that was set in step h, manually in the URL bar of the Web browser to get access to the HDI Remote Server again.

   For example, URL: https://<Mgmt. IP Address assigned in step(h)>/ admin

m) The HDI Remote Server login window is started and the Provisioning Wizard is booted when logging into the login window.

n) For the rest of the procedure, follow (e) to the last steps of procedure (1) "When using DHCP", shown above.

If Retry message is displayed, the Retry message may be output in the following cases, though particular operations are not required as the system executes Retry automatically.

- HCP-AW is in the Busy status.
- Timeout
- Service is not running.

A problem has occurred such as the HCP-AW is not found or an error has occurred while the Provisioning function is running, etc.

See *Chapter 6, Troubleshooting* to confirm FAQ (Initial installation FAQ).

Confirming report notification

After completing the settings using the Provisioning function, a Report will be sent from a node to the HCP-AW server. Confirm a Report and check that no failure occurs.

If a failure occurs, take appropriate action to resolve the problem referring to *Chapter 6, Troubleshooting* of this document.

Updating software

Log into the management GUI under and select "Software Update" from the [Resources] tab to update the software (see *Chapter 8, Updating software according to the request from a distributor*).

5

Overview and basic functions of HDI Remote Server

This chapter provides an overview and information about basic functions of the HDI Remote Server. The following key topics are covered:

- ☐ General overview
- ☐ Basic functions of HDI Remote Server

General overview

Data flow (Read/Write processing of client)

In the read/write processing in the Basic Configuration, which is not connected to the disk array subsystem, file read/write is performed for the internal HDD by the read/write requests from the client to the node.

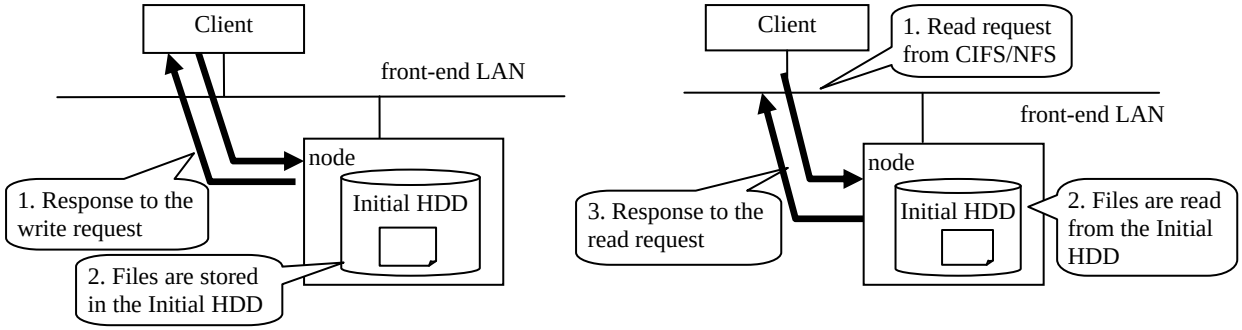


Figure 5-1: Flow of Write (left) / Read (right) processing

RAID configuration

Automatically determines the number of HDDs and configures RAID. In the case of 2 HDDs, RAID configuration will be RAID 1, and in case of the 4 HDDs, RAID configuration will be RAID 5.

An image of the LU configurations is shown below.

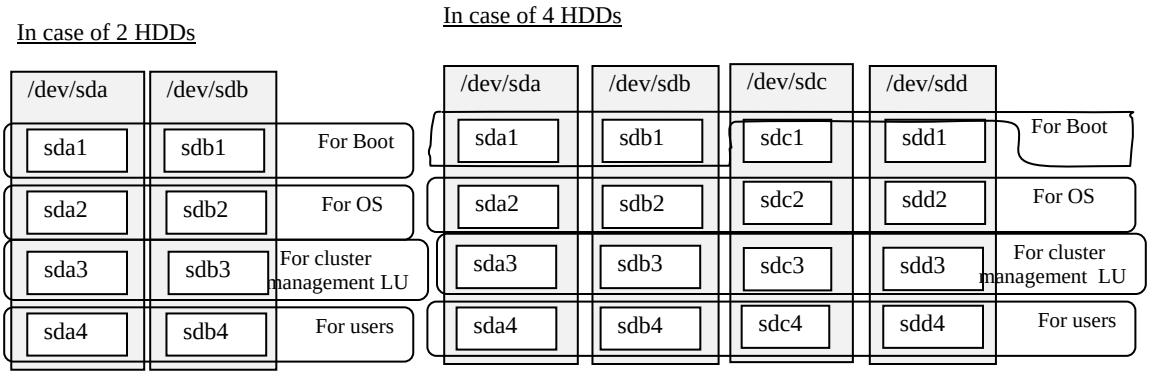


Figure 5-2: Image of RAID configuration

Resource group

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

Collaborating with HCP

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 replicated automatically to the HCP according to a replication policy.

The replicated 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 starts stubbing files regularly, if the free space of the file system is lower than the set value (Default: 10%), HDI selects WORM files and the old update files, and stubs them.

If HDI fails and the stub files are lost, the stub files can be restored from the data stored in the HCP.

Replication processing

The read/write processing in the single node configuration, and in the configuration of HDI for HCP / HDI for Cloud in the cluster configuration, includes replication and recall processing between HDI and HCP in addition to read/write from a client to HDI.

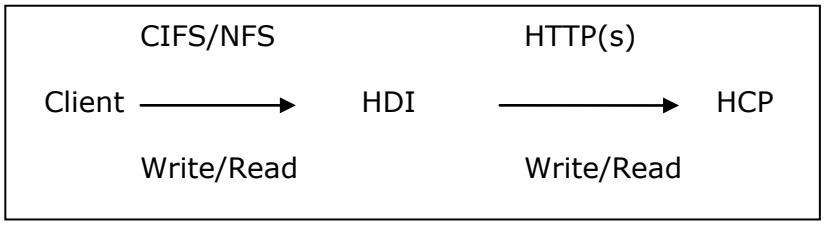


Figure 5-3: Replication processing

Recall processing

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

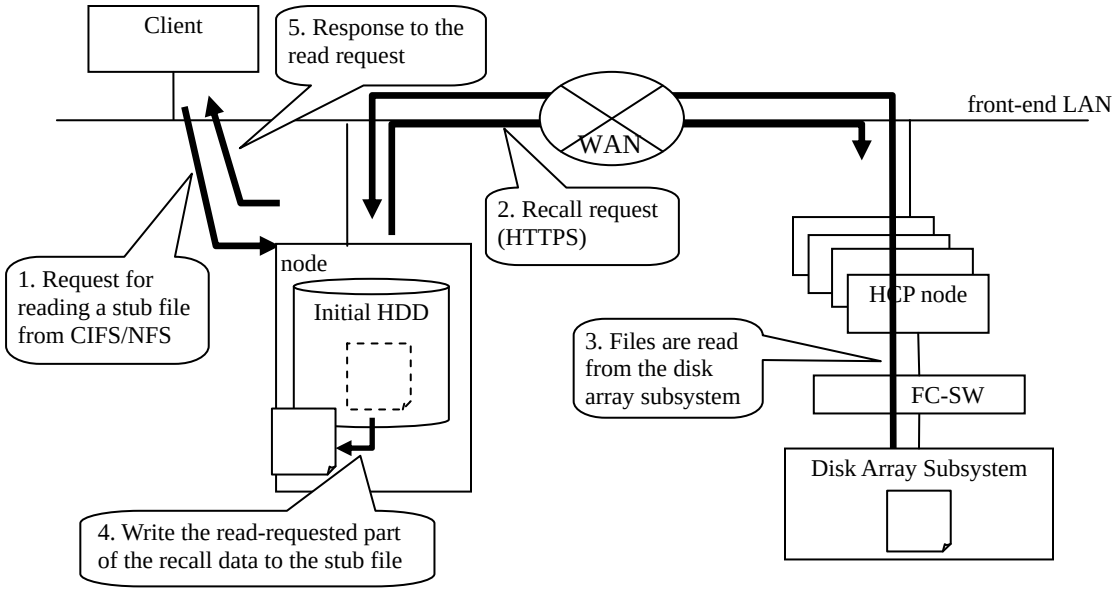


Figure 5-4: Recall processing

Considerations during 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 replication or recall processing fails. Figures 5-5 and 5-6 show the schematic figures of the failures.

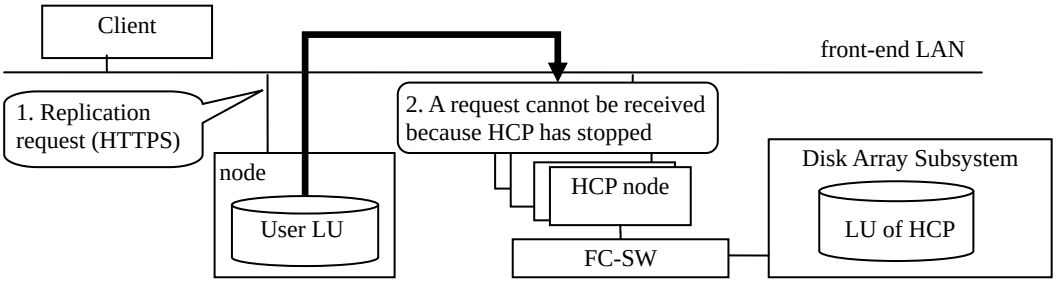


Figure 5-5: Replication Processing When HCP Stopped

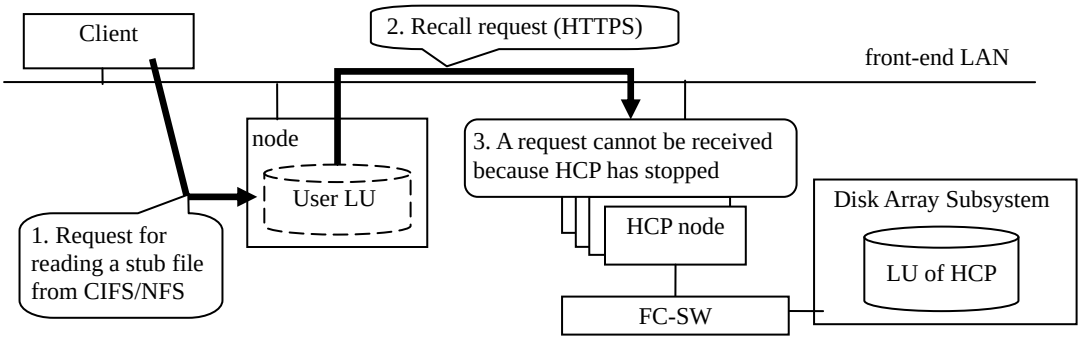


Figure 5-6: Recall Processing When HCP Stopped

Communication failure with HCP

In the configuration of HDI for Cloud, the Read/Write request from a client could fail because the communication is disconnected between HDI and HCP via WAN.

- It responds I/O error for the client.

Figure 5-7 shows an example of the recall operation when the WAN failure occurs.

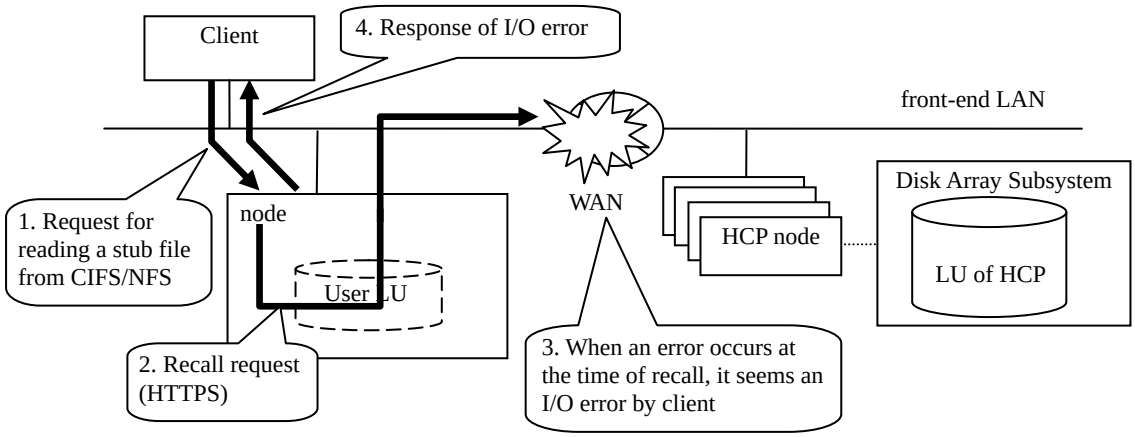


Figure 5-7: Operation When WAN Failure Occurs (Recall)

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 longer, but an I/O error still occurs, a network, hardware, or software failure might occur. In this case, determine the failure by following the procedure shown in *Chapter 6, Troubleshooting*.

Basic functions of HDI Remote Server

Provisioning function

Store the items to be set for HDI Remote Server on the HCP-AW in advance by referring to the HCP-AW manual, and boot the Provisioning Wizard from HDI Remote Server, and execute. Then the settings, including the file system, network, and each service are downloaded from HCP AW to HDI Remote Server. HDI Remote Server will reboot automatically immediately after the Provisioning function. If the Provisioning function has failed, the Reconfigure function will execute the configuration setting.

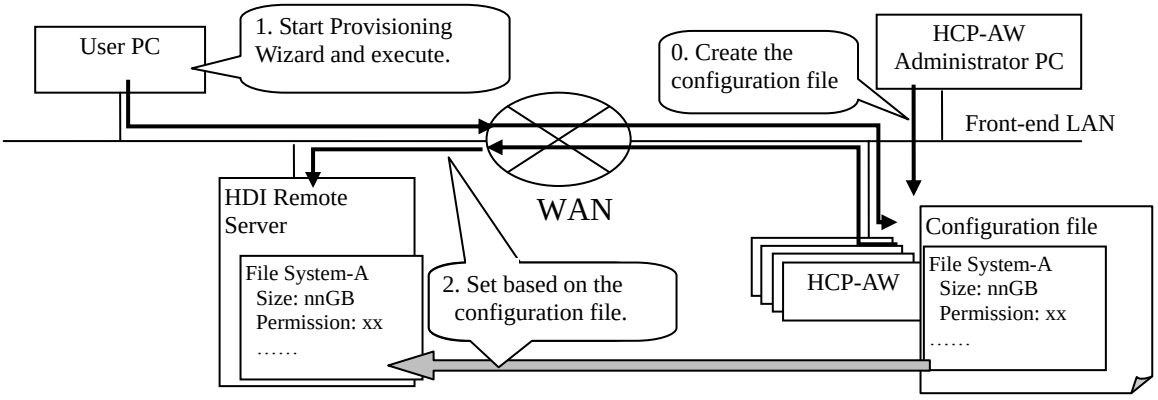


Figure 5-8: Overview of Provisioning function

Reporting function

This is the function to collect the configuration information and error information on a regular basis and send a report from HDI Remote Server to the HCP-AW.

If any emergency failure has occurred, notify the immediate error to the HCP-AW. Report is used to determine and recover from a failure. A sending report interval is configured by a HCP-AW administrator.

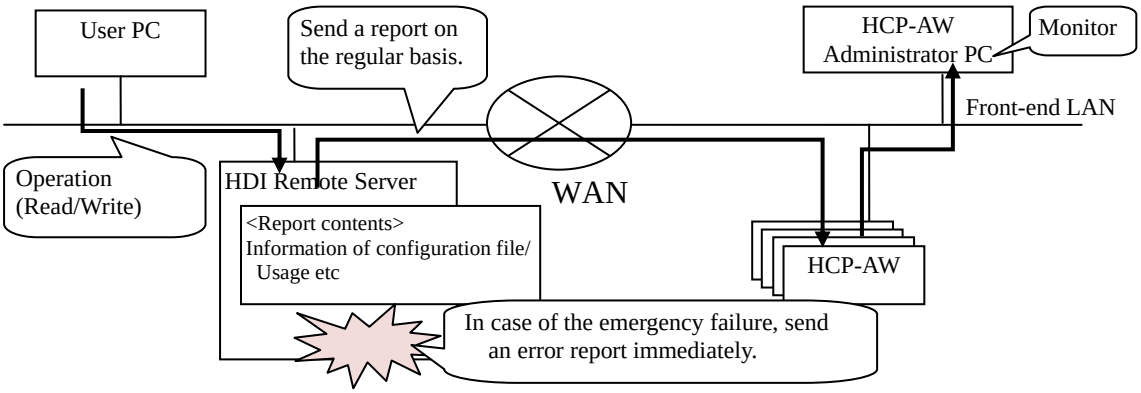


Figure 5-9: Overview of Reporting Function

In case of an emergency failure, an error message is displayed in the [Overview] tab that appears when the HDI Remote Server, which is desired to check on the Device page, is selected in the HCP-AW console. Also, the Report which is sent periodically can be checked using the [Health Report] tab, which appears when each HDI Remote Server is selected in like manner.

Reconfigure function

When the discrepancy of the configuration information is found between the HDI Remote Server and the record stored in HCP AW for this HDI RS in HCP-AW, this function reflects the discrepancy automatically to the HDI Remote Server as an extension of the Reporting function. If the configuration change, such as adding a file system during the operation, is required, use the Reconfigure function to change.

Even if the configuration information on HCP-AW was changed, Reconfigure is not executed until the next Report is exchanged.

If the change requires a system reboot, reboot the system shortly after the reconfiguration. If the reconfiguration has failed, execute the reconfiguration again after the next Report output.

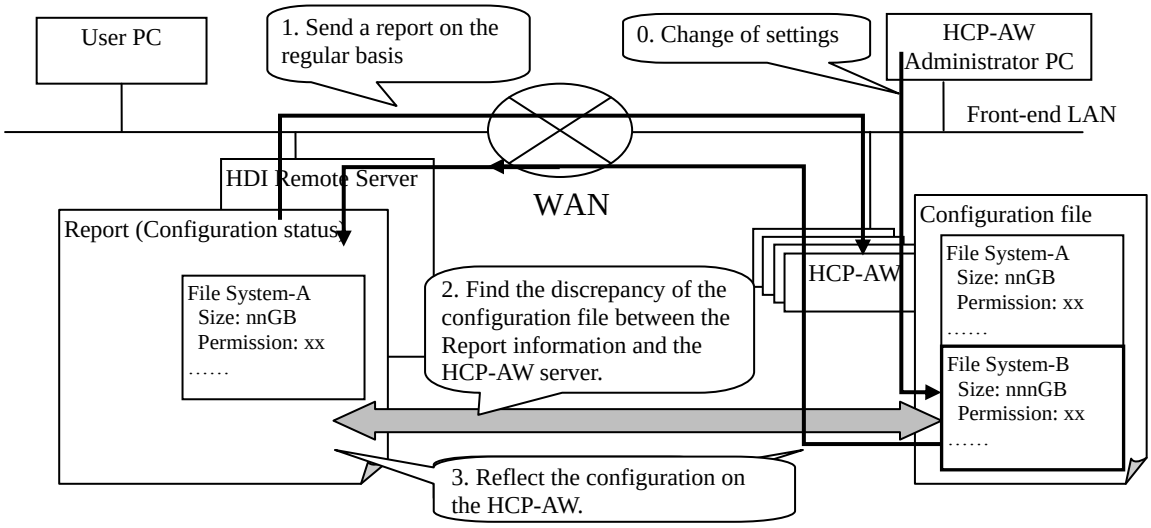


Figure 5-10: Overview of Reconfigure function

6

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 according to Finding a failure by users of this chapter to determine a failure and recovery.

If a failure occurred during installation of the 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 Report, take appropriate action and refer to the message confirmation table in this Chapter Message confirmation table.

Overview

An overview of the failure determination procedure is shown below.

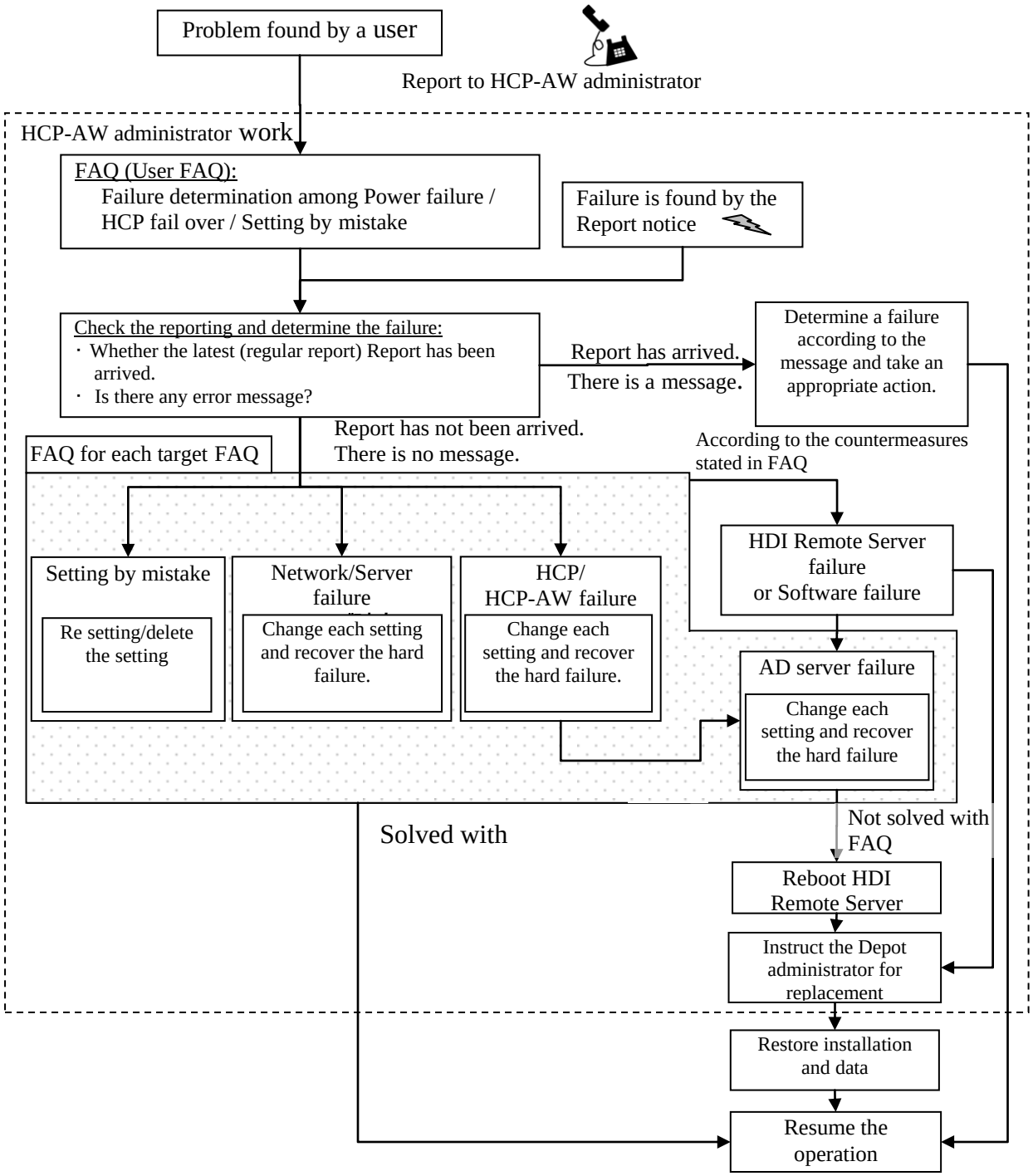


Figure 6-1: Overview of failure determination

Finding a failure by users

When a failure occurs during the HDI Remote Server operation, start the failure determination.
If any beep (memory error) or abnormal tone (hardware error) sounds, replace the node.
If an I/O error occurs, follow the failure determination procedure stated in the section *Checking FAQ*, below.

Checking FAQ (user FAQ)

1. Retry the system 20 minutes after the failure occurred. By waiting, the following temporary trouble may be restored.
   - I/O have not been executed due to the failover of HCP, which manages the data of the HDI Remote Server
   - Windows client IP address caching problem

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

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, the IP address is changed due to the reboot operation etc., and I/O may not be executed as a consequence.
   In this case, perform the following operations:
   - For the client using CIFS sharing, a particular operation is not required. (System will be recovered followed by the retry performed 20 minutes after the failure occurred as stated in (1), above)
   - For the client using NFS sharing, execute the mounting again.

3. Check that the power LED of the HDI Remote Server is turned on. If the power LED has been turned off, push the power switch. If the power LED is ON, proceed to the section *Confirming Report*. If the power LED is still OFF even if the power switch is pushed, check with the FAQ (Power FAQ) to determine whether any problem has occurred in the power supply system. After checking the FAQ (Power FAQ), confirm whether there is a problem with the items shown in Table 6-1. If no problem is found, place a check (or x) in the 'Place a check below' column. If all columns are filled, proceed to the section *Confirming Report*. If a problem is not resolved, even after checking the FAQ (Power FAQ), then there might be a hardware problem. Perform a node replacement based upon information in *Chapter 7, Replacement*.

Table 6-1: Confirmation table for power supply system

#	Confirmation Item	Place a check below
1	There is no problem with the power cable connection.	
2	Electricity is supplied to the HDI Remote Server.	
3	A power failure has not occurred.	

Confirming Report

1. A Report is delivered to HCP-AW regularly according to the set schedule. Confirm the periodic notification schedule (Default: 1h) of the Report which has been set using the Provisioning function.

2. Confirm that a report is delivered periodically.

   If a report is delivered, check the report and confirm that an error message is not output. If an error message exists, see Table 6-2, below.

   In case where an error message cannot be confirmed, and a report is not delivered periodically, it might be due to a problem with the network or server environment settings. Proceed to the section in this chapter, *Checking network environment*.

Message confirmation table

If a message, shown in the table below, is included in a report, take appropriate action. If a problem is not solved even after taking action, proceed to the section in this chapter, *Checking FAQ (AD server)*.

NOTICE There are two cases for the delivery time of an error message. The first case is an error message, which is delivered shortly after the failure occurs, and the other case is an error message that is delivered with the regular report. Therefore, sometimes an error occurrence time, and report notification time, may be different depending on the failure type.

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

In the “Action” items of the below table state “…wait for the completion of Reconfigure”, note that this “Reconfigure” will be executed at a maximum of 24 hour intervals.

Table 6-2: Failure recovery from Report notification message (1/3)

#	Code	Message	Detailed Code	Output display	Severity	Action
1	KAQX 10001	Internal disk failure. (slot ID =*ID-number,* status=*status*)	—	Alerts	–	Replace HDD or node (see Chapter 7 "HDD Replace procedure").
2	KAQX 10002	Active Directory authentication failure (*detailed info.*) **detailed info.*:cause	assignment of a new user-ID or group-ID failed	Major events	Error	1. Confirm and expand the configuration information on HCP-AW (UID/GID Range) and wait for the completion of Reconfigure.
3			Except #2			Execute the network (AD) FAQ.
4	KAQX 10003	NTP time-synchronization failure (*detailed info.*) **detailed info.*:cause	—	Major events	Warn	1. Execute the network FAQ. 2. Confirm and change the configuration information on HCP-AW and wait for the completion of Reconfigure.(automatically rebooted after the Reconfigure)
5	KAQX 10004	HCP communication failure(*detailed info.*) **detailed info.*:cause	—	Major events	Error	1. HCP-AW administrator should confirm and correct the configuration information on HCP-AW (HCP setting information: Settings for User name, password, tenant, name space) and wait for the completion of Reconfigure. 2. Execute the Network FAQ 3. Execute the HCP-FAQ
6	KAQX 10005	HCP versioning failure	—	Events	Error /Warn	1. Confirm and change the settings of the configuration information on HCP-AW (disk capacity) and wait for the completion of Reconfigure. 2.If the message "KAQX10004" has been output at the same time, take action according to the action stated in KAQX10004. 3. Switch off the power first and then switch on the power again.
7	KAQX 10006	Replication or stub-processing failure(*detailed info.*) **detailed info.*:cause	—	Major events	Error /Warn	1. Confirm and change the settings of the configuration information on HCP-AW (file system capacity) and wait for the completion of Reconfigure. 2. If the message KAQX10013 (file system is blocked) has been output, take an appropriate action. 3. If the problem was not solved, collect the logs and send.
8	KAQX 10007	User-data restoration failure (*detailed info.*) **detailed info.*:cause	—	Major events	Error /Warn	1. If the message KAQX10013 (file system is blocked) has been output, take appropriate action 2. If the problem was not solved, collect the logs and send.
9	KAQX 10008	Namespace-sharing synchronization failure(*detailed info.*)	Refer to Appendix 1	Major events	Error	Action to be taken will depend on the <detailed info>. See Appendix 1.

Table 6-2: Failure recovery from Report notification message (2/3)

#	Code	Message	Detailed Code	Output display	Sever-ity	Action
10	KAQX 10009	Service-start failure	—	Major events	Error	1. If the one of the following messages is output, take appropriate action accordingly. (KAQX10013 (blocking file system), KAQX10001 (HDD failure), KAQX10098(KAQG41010-E), KAQX10098 (KAQG41011-E),KAQX10098(KAQG41013-E)) 2. Switch off the power first and then switch on the power again. 3. If the problem was not solved, collect the logs first and execute the node replacement (see Chapter 7, “Replacement”)
11	KAQX 10010	Service-stop failure	—	Major events	Error	1. If the message KAQX10030 (Reconfigure error) has been output, take appropriate action. 2. Switch off the power first and then switch on the power again. 3. If the problem was not solved, collect the logs first and execute the node replacement (see Chapter 7, “Replacement”).
12	KAQX 10011	File system full(*detailed info.*) **detailed info.*:file system name	—	Major events	Error	1. If the message KAQX1006 (Replication error) has been output, take an appropriate action. 2. Confirm the configuration information on HCP-AW (file system capacity) and add the capacity. Then wait for the completion of Reconfigure.
13	KAQX 10012	File system nearly full(*detailed info.*) **detailed info.*:file system name	—	Events	Warn	1. If the message KAQX1006 (Replication error) has been output, take appropriate action. 2. Confirm the configuration information on HCP-AW (file system capacity) and add the capacity. Then wait for the completion of Reconfigure.
14	KAQX 10013	File system is blocked (*detailed info.*) **detailed info.*:file system name	—	Alerts	–	1. If the message KAQX10020 and KAQX10030 have been output concurrently, take appropriate action. 2. Switch off the power first and then switch on the power again. 3. If the problem is not recovered, replace a node. (see Chapter 7, “Replacement”)
15	KAQX 10014	A problem was detected in a fan. (fan_*fan-number*)	—	Alerts	—	Replace a node (see Chapter 7 “Replacement”). There is a danger of temperature increase. Stop the node immediately and switch off the node until a replacement arrives.
16	KAQX 10015	Inconsistent data was detected on the internal hard disk.	—	Alerts	—	Error occurred in the Consistency Check. Check the KAQX10098 message which was output concurrently first, and see the section in *Chapter 6, When finding the invalid data in Consistency Check.*
17	KAQX 10020	Provisioning failure (*detailed info.*)	See Appendix 2	Major events	Error	Confirm the configuration infornation on HCP-AW and execute the setting again. Then wait for the completion of Reconfigure. For the configuration information to be reviewed, see Appendix 2.
18	KAQX	Reconfiguration failure (detailed info.)	See Appendix 2	Major events	Error	1. Confirm the configuration infornation on HCP-AW and execute the setting again. Then wait for the completion of Reconfigure. For the configuration information to be reviewed, see Appendix 2. 2. If the failure is repeated, collect the logs and send.

Table 6-2: Failure recovery from Report notification message (3/3)

#	Code	Message	Detailed Code	Output display	Sever-ity	Action
19	KAQX 10098	Firmware failure (detailed info)	KAQG41010-E /KAQG41013-E	Major events	Error	See the section in *Chapter 6, Appendix A - When finding the invalid data in Consistency Check*.
20			KAQG41011-E/KAQG46531-E/KAQG46533-E	Major events	Error	Replace a node. (see *Chapter 7, Replacement*) However, if KAQG46531-E is contained in the message, the node could lead to a temperature rise. Stop using the node immediately and power off the node until a replacement arrives.
21			KAQM37246-E	Major events	Error	1. If the message KAQX10008 (Namespace-sharing error) has been output, take appropriate action. 2. Delete the Imported file system in the configuration information (file system information) on HCP-AW and wait until the Reconfigure is completed. When the deletion of the Report is confirmed, recreate an Imported file system and wait until the completion of Reconfigure. 3. If the problem was not solved, collect the logs and send to Hitachi Data Systems.
22			Other than #17 and #18, #19	Major events	Error /Warn	1. If the message KAQX10013 (File system is blocked) has been output, take appropriate 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 (see *Chapter 7, Replacement*).
23	KAQX 10099	Firmware failure (*detailed info*)		Events	Error	If the message other than KAQX10099 message has been output, take appropriate action. If the message has not been output, no action is required as the error may be temporary. However, if the error is not recovered more than one hour (recurrence), collect the logs and send to Hitachi Data Systems.

Appendix 1. Detailed Code of KAQX10008

#	Detailed Information	Severity	Action
1	automatic update failed	Error	1. If another KAQX10008 has been output, take an appropriate action. 2. If this error recurs even after waiting for a whole day, switch off the power and then switch on the power again. Then, wait for a few hours (interval between the data synchronizations). 3. If the problem was not solved, collect the logs and send.
2	HCP access failed		
3	invalid file system status	Error	1. If the message KAQX10013 (File system is blocked) has been output, take an appropriate action. 2. If the problem was not solved, collect logs and send.
4	acquisition of file attributes failed	Error	1. If the message KAQX10013 (File system is blocked) has been output, take an appropriate action. 2. If this error recurs even after waiting for a whole day, switch off the power and then switch on the power again. Then, wait for a few hours (interval between the data synchronizations). 3.If the problem was not solved, collect the logs and send.
5	authentication failed	Error	1.Check the HCP access account. 2. Collect a log and send with the information #1.
6	missing data	Error	1. In the HCP-AW console, confirm that the status of HDI Remote Server containing the file system of the import source is “Active”. If the status is not “Active”, change it to “Active”. 2. If this error recurs even after waiting for a whole day, switch off the power and then switch on the power again. Then, wait for a few hours (interval between the data synchronizations). 3. If the message KAQX10020 or 10030 message (“nfscreate”/ “cifscreate” is included in detailed info as the character fill (padding)) has been output, press [Save] without changing the configuration information and wait until the Reconfigure is executed again. 4. If the problem was not solved, collect the logs and send.
7	memory allocation failed	Error	1. If this error recurs even after waiting for a whole day, switch off the power and then switch on the power again. Then, wait for a few hours (interval between the data synchronizations). 2. If the problem was not solved, collect the logs and send.
8	invalid system status	Error	1. In the HCP-AW console, confirm that the status of HDI Remote Server is “Active”. (If the status is “Active (suspend)” or “Out of service”, it is not error.) 2. If the status of HDI Remote Server is “Active” and this message is output, confirm the message KAQX10008 has been output. If the message has been output, take an appropriate action. 3. If the problem was not solved, collect the logs and send.
9	insufficient free disk space	Error	Check the configuration information on HCP-AW (file system capacity) and execute the setting again. Then wait until the completion of Reconfigure.
10	invalid FQDN	Error	1. Execute the Network FAQ 2. If the problem recurs even after a whole day, switch off the power and then switch on the power again.
11	network error	Error	
12	name resolution failed	Error	
13	ACL type mismatch	Error	1. Collect the logs and send.
14	read-only file system	Warn	

Appendix 2. Detailed code of KAQX10020/10030

#	Detailed info.(*1)	Point to be reviewed for setting and countermeasure
1	keyword=*aaaaa*, id=*yyyynnnnn-z* (Determine the point to be reviewed by referring to the information in "*aaaaa*")	
2	archcpset	Configuration -> HCP
3		Filesystems -> HCP Replication Schedule
3.	archcpdel	Configuration -> HCP
4.	arcrestore	Reviewing the configuration information on AW is not required. Replace a node. 1 Try to replace of the same node. (-> see the Chapter9. "Node replacement − Replacing same node") 2. If the problem was not solved, replace a node.
5.	cifscreate	Filesystems -> Shares Filesystems -> Import
6.	cifsdelete	Filesystems -> Shares Filesystems -> Import
7.	cifssvauthset	Configuration -> Authentication
8.	cifssvdefset	Configuration -> Services
9.	cifssvumapset	Configuration -> Authentication
10	cifssvset	Configuration -> Services
11	dir*xxxxxx*	Filesystems -> Shares
12	dhcpset	Configuration -> Network
13	dnsset	Configuration -> Network
14	fsdelete	Reviewing the configuration information on AW is not required. (If this message is output continuously, a file system may be the WORM File System and it might not be able to be deleted (WORM file which is in the Retention term). However, it will not be a problem as the target File System will be deleted automatically in the next Reconfiguration once this WORM File System gets ready to be deleted.)
15	fsexpand	Filesystems -> Cache Size
16	fsxxxxxx other than fsdelete and fsexpand	Filesystems
17	hostnameedit	Configuration -> Network
18	if*xxxxxx*	Configuration -> Network
19	licenseset	Reviewing the configuration information on AW is not required. Press [Save] button without changing the configuration information and wait for the next Reconfiguration.
20	nasreboot	Reviewing the configuration information on AW is not required. Press [Save] button without changing the configuration information and wait for the next Reconfiguration.
21	nfscreate	Filesystems -> Shares Filesystems -> Import
22	nfsdelete	Filesystems -> Shares Filesystems -> Import
23	*xxxxxx*policy	Filesystems -> HCP Replication Schedule
24	prsreportingctl	Configuration -> Reporting
25	route*xxxxxx*	Configuration -> Network
26	sv*xxxxxx*	Configuration -> Services
27	sysluscheduleset	Reviewing the configuration information on AW is not required. Press [Save] button without changing the configuration information and wait for the next Reconfiguration.
28	timeset	Configuration -> Time
29	invalid configuration *(bbbbb)*	*bbbbb* (Determine the point to be reviews by referring to the information in character fill (padding). The reason why this character fill (padding) was determined as the invalid configuration information is filled. Review the configuration referring to the character fill (padding). ex. "invalid host name", "reduced file-system size"....)

30	Processing was interrupted.	Review of the configuration information on AW is not required. Press [Save] without changing the configuration information and wait until the Reconfigure is executed again.

*1: *xxxxxx* will be the convenient character strings.

Checking network environment

Check the following confirmation items. If no problem is found, place an x or check mark in the check column, and when all columns are filled, determine that there is no problem with the network environment and proceed to the following section, *Confirming HCP status*.

If the check columns are not filled, check the FAQ (Network FAQ) and confirm that there are no mistakes with the server settings.

Table 6-3: Checking network environment

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

Confirming HCP status

See the GUI in HCP, which manages the HDI Remote Server data, and confirm that any failure or failover has not occurred. If a failure occurs, take appropriate action according to the table below.

Table 6-4: 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 occurring)	- When the status is normal.	Proceed to the section, *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 ActiveDirectory has been operating, and is set normally.

If I/O by a user cannot be recovered, proceed to the section, *Rebooting HDI Remote Server*.

Rebooting HDI Remote Server

Since the problem might be solved, reboot the HDI Remote Server twice.

If the problem has not been solved yet, proceed to the next section, *When a problem is not solved*.

When a problem is not solved

Collect logs. Then send an alternate device to replace the failed HDI Remote Server.

For the log collection method, see the section, *All Log collection procedure*. And for the node replacement procedure, refer to *Chapter 7, Replacement*.

All log collection procedure

Collect log information and contact HDS Support.

To collect a log from a user PC, follow the procedure below. Note that a few log files are archived with "tar" and downloaded in the zipped format (gzip).

1. Start the management GUI and login to the system (see *Chapter 5, Overview and Basic functions of HDI Remote Server*)

2. Click "Action menu" in the Global menu, and select [Download All log].

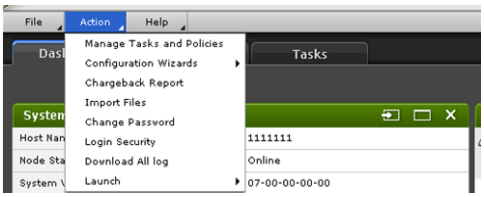


Figure 6-2: Action Menu window

3. Open the new window and "In Progress" window appears. Once the log collection is finished, a log collection completion window is displayed and [Download] button is activated. If you push [Download] button, the window in which you specify the destination to save a log, is output. Then specify the destination to save, and click [Save].

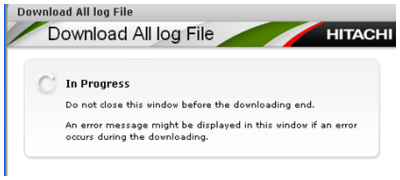


Figure 6-3: In Progress window 1

4. When log file is downloaded, the progress window is displayed.

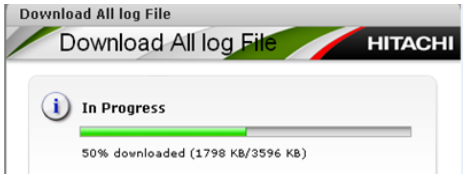


Figure 6-4: In Progress window 2

When the progress reaches 100%, download is complete. A button on the bottom-right corner is changed to [OK]. Click [OK], and close the window.

5. Make sure that a file named "Alllogdata_<serial number> _<date and time>.tar.gz" is created in the destination to save specified in the above step 3. Attach the log file to an email and sends it to a HCP-AW manager.

Appendix A - When finding the invalid data in Consistency Check

This section describes the countermeasures when a HCP-AW administrator finds invalid data.

Messages of invalid data:

- "KAQX10015 Inconsistent data was detected on the internal hard disk."
- "KAQX10098 Firmware failure (KAQG41010-E)" (M98 (KAQG41010) hereinafter)
- "KAQX10098 Firmware failure (KAQG41013-E)" (M98 (KAQG41013) hereinafter)

When finding invalid data

Concept

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

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

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

Table 6-5: Countermeasures

#	Countermeasure (*1)	Status after taking countermeasure
1	Execute the node replacement	Invalid data is resolved.
2	Execute the overwrite of the replicated data	An error is output to Report continuously as the failure remains. (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 this seldom happens).

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

When invalid data is found, see the following procedure and examples, below.

Execution procedure

1. Check whether M98 (KAQG41010) and M98 (KAQG41013) are output in the daily Report.
2. If a report of M98 (KAQG41010) or M98 (KAQG41013) is confirmed, you should arrange for a node replacement.

Overwrite the corrupted file with the past replicated "Normal data" before starting the node replacement.

Check whether the corrupted file is found, which was updated after the latest daily Consistency Check. If the corrupted data file is found, check the replicated data in the past and overwrite a corrupted data with the "Normal data". The most suitable data to overwrite a corrupted file is the file of the previous date rather 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), continue to monitor a Report. Invalid data message will not be issued if a node was replaced. If the overwrite of the past replicated data was executed, confirm that "M98 (KAQG41013)." is not output in Report until the node replacement is executed. If a message is output, execute the above procedure (2), again.
4. Replace the node when the new hardware arrives.

NOTICE	After checking the user data, leave it alone for a whole day (to allow time for the data to replicate), and replace the node. Data will be restored to the last replicated data point after the node replacement.

Execution example

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

[Assumed scenario] (Replication Schedule: once a day. Consistency Check: Twice a week (Tuesday and Friday), Retention period of the replicated 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 a user. Since the normal replicated data in the past may be gone, instruct a user to visually check the file and overwrite with a normal file and replicate.

Table 6-6: Example of recovery procedure when invalid data occurs

(Abbreviation in the HDI Remote Server event: C.C.= Consistency Check, M(data_mmdd)=Replication (data_backup-date))

#	Date	Time	HDI Remote Server event	Report notification/Action by AW 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, no need to report to HCP-AW)		↓
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 M98 (KAQG41010) is confirmed. Report to a user if this message is output. Start to arrange for HDI Remote Server change.		↓
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 last good file from data_0505 and over write.*1	↓
13.	5/12 (Tue)	1:00	M(data_0512)	(Normal data as a user data is replicated (assumption))		↓
14.		2:00	C.C. start			↓
15.		14:00	C.C. end	Report: Confirm that "M98 (KAQG41013)." 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 last good file from data_0512 and over write.	↓
18.	5/14 (Thu)	1:00	M(data_0514)	(Normal data as a user data is replicated (assumption))		↓
19.	…(HCP-AW administrator should keep monitoring Report until a node is arrived at the user side. If "M98 (KAQG41013)." was output in Report, execute the step #17 in the procedure. If "M98 (KAQG41013)." was not output, no operation is required.)…					↓
20.	5/21 (Thu)	1:00	M(data_0521)	(Repeat the overwrite and normal data is replicated)		↓
21.		9:00 -			HDI Remote Server is arrived. Notify to HCP-AW administrator.	Stop/Replace
22.				Operate GUI in the AW console after notified by a user.		↓
23.					Replace a node (+ "data_0521" is automatically restored)	↓
24.						Resume

*1: Sometimes data which was replicated 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 replicated on the date closer to the normal completion of the Consistency Check.

7

Replacement

This chapter contains information about replacement procedures.

Node replacement procedure

If a node replacement is required according to the failure determination process, then replace the node.

When replacing a node, follow the procedures below.

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

If the failed HDI Remote Server is still within the warranty period, a Depot administrator 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.

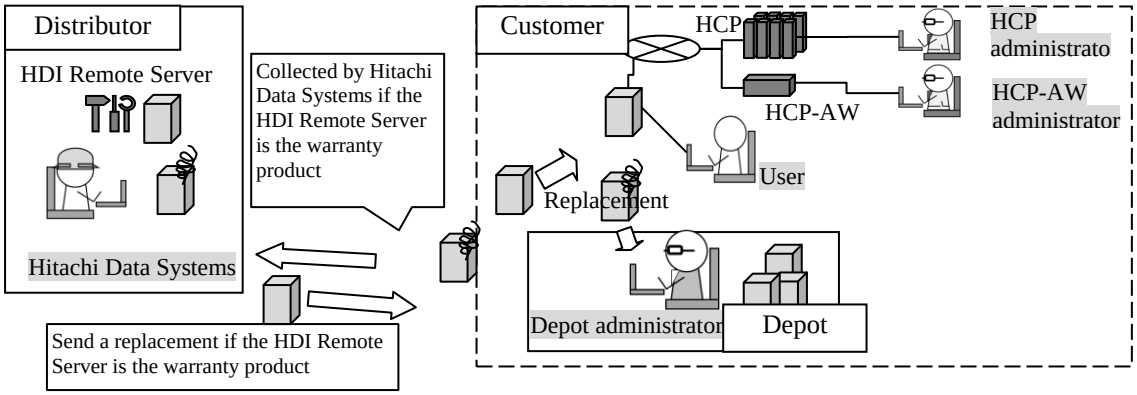


Figure 7-1: Replacement flow

Disconnecting older HDI Remote Server from the environment

1. Switch off the power if the power LED is on.
2. After confirming that the power is off, remove each cable.
3. Send the replaceable HDI Remote Server to the depot administrator.

Operation for node replacement

- Confirm a new HDI Remote Server serial number before shipment.
- If the node to be replaced is using the fixed IP address, then set the IP address. Confirm that the expected IP address has been set to a node.

1. Confirm that the new HDI Remote Server (Serial number) has been registered in the HCP-AW management console, and the status is "Available" by referring

to the HCP-AW manual. If the HDI Remote Server has not been registered, register it.

2. Perform the HDI Remote Server replacement by operating "Replace control" in the HCP-AW management console, referring to the HCP-AW manual.

Enter the password used to register the new serial number needed for the Provisioning, and make a note of it.

3. If the fixed IP address is being used, then distribute after setting the IP address to the new HDI Remote Server. For details about the IP address setting method, see *Chapter 4, Initial setting - Performing initial setting*, step (2), (a)-(i).
4. Once the HDI Remote Server arrives on site, confirm the label and serial number(s) with the billing information.
5. Connect the new HDI Remote Server to the network environment, referring to the Quick Reference Card.

   In the 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.
   - Make a host name of the new access destination known to a user who executes Provisioning.

6. Execute Provisioning. If DHCP is being used, follow the instructions according to the section in *Chapter 4, Performing initial setting*, step (1). When using the fixed IP address, execute the procedure according to the section in *Chapter 4, Performing initial setting*, step (2)(k). Then, the data replicated on the HCP is restored on the HDI Remote Server automatically.
7. After confirming that the Report is delivered, execute the OS update installation. If necessary, see *Chapter 8, Updating software according to the request from a distributor*.
8. Confirm that the I/O was executed successfully.

- 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 the case of using the shared CIFS and DHCP, let users know the host name of the destination access of the replaced node.
- If the local user was registered before replacement, the local user needs to be registered again.

If I/O was not recovered, proceed to *Chapter 6, All Log collection procedure* to collect All Log, and send.

Replacing the same node

Note: Replace cannot be performed by specifying a chassis with the same serial number on the management console of HCP-AW.

1. Register the dummy HDI Remote Server (serial number), and change the status "Available" referring to the HCP-AW manual.
2. Operate the management console of HCP-AW ("Replace control"), and replace the original node with the dummy node, referring to the HCP-AW manual.

Note: Password will be issued at this time, though there is no need to let a user know as it will not be used.

3. Open the management GUI of the original node. Move the cursor to the password input fields in the login screen, and execute "Factory Reset" (Press <Ctrl+ Alt+ J >) in accordance with the execution window. The HDI Remote Server power will be turned off when "Factory Reset" is finished.

Note: Do not manually power-off the system during the factory reset operation.

4. Execute the operation to move the original console to the Inventory tab on the management console of HCP-AW. Additionally, replace the dummy HDI Remoter Server with the original node.

Note: The password which was issued this time will be required for Provisioning. Make a note of the password.

5. Turn on power to the HDI Remote Server. Once power is turned on, log in using the simplified GUI, and perform Provisioning by entering the URL of HCP-AW, and the temporary password obtained in the previous step, (4) above.
6. Overwrite the HDI Remote Server (serial number) of the dummy node from the management console of the HCP.

Note:
- For the client operating DHCP, as well as using the NFS sharing, mounting is required after stopping the access and unmount the sharing.
- If the local user has already been registered before replacement, registration of the local user is required.

HDD replacement procedure

If a HDD failure message was included in a report, replace the HDD after checking the OS status. For the detailed procedure, see below.

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

1. Confirm that the OS status is up (determine this by checking whether you can access the HDI Remote Server) and check the following messages, which indicate HDD failure in the report.

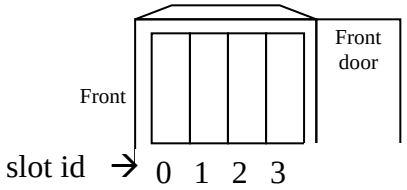
In the following cases, a node needs to be replaced. (See section *Node replacement - Operation for node replacement*)

- When the failure message (KAQX10001) is output for two or more HDDs (slot).
- A failure message (KAQX10001) is output and OS goes down as well.
- An automatic recovery failure message (KAQX10098 Firmware failure (KAQG41011-E)) is output.

2. A HDD replacement is.

3. Specify which HDD has a failure according to the message.

KAQX10001 Internal disk error. (slot id =XX,



* 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 7-2: HDD installation example

4. Confirm that the status of the failed HDD is [removed] in Report. If the status [removed] is confirmed, make a note of the location of the failed HDD, and prepare to replace the HDD.

Note

When replacing a HDD, wait more than 1 minute between removing and installing the replacement HDD.

If over 1 minute has passed after the removal of the HDD, “nodevice” is output. If the time is less than 1 minute 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. The time required for rebuilding varies depending on the I/O load.

5. HCP-AW should confirm a Report and make sure that the HDD status is “normal”. If the status includes “failed”, then “Rebuild” has failed. In that case, replace a node.

8

Updating software according to the request from a distributor

This chapter contains information about updating software according to the request from a distributor. The following key topics are covered:

- ☐ Overview

Overview

Sometimes a distributor may ask the HCP-AW administrator for the software update.

Store the OS image, which requires the update in HCP, and execute the installation.

Software is given from a distributor to HCP-AW administrator through HTTP.

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

1. (HCP) administrator stores the installation image on HCP.

The procedures shown below need to be performed by a (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 (system-backup-data-user: it is automatically created by the HCP-AW site). 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 "system-backup-data-user"). For "Role" of the account for the image registration, assign the same Role as the one assigned to "system-backup-data-user". 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).

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 a Linux server that 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. Perform the following procedure.

KAQX10013 message may output during the software update. In this case, confirm the status of all file systems is normal with the report after the installation is completed. If the status of some file systems is not normal, solve the problem referring to the section in *Chapter 6, Confirming Report - Message confirmation table*.

---

a) Start management GUI, and login (see *Chapter 5, Overview and basic function of HDI Remote Server - Starting management GUI*).

b) Select the [Software Update] tab from the [Resources] tab in the management GUI.

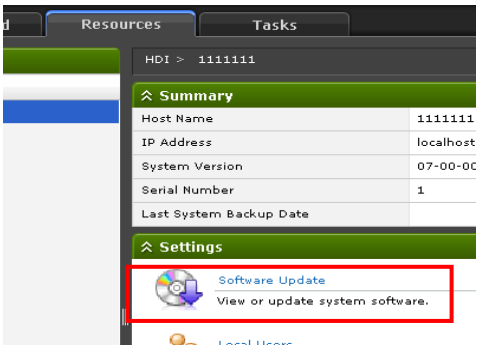


Figure 8-1: Software update

c) The installed OS version and the OS version that can be updated are displayed. If "The latest system software is installed" is displayed, a software update is not required. If a few versions are displayed, select the desired version and check the confirmation message box.

d) When you click the [Install] button, an advance preparation of the download and installation will start. Progress is displayed in the window. If you click Details next to the item name in progress, the estimated remaining time and transfer size, and the transfer speed are displayed. Download takes around 15 minutes.

e) When the download and preparation are completed, Install window is displayed. Displaying and accessing the management GUI are not available during the installation. Since the approximate installation time is displayed on the Install window, log into the management GUI window again after passing the approximate installation time, and Click the [Close] button to start the installation.

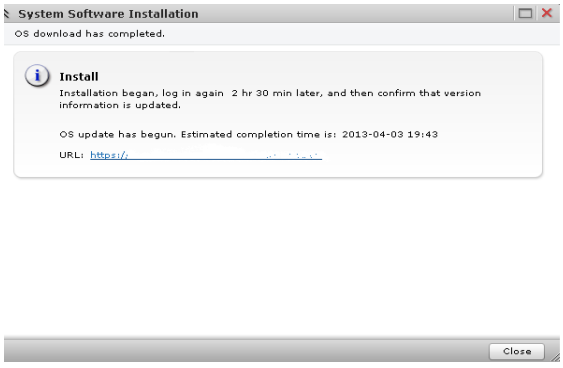


Figure 8-2: Install window

If the installation has failed during download and at the time of the preparation of the installation, this failure is displayed in management GUI. Get to know the situation according to the message ID and recover the failure. Then try to install again.

f) When the approximate time has passed, confirm that you can access the management GUI of the HDI Remote Server from the client PC. If UPnP is used, check the HDI Remote Server icon using Explorer, and if UPnP is not used, specify the IP address to check the accessibility.
If you can access the management GUI of the HDI Remote Server successfully, go to (g). If the icon is not visible or you cannot access the management GUI of HDI Remote Server, follow the procedure from (i) to (ii), shown below.
   i. Wait for another 30 to 60 minutes and then confirm that you can access to management GUI. If you can access management GUI successfully, go to (g). If icon is not visible or you cannot access the management GUI, go to (ii).
   ii. Check the HDI Remote Server power status. If the power is OFF, switch to ON and wait for 15 minutes. Then try to access again. If you can access the management GUI, go to (g). If the icon is not visible, or you cannot access the management GUI, go to (h).

g) Log into the management GUI and confirm the OS version stated in [System Version], of [System Information], in the Dashboard tab.
If the version information has already been updated to the installation specified version, this means that the installation was completed successfully and the installation procedure is complete.
If the version information has not been updated to the installation specified version, go to (h).

h) Installation may have failed.
If the version information has not been updated, reboot the system and check the version information.
If the status falls into any of the following categories, execute the installation procedure again. If the installation fails again, replace a node.
   - Despite the power is ON, the power status is still OFF.
   - Icon is not visible or access is denied even though the power is ON.
   - Version is not updated to the specified installation version even after the reboot.

   In case the power is OFF, the management GUI icon is invisible or you cannot access the management GUI despite the power being ON, a version is still not updated to the installation specified version after the reboot, contact the distributor.

3. Check the firmware information in a Report and confirm that the OS version is updated.

9

Procedure to use HDI Remote Server on another site

- Confirm that the HDI Remote Server is powered on before executing the following procedure.
- Do *not* power-off the system during the factory reset operation.

Follow the procedure below to use the HDI Remote Server at another site.

1. Set the HDI Remote Server to be moved to the "Decommissioned" status.
2. The HDI Remote Server deletes the user data, setting information, and logs when it detects that the HDI Remoter Server was operated in the "Decommissioned" status on the HCP-AW console at the time of reporting.

The OS of the HDI Remote Server is shutdown automatically when user data, setting information, and log were deleted.

3. Confirm the power LED of a node more than 15 minutes later (Reporting interval and 15 minutes). If the power LED is turned off, this means that the factory reset has completed successfully. Go to the step (4). If the power LED is still on, this means that the factory reset has failed. Then go to step 5.
4. Turn on the node and start the management GUI. Log into the management GUI and confirm that the Provisioning Wizard will start (Introduction window is displayed). If the start of Provisioning Wizard is confirmed, press the "x" box on the upper right side of the window to turn it off (see *Chapter 3, How to switch off the power*) and go to step (6). If Provisioning Wizard did not boot, go to step (5).

5. Sometimes the power LED may not be powered on even though the reporting interval of 15 minutes elapsed, or Provisioning might not start even if logged into the management log after turning on in step (4), above. Sometimes the Provisioning might not start after the redistribution. It might occur when the fact that HCP-AW administrator performed "Decommissioned" on the HCP-AW console, and was not reported to the HDI Remote Server. Or it might be a hardware failure. In this case, follow the steps below.

    a) Boot the device and log in to the management GUI.
    b) Move the cursor to Password input fields in the management login screen and press <Ctrl+ Alt+ J>. If the execution confirmation window is displayed, follow the instructions. Then the Factory Reset (deletion of user data and logs) will start.
    c) If the power LED is turned off, this means that the Factory Reset has been completed successfully. Power on and log in to the management GUI. Also, check whether the Provisioning Wizard boots. In this case, due to the high potential for a hard failure, forcibly power off the node (see *Chapter 3, How to switch off the power forcibly*) first, then replace with a new HDI Remote Server.

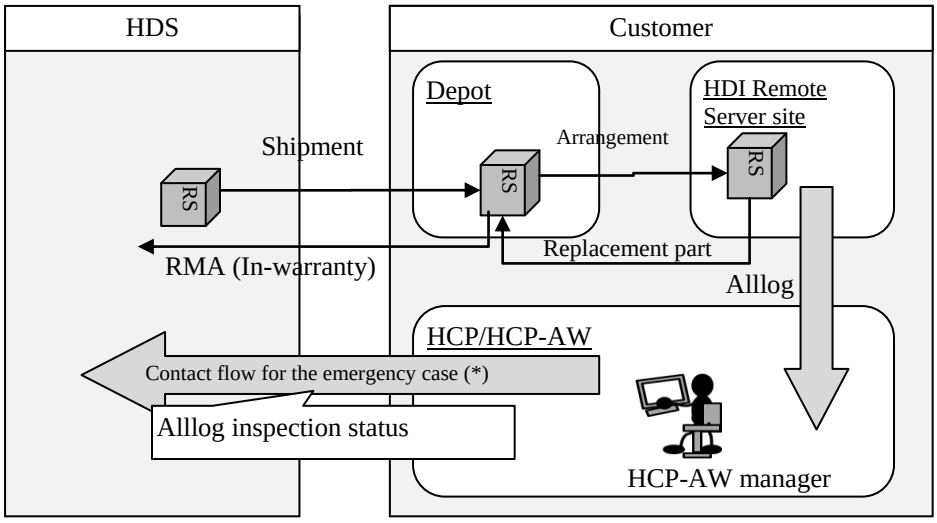
6. Collect and replace the HDI Remote Server.

10

Quality assurance system and new OS distribution path

Since the warranty period varies depending on the time of delivery, check the specifications or any other documents that came 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.
The local distributor should consider taking measures such as providing an alternative HDI Remote Server to a user.

If a node is out of warranty, purchase a new HDI Remote Server. Note that continuous use of an 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 10-1: Escalation route

11

Miscellaneous

Glossary

Table 11-2: Definition of terms

#	Term	Meaning
1	HCP	Abbreviation for 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 replicated to HCP.
2	HCP-AW	Abbreviation for HCP-Anywhere It is a system which is shared by accessing 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). HCP-AW administrator builds and monitors several nodes in remote. HCP-AW administrator configures, monitors, and manages the system using the Web application called the management console.
3	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.
4	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 replication.
5	Replication	A function to copy the file data on a node to HCP.
6	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.
7	Stub file	A file where file property is retained, but that data on a node is moved to HCP. About the file on a node the data of the file are duplicated to HCP by Replication, but after that the file on a node become unsubstantial because a node stub data and remained only property. If a client requires to read /write stub file, a node respond to it using Recall function that reads out the substantial data of the file from HCP.
8	Management GUI	Management GUI is a user interface used by the system administrator to manage a node.
9	UPnP Control Point	A client which received the UPnP service.

10	Factory Reset	The removal of all configuration and data from an HDI device, returning the device to the state it was in when it was newly shipped from the factory.
11	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.
12	front-end LAN	LAN which the client uses for accessing data.

Precautions

This section describes the precautions and supplementary notes on operating the HDI Remote Server.

Table 11-3: Precautions and supplementary notes (1/2)

#	Overview and Related Function	Description
1	Configuration plan <Precaution when operating DHCP >	- For the switch connected to the HDI Remote Server, if Spanning Tree Protocol is enabled, a port connected to the HDI Remote Server needs to be set as an edge port.
	Initial configuration <Precaution when operating DHCP >	- For the client access against the HDI Remote Server, specify the host name of the HDI Remote Server. - If the time of the DHCP server has changed, a contention of IP address may occur due to the divergence of the lending time managed by the server. If the change of the time is required, take countermeasures to deal with the contention of IP address such as enabling the IP address contention detection function and changing the range of the IP address to be lent.
2	Initial configuration <Precaution when sharing with NFS>	When files shared on NFS are excluded, use the fixed IP address for the NFS client as well.
3	Configuration plan <Precaution when registering the HDI Remote Server configuration information> Setting replication policy	In case of creating multiple file systems in one node, HCP-AW administrator should disperse the starting time of the replication policy. If the multiple replication policies are executed at the same time, load will be concentrated which may induce a failure.
4	Configuration plan <Create a file system >	Only the file system that was made by HCP-AW, guarantees action. When the file system was made by management GUI, it might be deleted in an opportunity of Reconfigure or it might continue to notify an error. And it is more likely to disturb to use.
5	Reconfigure <Precaution when changing a configuration> Recreate a file system	When creating a file system again, confirm that an older file system with the same name has been deleted in Report and then register the file system information to be created to execute the Reconfigure. If the file system before the configuration change has not been deleted, an error will occur.

Table 11-3: Precautions and supplementary notes (2/2)

#	Overview and Related Function	Description
6	Supplement at the time of registering a local user	To register a local user, HCP-AW administrator should set "Authentication" in "Local" in a console of HCP-AW. Then, HCP-AW administrator register a local user in management GUI at the following procedure. 1. Access the management GUI, and log on to the system. (Basic function of HDI Remote Server - Starting Management GUI) 2. In the top-left corner of the management GUI, choose the [**Resources**] tab, and click **Local Users** in the **Settings** area.

		3. On the "**List of Users / Groups**" page (for List of users) of the "**Local Users**" dialog box, select **List of groups** from the drop-down list, and then click [**Display**] button. 4. On the "**List of Users / Groups**" page (for List of groups), click [**Add New Group**]. 5. On the "**Add Group**" page, add groups that access shared directories on the node, and then click [**OK**] button. To enable the group to access CIFS shared directories, select "**Apply to CIFS ACL environment**". 6. If the group which added with step5 is displayed at "**List of Users / Groups**" page (for List of groups), select **List of users** from the drop-down list, and click [**Display**] button. 7. On the "**List of Users / Groups**" page (for List of users), click [**Add New User**]. 8. On the "**Add User**" page, add users that access shared directories on the node, and then click [**OK**] button. To enable the user to access CIFS shared directories, select "**Apply to CIFS environment**". 9. If the user which added with step8 is displayed at "**List of Users / Groups**" page (for List of users), operation in the management GUI is completed. Log out from management GUI, and please inform the user that local user name was registered.

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0) 1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

MK-90HDI040-00