HITACHI
Inspire the Next

HDI Remote Server Administrator Guide (Centrally Managed HDI RS)

Hitachi Data Systems

MK-90HDI053-02

Contents

Copyright © 2017, Hitachi, Ltd.

Copyright © 2017, Hitachi, Ltd.

Preface

Hitachi, Ltd. owns the copyrights of this guide. No part of this guide may be reused or reproduced without permission of Hitachi, Ltd.
In HDI Remote Server, there are HDI-RS CM (Centrally Managed HDI Remote Server) that coordinates with HCP Anywhere and HDI-RS LM(Locally Managed HDI Remote Server) that does not coordinate with HCP Anywhere.
When managing the Centrally 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 HDI-RS CM (Centrally Managed HDI Remote Server) that coordinates with HCP Anywhere.
To confirm the HDI-RS to be maintained is the model that coordinates with HCP Anywhere, check whether the serial number is registered in the management GUI of HCP Anywhere. If the serial number of the HDI-RS is not registered, contact to (HDS)
In addition, this document does not describe the transition procedure into HDI-RS LM.

Role and job description in this guide

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

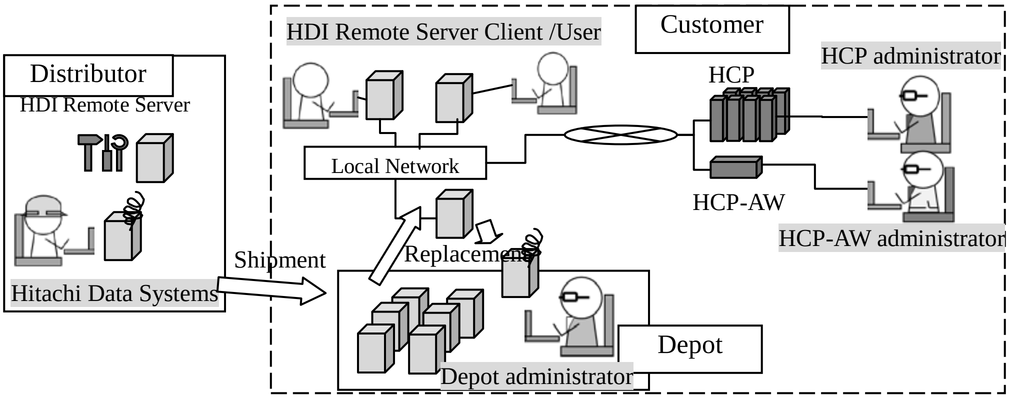


Figure 1. Image of each administrator

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	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.

Copyright © 2017, Hitachi, Ltd.

Chapter 1. *Flow of introducing HDI Remote Server*

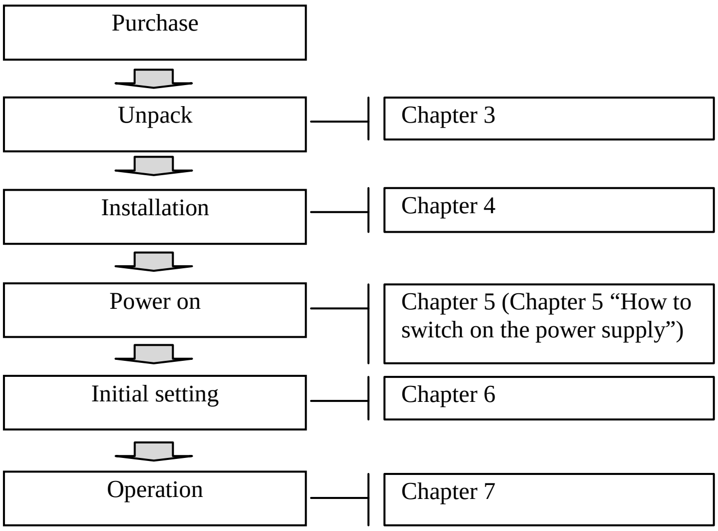


Figure 1-2. Flow of Introduction

Copyright © 2017, Hitachi, Ltd.

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.

Copyright © 2017, Hitachi, Ltd.

Chapter 3. *Package Contents and Getting to Start*

When the HDI Remote Server arrived at the user`s site, open the box and start to introduce and set the system referring to Quick Reference Card.

Chapter 4. *Installation*

Installation place

Regarding the conditions for installation environment, refer to the section Chapter13 “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-AW server, HCP, AD / DC servers, UPnP control point, DHCP server and DNS server. Build the environment referring to the figure shown below.

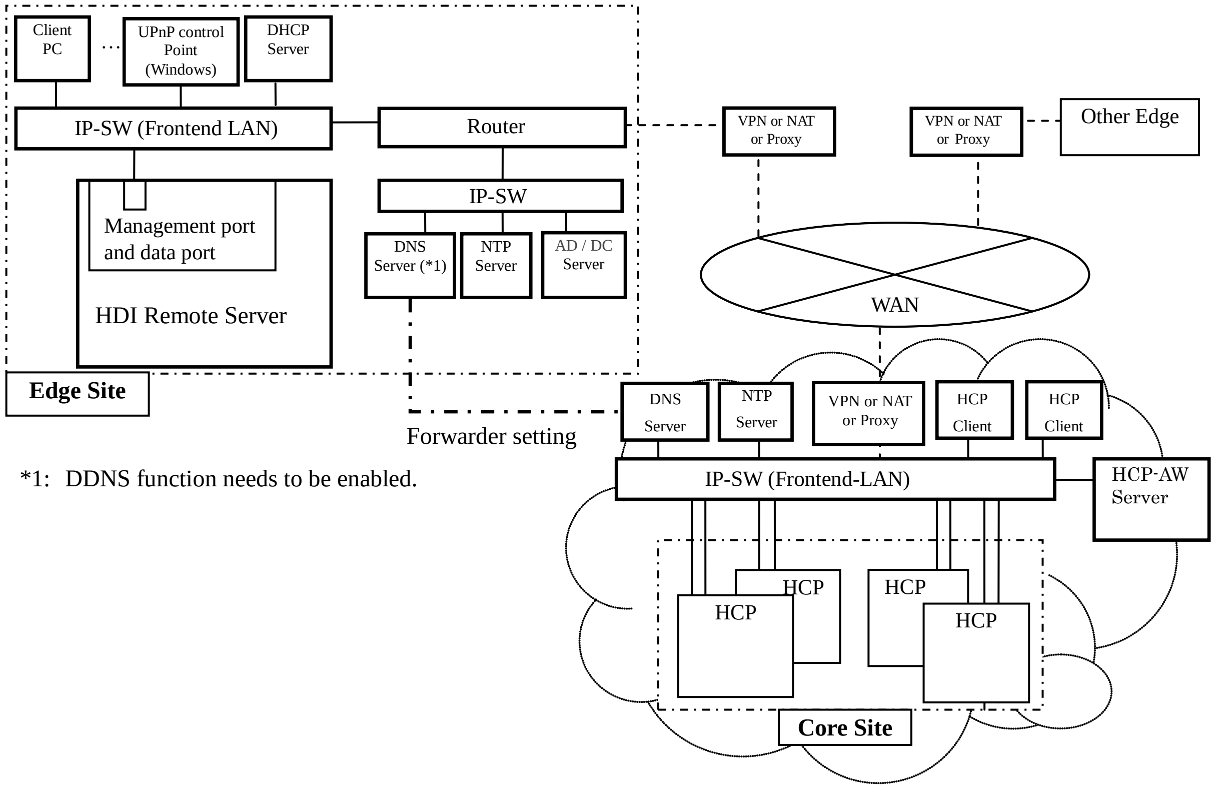
Note that the Edge Site and Core Site are linked through WAN.

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 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

Copyright © 2017, Hitachi, Ltd.

Connecting cable - Connecting each cable

For the connecting location, refer to the rear view of Quick Reference Card.

(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. If you use an unchanging 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 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	⋎ (mandatory)	-	Auto Negotiation	1500
⋎=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.

Copyright © 2017, Hitachi, Ltd.

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

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-AW	HDI RS and HCP	HDI RS and peripheral server (AD/DC/DNS/NTP, etc. (Core Site side))	HDI RS and User`s PC
22	tcp	ssh	Used for ssh			→RS	
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	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→		
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			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
600～1023	udp/tcp	rquota	Used for file shared by NFS				→RS
8005	tcp	tomcat	Used for Tomcat shutdown				→RS
8443	tcp	tomcat	Used for communication with Tomcat by HTTPS				→RS
15000~15019, 19012	udp/tcp	Data Management	Used for Migration management port 0			→RS	
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

Copyright © 2017, Hitachi, Ltd.

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-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				→RS

Copyright © 2017, Hitachi, Ltd.

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 Quick Reference Card.

(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.

Copyright © 2017, Hitachi, Ltd.

Chapter 6. *Initial Setting*

To perform the initial setting, take the following procedure.

・Confirmation points before initial setting.

・Executing the initial settings (In case of using DHCP / In case of the unchanging IP address)

・Confirming the Report notification

・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 that the power of HCP and HCP-AW which manages the data of using 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 data of HDI Remote Server to be used.
- Confirm with a user 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.

Performing initial setting

For the initial setting, use the Provisioning function.

At the time of the initial installation and after the node replacement, a user performs 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 and HCP-AW administrator should instruct a user to execute the installation if necessary.

In case of not using the DHCP server, use the Provisioning function after setting the unchanging IP address.

In case of using the DHCP server, follow the procedure (1). When the unchanging IP address is used, follow the procedure (2) to set the controlled IP address by the administrative terminal, or the procedure (3) to set the controlled IP address by the display.

Copyright © 2017, Hitachi, Ltd.

(1) In case of using DHCP [Setting by the administrative terminal]

NOTE:The following procedures (a) to (h) are the same as the procedure written in Quick Reference Card.

(a) After confirming HCP-AW and DNS server and etc, are running, press Remote Server power button and wait for 5 minutes.

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

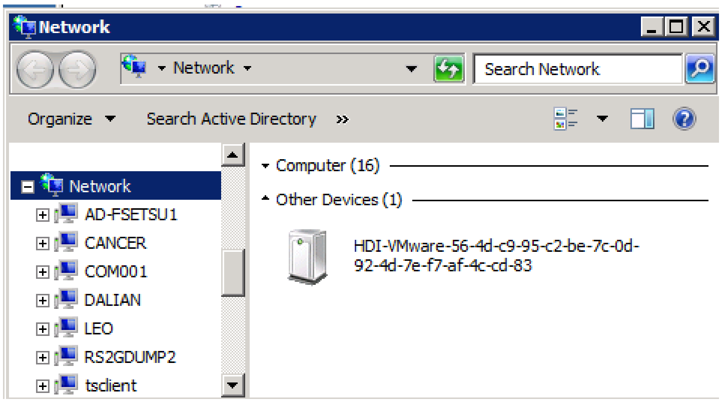


Figure 6-1 Booting GUI on HDI Remote Server

Tip: <u>HDI Remote Server icon is not found in the administrative terminal!!</u>
Resolve the problem referring to FAQ (Network FAQ).

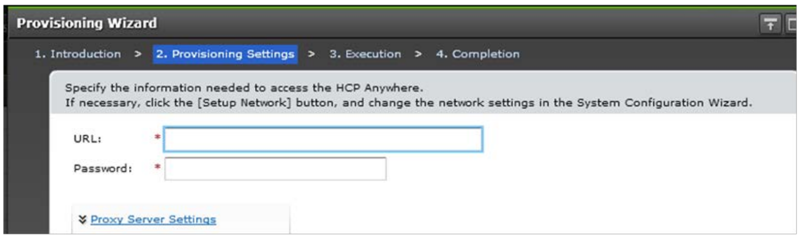
If the retrieval of the address on the DHCP server has failed, the default IP address may have been set. To change to the configuration using the unchanging IP address, directly link the administrative terminal and HDI Remote Server through the network and follow the procedure (2) to configure from the unchanging IP address.
(-> To (2) or network FAQ)

(c) Refer to Quick Reference Card to log into 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 in the first place, read the description and click [Next].

(f) When the Provisioning Settings window is displayed, input the URL of HCP-AW server and password. Execute the setting of the Proxy server if necessary.


Provisioning Wizard
1. Introduction > 2. Provisioning Settings > 3. Execution > 4. Completion
Proxy Server Settings

Specify the information needed to access the HCP Anywhere.
If necessary, click the [Setup Network] button, and change the network settings in the System Configuration Wizard.

URL: *

Password: *

Figure 6-2 Provisioning Wizard window 1

Then press [Next] button.

(g) When the confirmation window is displayed, confirm the setting of Portal URL and press [Next] button. HDI Remote Server will retrieve the configuration information from the HCP-AW server.

(h) Progress window is displayed. Each process reaches 100% and “Completed” is appeared, then the configuration is complete.

(i) When the setting has completed, go to the Chapter 6 “Confirming report notification”.

Copyright © 2017, Hitachi, Ltd.

(2) In case of using the unchanging IP address [Setting by the administrative terminal]

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

(a) Link the PC (the administrative terminal) and HDI Remote Server directly.

Set the segment of the PC to be able to connect to "169.254.1.100", and then the netmask set to 255.255.0.0.

Ex) Assign IP address: 169.254.1.99, Netmask: 255.255.0.0, Gateway: (None)

(b) Power on HDI Remote Server and wait for 5 minutes after the power lump is turned on.

(c) Access to HDI Remote Server with the default IP address (169.254.1.100) in the Web browser. When the login window is displayed, input the following User ID and Password to login.
(-> For the booting management GUI, see the Chapter 7 "Basic function of HDI Remote Server - Starting Management GUI")

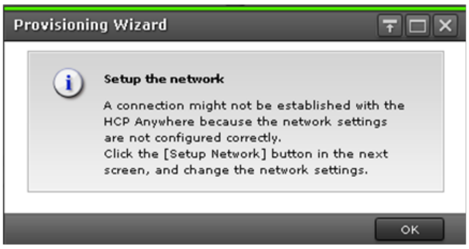
Ex) URL: https://169.254.1.100/admin/
User ID: admin
Password: chang3me!

(d) When logging into the management GUI, the HDI Remote Server GUI password change dialog will open (first time only).
Change the password in accordance with the GUI window. If the password changing processing has completed, press [Close] to close the dialog box.

HCP-AW administrator should tell the changed password to a user.

(e) Closing the password change window, Provisioning Wizard is started.

(f) Introduction window is displayed in the first place. Then press [Next] to display "Provisioning wizard Settings" and Information. Read the description in the Information window and press [OK].



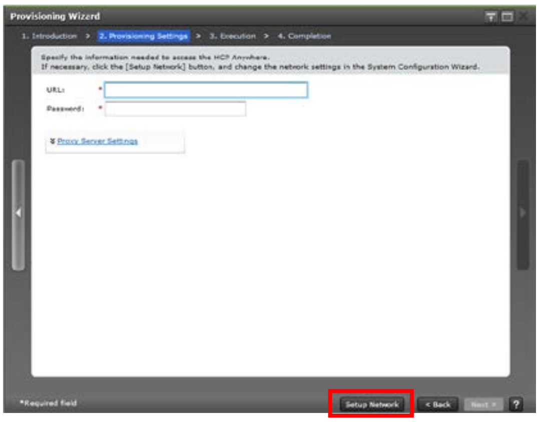
Provisioning Wizard

Setup the network

A connection might not be established with the HCP Anywhere because the network settings are not configured correctly.
Click the [Setup Network] button in the next screen, and change the network settings.

Figure 6-3 Provisioning Wizard window 1

(g) Press [Setup Network] shown on the lower side of "Provisioning Settings" window.



Provisioning Wizard

1. Introduction > 2. Provisioning Settings > 3. Execution > 4. Completion

Specify the information needed to access the HCP Anywhere.
If necessary, click the [Setup Network] button, and change the network settings in the System Configuration Wizard.

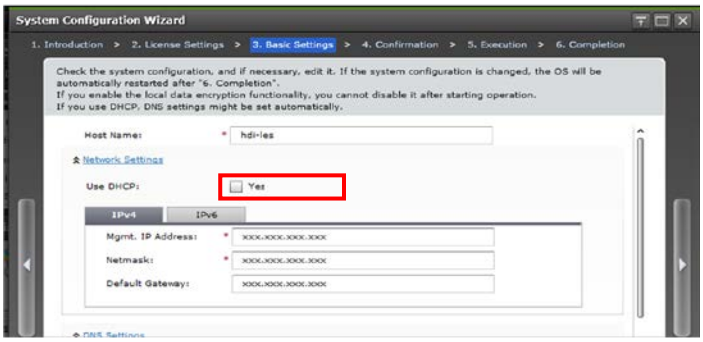
URL: *
Password: *

Proxy Server Settings
*Required field
Setup Network
< Back
Next >
?

Figure 6-4 Provisioning Wizard window 2

(h) When “Introduction” window of System Configuration Wizard is displayed, press [Next].

(i) Uncheck the checkbox “Yes” next to “Use DHCP” and enter the controlled IP address, netmask. Default gateway, DNS server address and NTP server address. Then press [Next].


System Configuration Wizard
1. Introduction > 2. License Settings > 3. Basic Settings > 4. Confirmation > 5. Execution > 6. Completion
Network Settings
IPv4
IPv6
DNS Settings

Check the system configuration, and if necessary, edit it. If the system configuration is changed, the OS will be automatically restarted after "6. Completion".
If you enable the local data encryption functionality, you cannot disable it after starting operation.
If you use DHCP, DNS settings might be set automatically.

Host Name: * hdi-les

Use DHCP: □ Yes

Mgmt. IP Address: * xxx.xxx.xxx.xxx

Netmask: * xxx.xxx.xxx.xxx

Default Gateway: xxx.xxx.xxx.xxx

Figure 6-5 System Configuration Wizard window 1

(j) When the confirmation window is appeared, confirm the contents and check the checkbox shown on the lower side of the window. Then press [Apply] button. The system reboots automatically after the progress window showed the completion of the network configuration.

※ Execute the following procedure after distributing a node.

(k) Connect HDI Remote Server to the network in the operation environment.

(*l*) Set the segment of the administrative terminal (Control Point) to be able to connect to HDI Remote Server, and connect the administrative terminal to HDI Remote Server.

(m) Enter the set IP address in the URL bar of the Web browser a few minutes later and access to HDI Remote Server again.

(n) Enter the IP address which was set and notified in the procedure (i) manually in the URL bar of the Web browser a few minutes later and access to HDI Remote Server.

Ex) https://<Mgmt. IP Address assigned in step(i)>/ admin/

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

(p) For the rest of the procedure, follow (e)-to-last steps of “(1) In case of using DHCP [Setting by the administrative terminal]” shown above.

Tip: If Retry message is displayed.

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.

Tip: Problem has occurred such as the HCP-AW is not found or an error has occurred during the Provisioning function is running etc.

See the chapter 8 “Troubleshooting” to confirm FAQ (Initial installation FAQ).

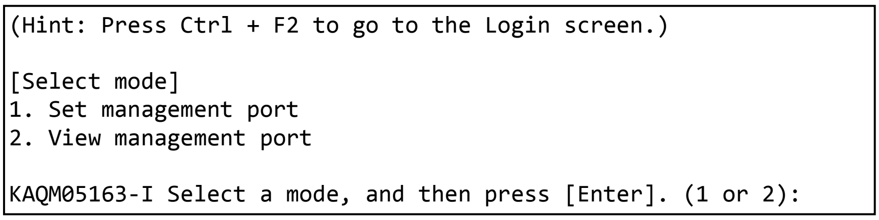
Copyright © 2017, Hitachi, Ltd.

(3) In case of using the unchanging IP address [Setting by the display]

(a) Connect the key board and the display to the HDI Remote Server.

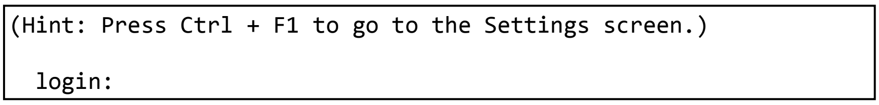
(b) Power on the HDI Remote Server and wait for five minutes after the power lump is turned on.

(c) When the window shown in Figure 6-6 appears in the display, go to the procedure (d). If the login window shown in Figure 6-7 appears, press the [Ctrl] and [F1] keys at the same time to switch to the window shown in Figure 6-6.



```
(Hint: Press Ctrl + F2 to go to the Login screen.)

[Select mode]
1. Set management port
2. View management port

KAQM05163-I Select a mode, and then press [Enter]. (1 or 2):
```

Figure 6-6 Controlled IP Address Setting/Confirmation Mode Selection Window 1

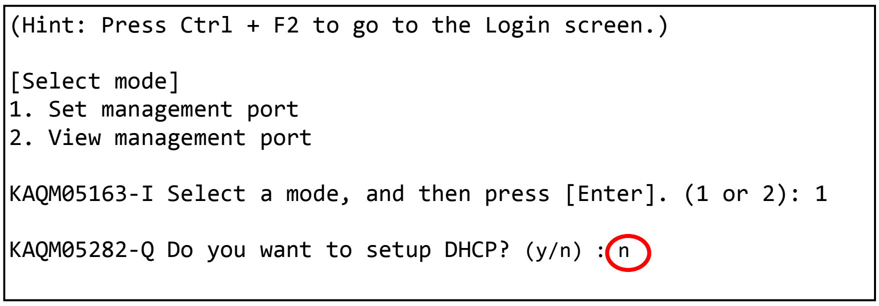


```
(Hint: Press Ctrl + F1 to go to the Settings screen.)

  login:
```

Figure 6-7 Login Window

(d) Enter “1” in the window shown in Figure 6-6, and press the [Enter] key.

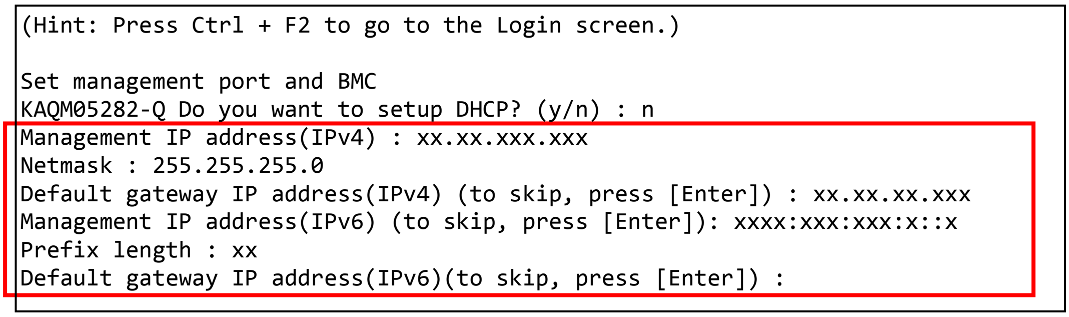
(e) Enter “n” for the confirmation message, and press the [Enter] key.



```
(Hint: Press Ctrl + F2 to go to the Login screen.)

[Select mode]
1. Set management port
2. View management port

KAQM05163-I Select a mode, and then press [Enter]. (1 or 2): 1

KAQM05282-Q Do you want to setup DHCP? (y/n) : n
```

Figure 6-8 Controlled IP Address Setting Window 1

(f) Enter the controlled IP address, netmask, and default gateway respectively and press the [Enter] key.

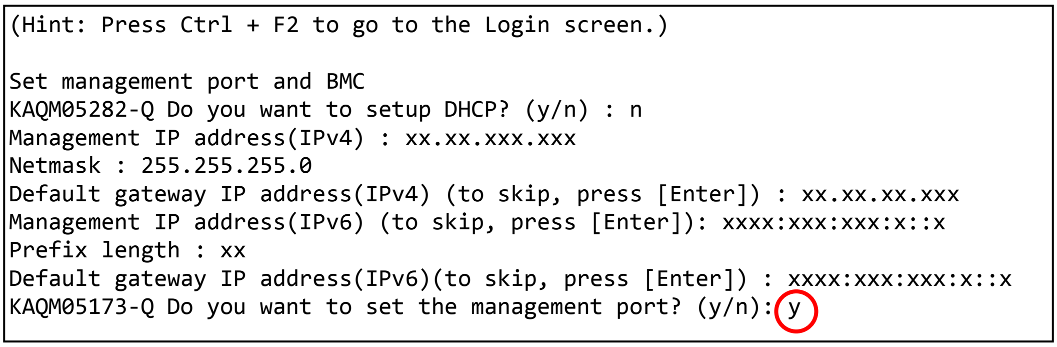


```
(Hint: Press Ctrl + F2 to go to the Login screen.)

Set management port and BMC
KAQM05282-Q Do you want to setup DHCP? (y/n) : n
Management IP address(IPv4) : xx.xx.xxx.xxx
Netmask : 255.255.255.0
Default gateway IP address(IPv4) (to skip, press [Enter]) : xx.xx.xx.xxx
Management IP address(IPv6) (to skip, press [Enter]): xxxx:xxx:xxx:x::x
Prefix length : xx
Default gateway IP address(IPv6)(to skip, press [Enter]) :
```

Figure 6-9 Controlled IP Address Setting Window 2

Copyright © 2017, Hitachi, Ltd.

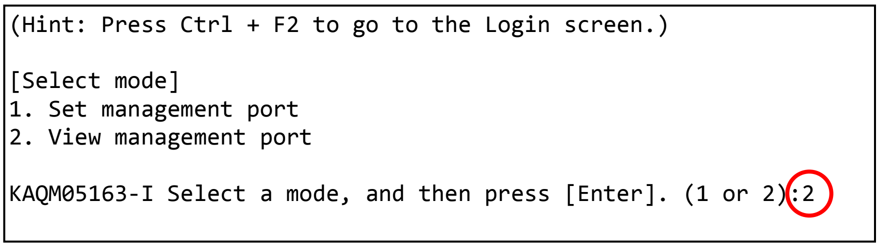
(g) When the confirmation message appears and if no problem with the entered items, enter “y” and press the [Enter] key.



```
(Hint: Press Ctrl + F2 to go to the Login screen.)

Set management port and BMC
KAQM05282-Q Do you want to setup DHCP? (y/n) : n
Management IP address(IPv4) : xx.xx.xxx.xxx
Netmask : 255.255.255.0
Default gateway IP address(IPv4) (to skip, press [Enter]) : xx.xx.xx.xxx
Management IP address(IPv6) (to skip, press [Enter]): xxxx:xxx:xxx:x::x
Prefix length : xx
Default gateway IP address(IPv6)(to skip, press [Enter]) : xxxx:xxx:xxx:x::x
KAQM05173-Q Do you want to set the management port? (y/n):y
```

Figure 6-10 Controlled IP Address Setting Window 3

(h) When the setting is complete, “KAQM05208-I Press the Enter key to return to selection mode.” is displayed followed by “KAQM05174-I The IP address of the management port was set.”.
Press the [Enter] key to return to the Controlled IP Address Setting/Confirmation Mode Selection window and enter “2” in the Controlled IP Address Setting/Confirmation Mode Selection window. Then press the [Enter] key.



```
(Hint: Press Ctrl + F2 to go to the Login screen.)

[Select mode]
1. Set management port
2. View management port

KAQM05163-I Select a mode, and then press [Enter]. (1 or 2):2
```

Figure 6-11 Controlled IP Address Setting/Confirmation Selection Window 2

(i) Confirm that the displayed setting is same as the value entered in the procedure (f).
If no problem, enter the [Enter] key to return to the Controlled IP Address Setting/Confirmation Mode Selection window, and remove the key board and the display.
If the set address is wrong, perform the setting procedures again from the procedure (c).

(j) Connect the HDI Remote Server to the network, and perform the procedures after the procedure (c) in “(2) In case of using the unchanging IP address [Setting by the administrative terminal]”. For the address of the Web browser, specify the controlled IP address that was set in the procedure (f).

Copyright © 2017, Hitachi, Ltd.

Confirming report notification

After completing the settings using the Provisioning function, a Report will be set from a node to the HCP-AW server. A HCP-AW administrator should confirm a Report and check that no failure occurs.

If a failure occurs, take an appropriate action to resolve the problem referring to the Chapter 8 “Troubleshooting” of this document.

Updating software

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

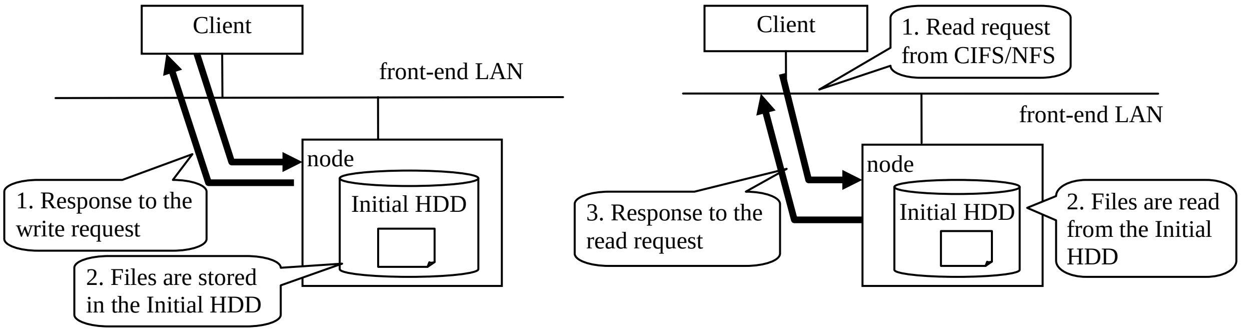
Copyright © 2017, Hitachi, Ltd.

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.



Client
front-end LAN
node
Initial HDD
1. Response to the write request
2. Files are stored in the Initial HDD
Client
1. Read request from CIFS/NFS
front-end LAN
node
Initial HDD
3. Response to the read request
2. Files are read from the Initial HDD

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.

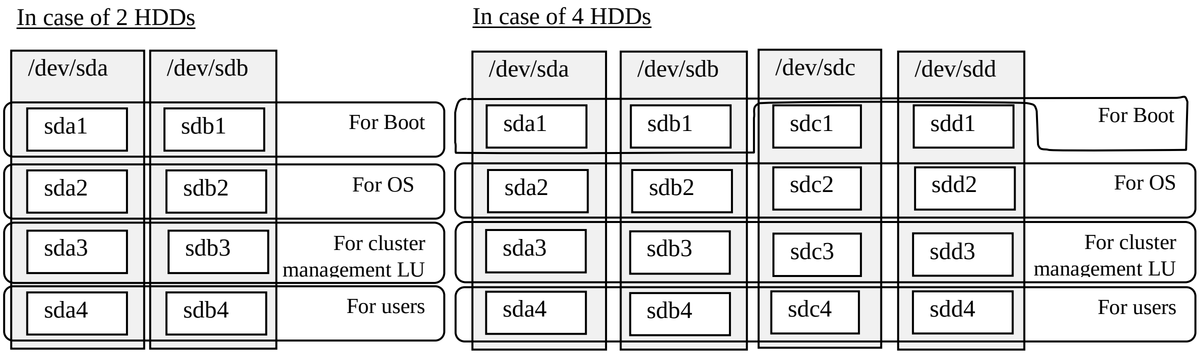


Figure 7.1-2 Image of RAID Configuration

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.

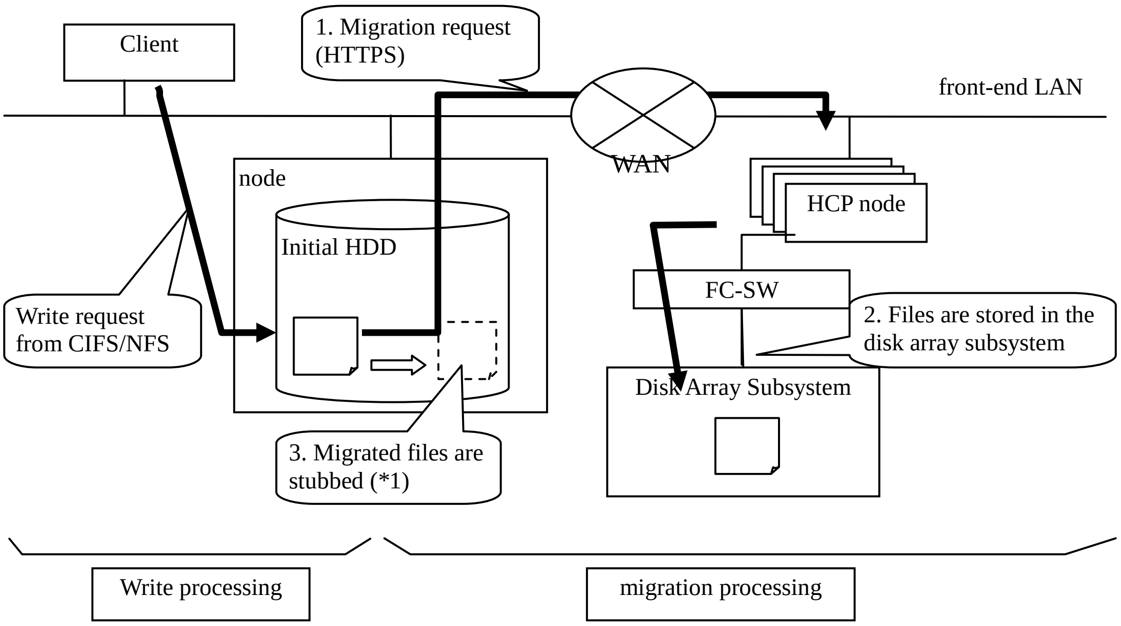
Copyright © 2017, Hitachi, Ltd.

(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 Provisioning.


Client
1. Migration request (HTTPS)
front-end LAN
WAN
node
Initial HDD
HCP node
FC-SW
Write request from CIFS/NFS
2. Files are stored in the disk array subsystem
Disk Array Subsystem
3. Migrated files are stubbed (*1)
Write processing
migration processing

*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

Copyright © 2017, Hitachi, Ltd.

(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.

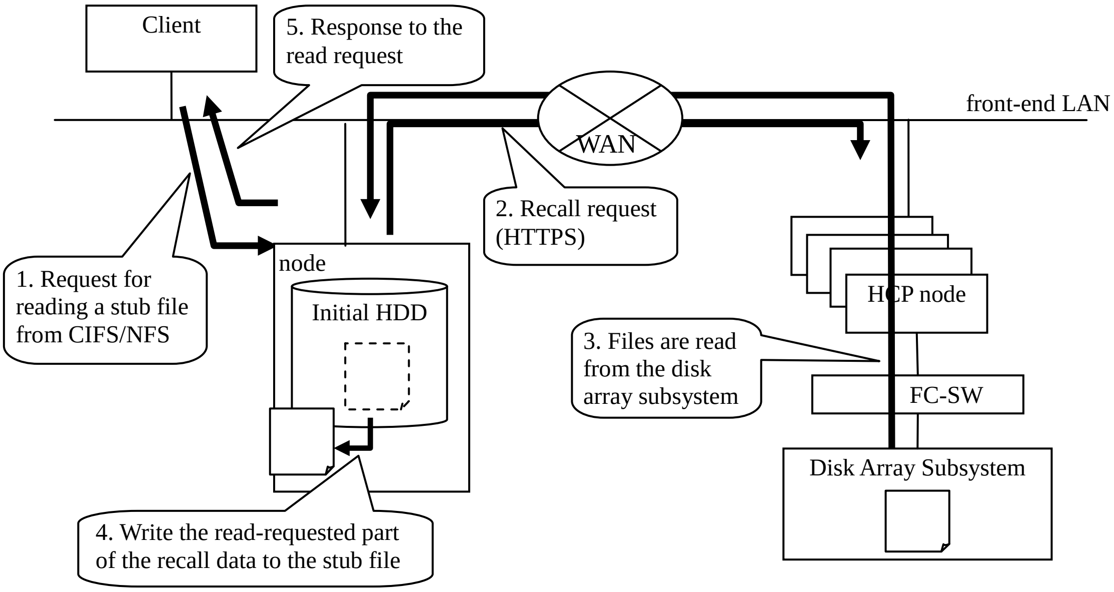

Client
5. Response to the read request
front-end LAN
WAN
2. Recall request (HTTPS)
1. Request for reading a stub file from CIFS/NFS
node
Initial HDD
HCP node
3. Files are read from the disk array subsystem
FC-SW
Disk Array Subsystem
4. Write the read-requested part of the recall data to the stub file

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 the recall processing fails. Figures 7.1.4-4 and 7.1.4-5 show the schematic figures of the failures.

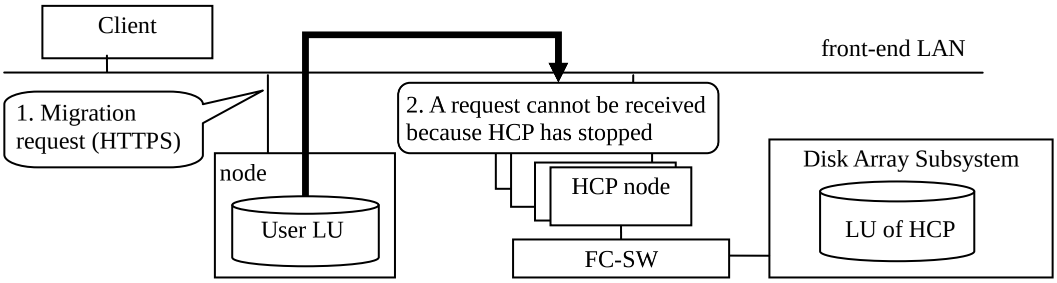

Client
front-end LAN
1. Migration request (HTTPS)
2. A request cannot be received because HCP has stopped
node
User LU
HCP node
FC-SW
Disk Array Subsystem
LU of HCP

Figure 7.1.4-4 Migration Processing When HCP Stopped

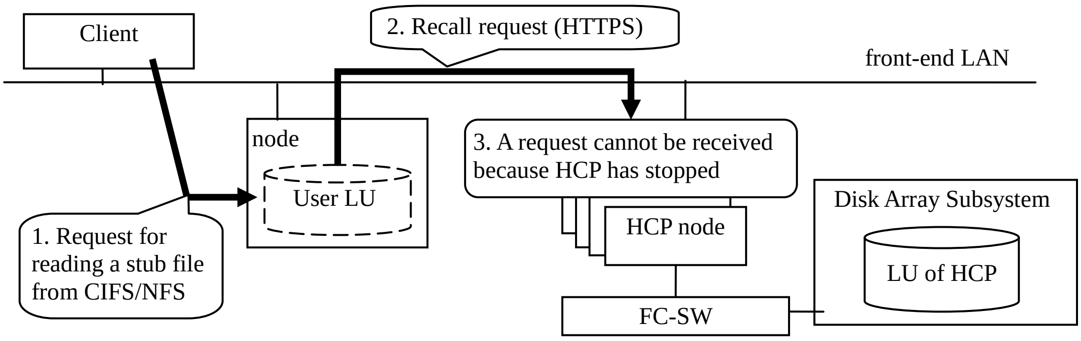

Client
2. Recall request (HTTPS)
front-end LAN
node
User LU
3. A request cannot be received because HCP has stopped
1. Request for reading a stub file from CIFS/NFS
HCP node
Disk Array Subsystem
LU of HCP
FC-SW

Figure 7.1-5 Recall Processing When HCP Stopped

Copyright © 2017, Hitachi, Ltd.

(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 7.1.4-6 shows the recall operation when the WAN failure occurs as an example.

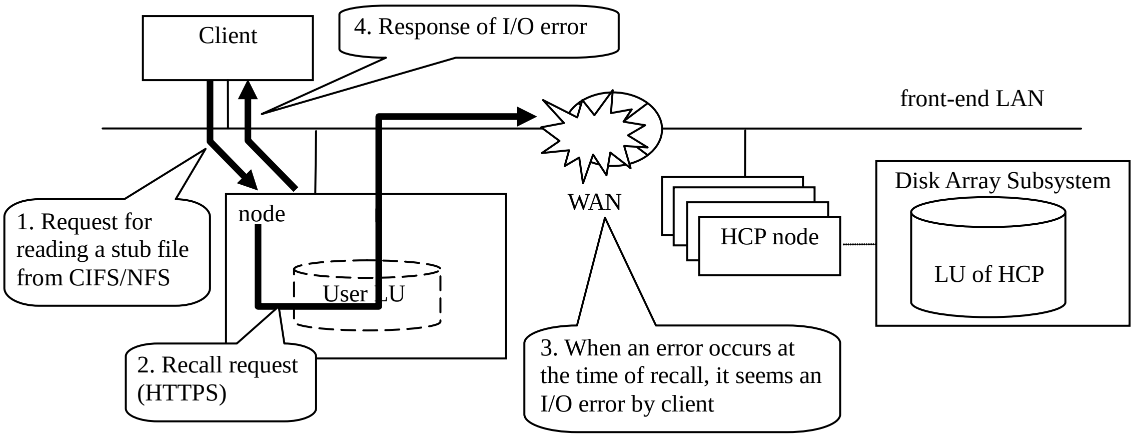

Client
4. Response of I/O error
front-end LAN
WAN
Disk Array Subsystem
HCP node
LU of HCP
node
User LU
1. Request for reading a stub file from CIFS/NFS
2. Recall request (HTTPS)
3. When an error occurs at the time of recall, it seems an I/O error by client

Figure 7.1-6 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”.

Copyright © 2017, Hitachi, Ltd.

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 - 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 reflected 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.

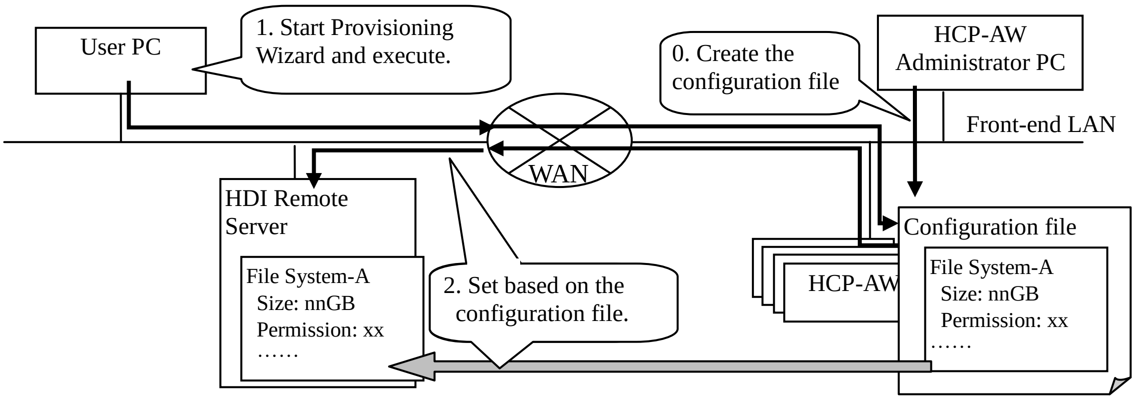


Figure 7.2-1 Overview of Provisioning Function

Copyright © 2017, Hitachi, Ltd.

Basic function of HDI Remote Server - Reporting function

This is the function to collect the configuration information and error information on the 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 a failure. An interval of sending report is configured by a HCP-AW administrator.

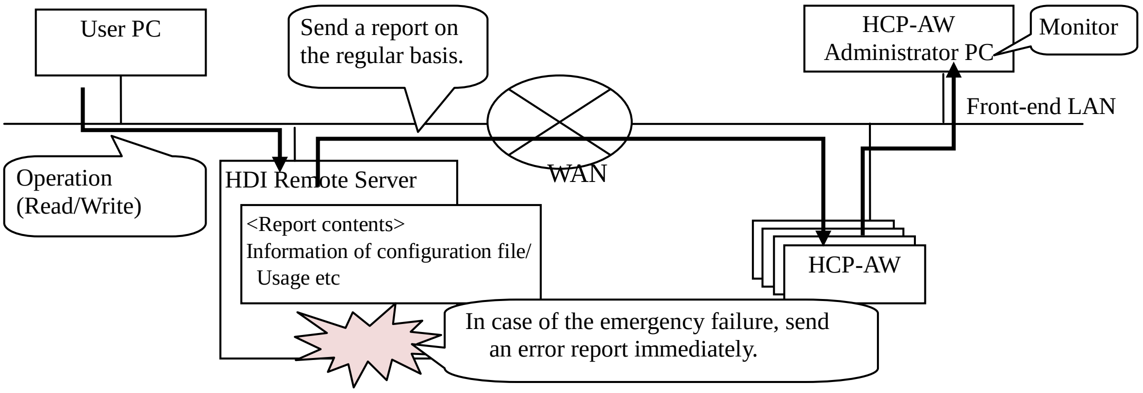

User PC
Send a report on the regular basis.
HCP-AW Administrator PC
Monitor
Front-end LAN
WAN
Operation (Read/Write)
HDI Remote Server
<Report contents>
Information of configuration file/ Usage etc
HCP-AW
In case of the emergency failure, send an error report immediately.

Figure 7.2-2 Overview of Reporting Function

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

Basic function of HDI Remote Server - Reconfigure function

When the discrepancy of the configuration information is found between HDI Remote Server and the HCP-AW, this function reflects the discrepancy automatically to 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 Report is exchanged.

If the change requires the system reboot, automatically reboot the system shortly after the reconfiguration. If the reconfiguration has failed, execute the reconfiguration again in the next timing of Report.

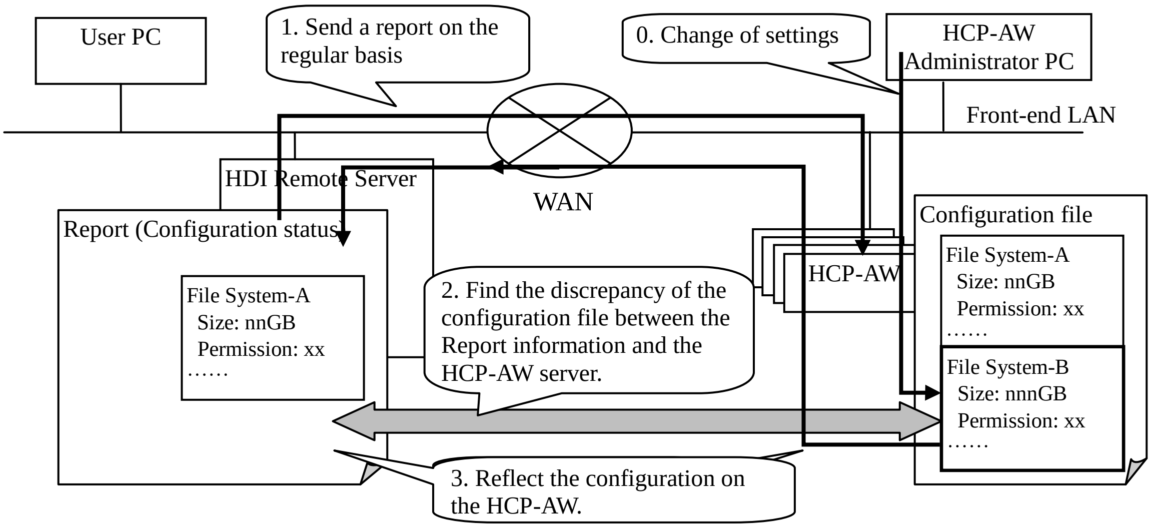


Figure 7.2-3 Overview of Reconfigure Function

Copyright © 2017, Hitachi, Ltd.

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 Report, take an appropriate action referring to the message confirmation table in the Chapter 8 “Confirming Report - Message confirmation table”.

Table 8-1 Structure of Chapter8

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

Copyright © 2017, Hitachi, Ltd.

Overview of the failure determination procedure is shown below.

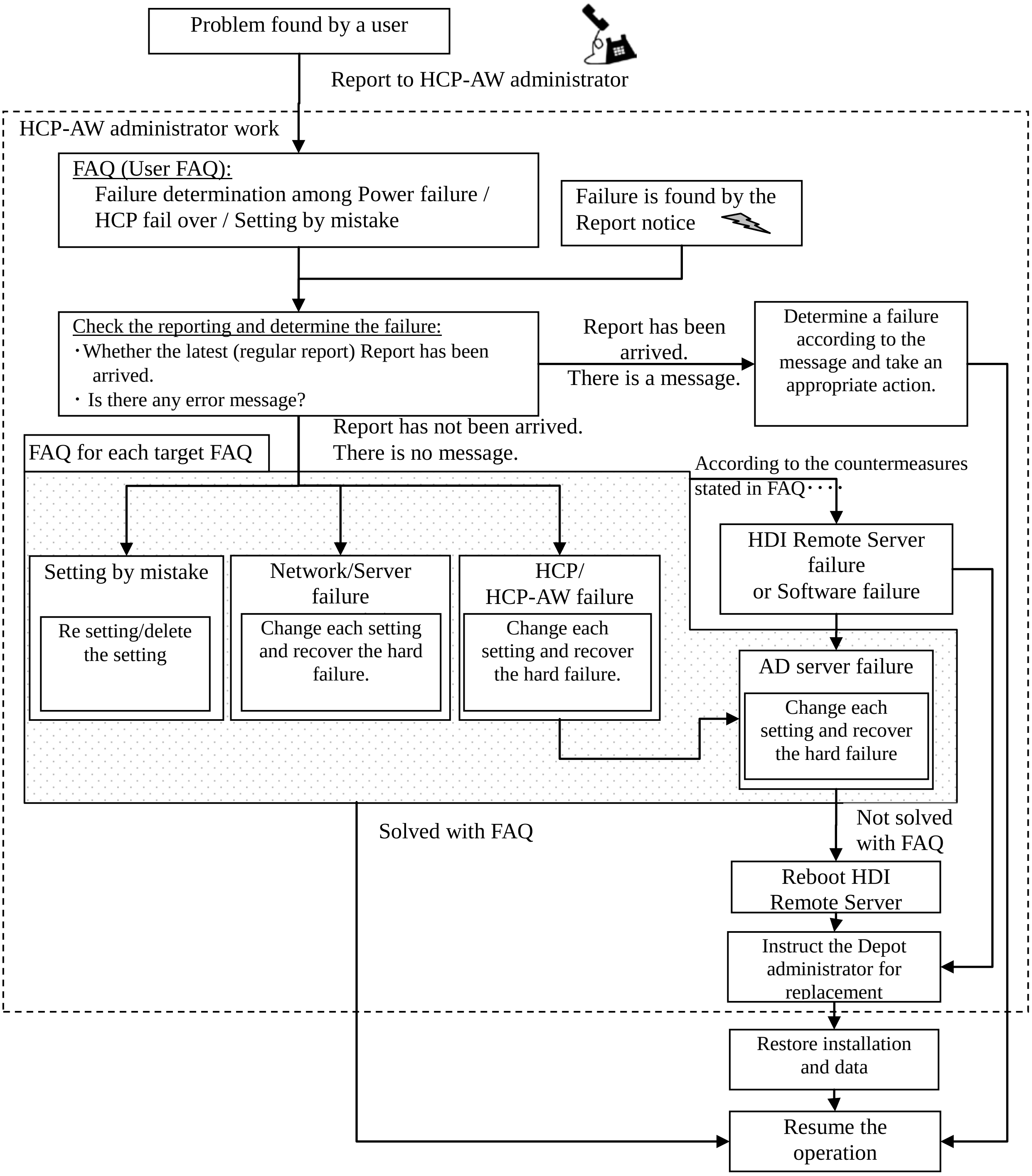

Problem found by a user
Report to HCP-AW administrator
HCP-AW administrator work
FAQ (User FAQ):
Failure determination among Power failure / HCP fail over / Setting by mistake
Failure is found by the Report notice
Check the reporting and determine the failure:
・Whether the latest (regular report) Report has been arrived.
・ Is there any error message?
Report has been arrived.
There is a message.
Determine a failure according to the message and take an appropriate action.
Report has not been arrived.
There is no message.
FAQ for each target FAQ
According to the countermeasures stated in FAQ・・・
Setting by mistake
Re setting/delete the setting
Network/Server failure
Change each setting and recover the hard failure.
HCP/ HCP-AW failure
Change each setting and recover the hard failure.
HDI Remote Server failure or Software failure
AD server failure
Change each setting and recover the hard failure
Solved with FAQ
Not solved with FAQ
Reboot HDI Remote Server
Instruct the Depot administrator for replacement
Restore installation and data
Resume the operation

Figure 8-1 Overview of Failure Determination

Copyright © 2017, Hitachi, Ltd.

Finding a failure by users

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

If any beep (memory error) or abnormal tone (hardware error) sounds, instruct for the node replacement.

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

Checking FAQ (User FAQ)

(1) HCP-AW 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 Report”.

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 “✓” in the Check column.

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

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.	

Copyright © 2017, Hitachi, Ltd.

Confirming Report

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

(2) HCP-AW administrator needs to confirm that a report is delivered periodically.

If a report is delivered, check a report and confirm that an error message is not output. If an error message exists, see the message confirmation table in the Chapter 8 “Confirming Report - Message confirmation table”.
In case that an error message cannot be confirmed and a report is not delivered periodically, it may be a problem of the network or environment server settings. Proceed to the Chapter 8 “Checking network environment”.

Copyright © 2017, Hitachi, Ltd.

Confirming Report - Message confirmation table

If “Message” shown in the below table is included in a report, take an appropriate action. If a problem is not solved even took an action, proceed to the Chapter 8 “Checking FAQ (AD server)”.

Note:

- There are two cases for the delivery time of an error message. First case is an error message which is delivered shortly after the failure occurrence and the other case is an error message which is delivered with the regular report. Therefore sometimes an error occurrence time and report notification time may be different depending on the failure type.
- HCP-AW administrator confirms the model name of the registered device in HCP-AW management console by following procedure. If it is not “Model: HDI-RSxx”, not supported on this documents. Please inform Hitachi Data Systems of the model name and output messages.
  (1) After login to HCP-AW management console, click “HDI Devices” button, and open [Devices] page.
  (2) Select the serial number of the each device and identify the model name on [Overview] window.

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.

In the “Action” items of the below table state “…wait for the completion of Reconfigure”, note that this “Reconfigure” will be executed in the maximum of 24 hours interval.

Table 8.3-1 Failure Recovery from Report Notification Message (1/4)

#	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 the Chapter 9 “HDD Replace procedure” at the start).
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	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 an action according to the action stated in KAQX10004. 3. Switch off the power first and then switch on the power again.
7	KAQX 10006	Migration 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.

Table 8.3-1 Failure Recovery from Report Notification Message (2/4)

#	Code	Message	Detailed Code	Output display	Severity	Action
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 an 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 be varied depending on the <detailed info>. See the Appendix 1.
10	KAQX 10009	Service-start failure	—	Major events	Error	1. If the one of the following messages is output, take an 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 9 "Replacement")
11	KAQX 10010	Service-stop failure	—	Major events	Error	1. If the message KAQX10030 (Reconfigure error) has been output, take an 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 9 "Replacement").
12	KAQX 10011	File system full(*detailed info.*) **detailed info.*:file system name	—	Major events	Error	1. If the message KAQX1006 (Migration 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 (Migration 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.
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 an appropriate action. 2. Confirm the configuration information on HCP-AW (Encryption: enable encryption at rest). If the encryption is enabled and the message KAQX10004 have been output concurrently, take an appropriate action. 3. Switch off the power first and then switch on the power again. 4. If the problem is not recovered, replace a node. (-> Chapter 9 "Replacement")
15	KAQX 10014	A problem was detected in a fan. (fan_*fan-number*)	—	Alerts	–	Replace a node (→Chapter9 "Replacement"). There is a danger of temperature increase. Stop the node immediately and contact a user to switch off the node until the replacement.
16	KAQX 10015	Inconsistent data was detected on the internal hard disk.	—	Alerts	–	Error occurred in the Consistency Check. Check if KAQX10098(KAQG41010-E) or KAQX10098(KAQG41013-E) was output in the same time. If it was not output in the same time, nothing to do. If it was output in the same time, refer to Chapter 8 "When finding the invalid data in Consistency Check".

Copyright © 2017, Hitachi, Ltd.

Table 8.3-1 Failure Recovery from Report Notification Message (3/4)

#	Code	Message	Detailed Code	Output display	Severity	Action
17	KAQX 10018	An attempt to start the NFS service failed.	—	Major events	Error	1. If the message KAQX10020 and KAQX10030 have been output concurrently, take an 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. (-> Chapter 9 "Replacement")
18	KAQX 10019	An attempt to start the CIFS service failed.	—	Major events	Error	1. If the message KAQX10020 and KAQX10030 have been output concurrently, take an 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. (-> Chapter 9 "Replacement")
19	KAQX 10020	Provisioning 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 infornation to be reviewed, see Appendix 2.
20	KAQX 10021	Attempts to start the file version restore function failed.	—	Major events	Error	1. If the message KAQX10020 and KAQX10030 have been output concurrently, take an 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. (-> Chapter 9 "Replacement")
21	KAQX 10022	An attempt to start the resource group failed.	—	Major events	Error	Collect the logs first and execute the node replacement (-> see Chapter 9 "Replacement")
22	KAQX 10030	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 infornation to be reviewed, see Appendix 2. 2. If the failure is repeated, collect the logs and send.

Table 8.3-1 Failure Recovery from Report Notification Message (4/4)

#	Code	Message	Detailed Code	Output display	Severity	Action
23	KAQX 10098	Firmware failure(*detailed info.*)	KAQG41010-E /KAQG41013-E	Major events	Error	See the section Chapter 8 “Appendix A - When finding the invalid data in Consistency Check”.
24			KAQG41011-E/KAQG46531-E/KAQG46533-E	Major events	Error	Replace a node. (-> Chapter 9 “Replacement”) However, if KAQG46531-E is contained in the message, the node could lead to the temperature rise. Please inform user to stop using the node immediately and to power off the node until replacement.
25			KAQM37246-E	Major events	Error	1. If the message KAQX10008 (Namespace-sharing error) has been output, take an 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.
26			Other than #23 and #24, #25	Major events	Error /Warn	1. If the message KAQX10013 (File system is blocked) has been output, take an 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 (-> Chapter 9 “Replacement”).
27	KAQX 10099	Firmware failure(*detailed info.*)		Events	Error	If the message other than KAQX10099 message has been output, take an appropriate action. If the message has not been output, any action is not required as the error may be temporal. However, if the error is not recovered more than one hour (recurrence), collect the logs and send.

Copyright © 2017, Hitachi, Ltd.

Appendix 1.Detaild 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	Collect the logs and send.
14	read-only file system	Warn	

Copyright © 2017, Hitachi, Ltd.

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.	arcactmigctl	Filesystems
3.	archcpset	Configuration -> HCP
4.		Filesystems -> HCP Migration Schedule
5.	archcpdel	Configuration -> HCP
6.	arcmigdel	Filesystems -> HCP Migration Schedule
7.	arcmigset	Filesystems -> HCP Migration Schedule
8.	arcrestore	Reviewing the configuration information on AW is not required. 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.
9.	cifscreate	Filesystems -> Shares Filesystems -> Import
10	cifsdelete	Filesystems -> Shares Filesystems -> Import
11	cifssvauthset	Configuration -> Authentication
12	cifssvdefset	Configuration -> Services
13	cifssvumapset	Configuration -> Authentication
14	cifssvset	Configuration -> Services
15	dir*xxxxxx*	Filesystems -> Shares
16	dhcpset	Configuration -> Network
17	dnsset	Configuration -> Network
18	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.)
19	fsexpand	Filesystems -> Cache Size
20	fsxxxxxx other than fsdelete and fsexpand	Filesystems
21	hostnameedit	Configuration -> Network
22	if*xxxxxx*	Configuration -> Network
23	licenseset	Reviewing the configuration information on AW is not required. Press [Save] button without changing the configuration information and wait for the next Reconfiguration.
24	nasreboot	Reviewing the configuration information on AW is not required. Press [Save] button without changing the configuration information and wait for the next Reconfiguration.
25	nfscreate	Filesystems -> Shares Filesystems -> Import
26	nfsdelete	Filesystems -> Shares Filesystems -> Import
27	*xxxxxx*policy	Filesystems -> HCP Migration Schedule
28	prsreportingctl	Configuration -> Reporting
29	route*xxxxxx*	Configuration -> Network
30	sv*xxxxxx*	Configuration -> Services
31	sysluscheduleset	Reviewing the configuration information on AW is not required. Press [Save] button without changing the configuration information and wait for the next Reconfiguration.
32	timeset	Configuration -> Time
33	invalid configuration (*bbbbb*)	*bbbbb* (Determine the point to be reviews by referring to the information in character fill (padding). 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"....)
34	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.

Copyright © 2017, Hitachi, Ltd.

Checking network environment

Check the following confirmation items. If no problem is found , write “⋎” in the check column and when all columns are filled with “⋎”, determine that there is no problem with the network environment and proceed to the Chapter 8 “Confirming HCP status”.

If the check columns are not filled with “⋎”, 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.		ActiveDirectory is operated normally.	
7.		HDI Remote Server is registered in ActiveDirectory.	
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.	
17.	HCP-AW	HCP-AW is operated normally.	

Copyright © 2017, Hitachi, Ltd.

Confirming HCP status

See GUI in HCP which manages the data of HDI Remote Server, and confirm that any failure or failover has not been occurred.

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 ActiveDirectory 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, ask a user to reboot HDI Remote Server.

Ask a user to try to reboot for twice.

(1st reboot)

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

(2) Switch on the node.
(-> 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”

Copyright © 2017, Hitachi, Ltd.

When a problem is not solved

HCP-AW administrator should collect logs. Then contact the Depot administrator 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

Ask a user to collect a log and contact the distributor with the collected log as necessary.

●Log acceptance at the distributor site

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

To collect a log from a user PC, follow the following procedure. 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 the Chapter 7 “Basic function of HDI Remote Server - Starting Management GUI”)

(2) Click “Action menu” in Global menu and select [Download All log data].

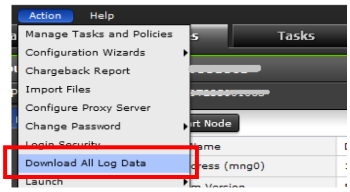
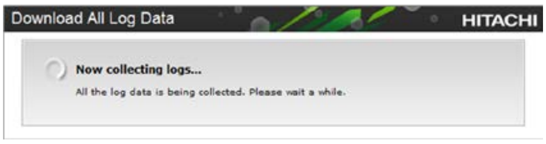


Figure 8.9-1 Action Menu window

(3) Open the new window and “Now collecting logs...” window is appeared.

Once the log collection is finished, 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].

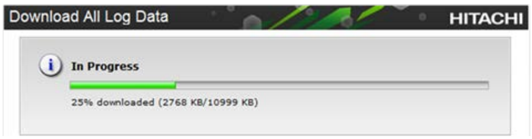

Download All Log Data

Now collecting logs...

All the log data is being collected. Please wait a while.

Figure 8.9-2 Download All Log Data window 1

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


Download All Log Data

In Progress

25% downloaded (2768 KB/10999 KB)

Figure 8.9-3 Download All Log Data window 2

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

(5) Make sure that a file named “Alllogdata_<host name/D+serial number> _<date and time>.tar.gz” is created in the destination to save specified in the above step (3). The user attaches the log file to an email and sends it to a HCP-AW manager.

Copyright © 2017, Hitachi, Ltd.

Appendix A - When finding the invalid data in Consistency Check

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

When the invalid data message of M98(KAQG41010) or M98(KAQG41013) is output, HCP-AW administrator asked a user to do the log analysis in Chapter 8 “When finding an invalid data - distinguish the area that data invalid occurred”.

If the result of the log analysis shows invalid data is not in the OS area, replace the node. If the result of the log analysis shows invalid data is in the OS area, no action is necessary.

NOTE: If the invalid data is in the OS area, no action is necessary. But KAQX10015 is displayed in report every time until invalid data become zero. Once KAQX10015 found, confirm M98(KAQG41010) or M98(KAQG41013) is not output with KAQX10015.

In the case invalid data is not found in the OS area, an HCP-AW administrator should arrange for a new node immediately, in parallel, ask a user to 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, 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 in a Report 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 [Boot area] or [cluster management LU 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 in following pages.

Copyright © 2017, Hitachi, Ltd.

When finding an invalid data - Execution procedure

For the procedure when invalid data is found is shown below.

(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, an HCP-AW administrator should asked a user to execute the log analysis in Chapter 8 “When finding an invalid data - distinguish the area that data invalid occurred”.

(3) If the result of the log analysis shows invalid data is in the OS area, no action is necessary. The service is able to continue.
If the result of the log analysis shows invalid data is not in the OS area, HCP-AW administrator arrange for a new node, and proceed to step (4).

(4) 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 Boot area or cluster management area or instead.

(5) After taking the above countermeasure (4), HCP-AW 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“M98 (KAQG41013).” is not output in Report until the node replacement is executed. In case that a message is output, execute from the step (2) again.

(6) When a new hardware has arrived at the user side, ask a user to replace a node.

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

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

Copyright © 2017, Hitachi, Ltd.

When finding an invalid data - Execution example

The following 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). HCP-AW administrator report it and asked user to do the log analysis immediately. Result is shown that the invalid data was not in OS area, and HCP-AW administrator arrange for the HDI Remote Server for replacement. However, it takes over 7 days until delivered to a user. 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 (1/2)

(Abbreviation in the HDI Remote Server event: C.C.= Consistency Check, M(data_*mmdd*)=Migration (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. HCP-AW administrator report to the user if this message is output, and ask the user to analyze logs.	When the user accepts a report from the HCP-AW administrator, user analyzes logs. User found the invalid data does not exist in the OS area. User inform HCP-AW administrator of the result.	↓
9.		17:00		HCP-AW administrator heard the invalid data is not in the OS area. Start to arrange for HDI Remote Server for replacement. HCP-AW administrator ask user to overwrite a user data.		↓
10	5/ 9 (Sat)	1:00	M(data_0509)			↓
11	5/10 (Sun)	1:00	M(data_0510)			↓
12	5/11 (Mon)	1:00	M(data_0511)			↓
13		9:00 - 17:00			Check the file. If a corrupted file is found, find the normal file from data_0505 and over write.*1	↓
14	5/12 (Tue)	1:00	M(data_0512)	(Normal data as a user data is migrated (assumption))		↓
15		2:00	C.C. start			↓
16		14:00	C.C. end	Report: Confirm that “M98 (KAQG41013).” is output. HCP-AW administrator report to the user if the message is output, and ask the user to analyze logs.	When the user accepts a report from the HCP-AW administrator, user analyzes logs. User found the invalid data does not exist in the OS area.	↓

Continued on next page.

Copyright © 2017, Hitachi, Ltd.

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

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

#	Date	Time	HDI Remote Server event	Report notification/Action by AW administrator	Action by users	Operation
17	5/13 (Wed)	1:00	M(data_0513)			↓
18		9:00 - 17:00			Check the file. If a corrupted file is found, find the normal file from data_0512 and over write.	↓
19	5/14 (Thu)	1:00	M(data_0514)	(Normal data as a user data is migrated (assumption))		↓
20	…(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.)…					↓
21	5/25 (Mon)	1:00	M(data_0521)	(Repeat the overwrite and normal data is migrated)		↓
22		9:00 -			HDI Remote Server is arrived. Notify to HCP-AW administrator.	Stop/Replace
23				Operate GUI in the AW console after notified by a user.		↓
24					Replace a node (+ “data_0521” is restored)	↓
25						Resume

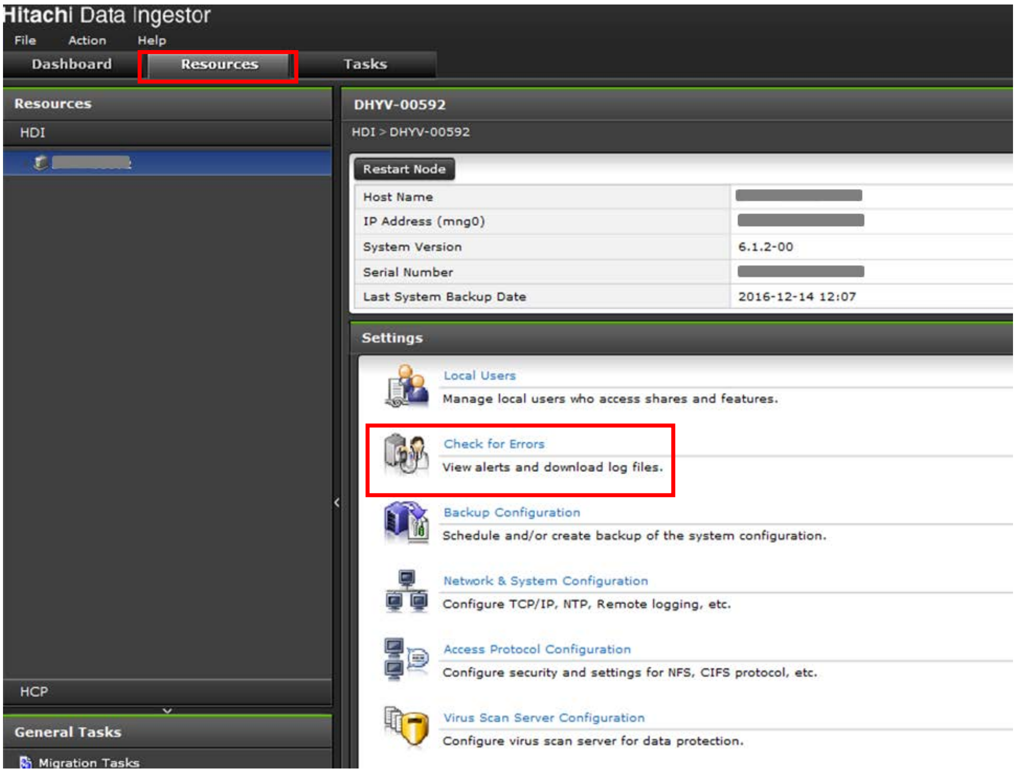
*1: Sometimes data which was migrated on the specified date may not be found depending on the timing of file creation. In that case, find a normal file from the files which was migrated on the date closer to the normal completion of the Consistency Check.

Following procedure show us how to distinguish the area that data invalid occurred, when M98(KAQG41010) and M98(KAQG41013) were output in the report.

(1) HCP-AW administrator ask a user to do the following steps.
HCP-AW administrator inform a user of the time that M98(KAQG41010) or M98(KAQG41013) was reported.

(a) Start the management GUI and login to the system. (-> see the Chapter 7 “Basic function of HDI Remote Server - Starting Management GUI” .)

(b) Open the “Resources” tab window, and click the icon of [Check for Errors].



Host Name	[redacted]
IP Address (mng0)	[redacted]
System Version	6.1.2-00
Serial Number	[redacted]
Last System Backup Date	2016-12-14 12:07

Local Users
Manage local users who access shares and features.

Check for Errors
View alerts and download log files.

Backup Configuration
Schedule and/or create backup of the system configuration.

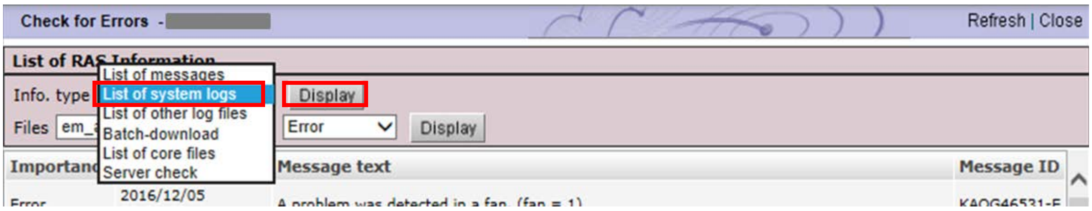
Network & System Configuration
Configure TCP/IP, NTP, Remote logging, etc.

Access Protocol Configuration
Configure security and settings for NFS, CIFS protocol, etc.

Virus Scan Server Configuration
Configure virus scan server for data protection.

Figure 8.10-1 [Resources] tab window

(c) New window is opened. Select a “List of system logs” in a list of drop-downs of “Info. type” in “List of RAS Information” window, and click the [Display] button.

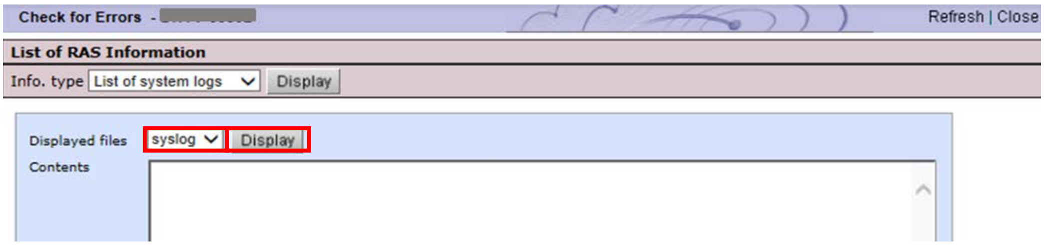


Error 2016/12/05 A problem was detected in a fan. (fan = 1) KAQG46531-E

Figure 8.10-2 List of RAS Information window 1

Copyright © 2017, Hitachi, Ltd.

(d) Confirm the “syslog” is displayed in drop-down list next to “Displayed files” in displayed window, click the [Display] button. Logs are displayed in “Contents” frame.



Check for Errors - [redacted]

List of RAS Information

Info. type: List of system logs

Displayed files: syslog

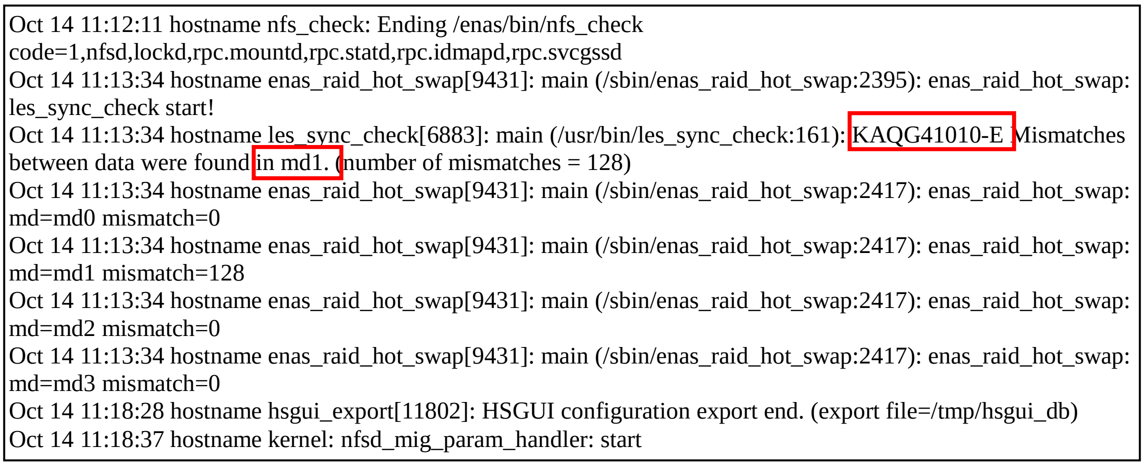
Figure 8.10-3 List of RAS Information window 2

(e) User identify the following message that output on the time HCP-AW administrator informs in “Contents” frame.
” KAQG41010-E Mismatches between data were found in *xxx*. (number of mismatches = *yyy*)”
xxx is shown the LU name in the message, and shown any of md0, md1, md2 and md3. *yyy* is shown block number of data invalid is occurred.

Tips: <u>If user were not able to find the message in the scope of “Contents” frame which displayed after clicking the [Display] button:</u>

1. Search the message with downing the scroll bar which is right side of “Contents” frame.
   In “Contents” frame, a bottom syslog message is the newest.
   When the message was found, proceed to step (f) in this argument, and when the message was not found, proceed to #2 in this Tips.
2. Execute the step (g) and step (h) in this argument. And then, to distinguish the area which invalid data is, collect logs and send it to the distributor.
   About the procedures to collect logs, refer to Chapter 8 “All Log collection procedure”.
3. After the HDI administrator send logs to the distributor, until the log analysis result is shown, HDI administrator ask a user to execute step (4) on Chapter 8 “When finding an invalid data - Execution procedure”.
4. When the distributor inform the HCP-AW administrator that the invalid data area is on the OS area, user is nothing to do. HCP-AW administrator inform a user to restart the service.
   When the invalid data area is not on the OS area, HDI administrator execute step (5) on Chapter 8 “When finding an invalid data - Execution procedure”.

Note: Multiple messages maybe output on the same time.



```
Oct 14 11:12:11 hostname nfs_check: Ending /enas/bin/nfs_check
code=1,nfsd,lockd,rpc.mountd,rpc.statd,rpc.idmapd,rpc.svcgssd
Oct 14 11:13:34 hostname enas_raid_hot_swap[9431]: main (/sbin/enas_raid_hot_swap:2395): enas_raid_hot_swap:
les_sync_check start!
Oct 14 11:13:34 hostname les_sync_check[6883]: main (/usr/bin/les_sync_check:161): KAQG41010-E Mismatches
between data were found in md1. (number of mismatches = 128)
Oct 14 11:13:34 hostname enas_raid_hot_swap[9431]: main (/sbin/enas_raid_hot_swap:2417): enas_raid_hot_swap:
md=md0 mismatch=0
Oct 14 11:13:34 hostname enas_raid_hot_swap[9431]: main (/sbin/enas_raid_hot_swap:2417): enas_raid_hot_swap:
md=md1 mismatch=128
Oct 14 11:13:34 hostname enas_raid_hot_swap[9431]: main (/sbin/enas_raid_hot_swap:2417): enas_raid_hot_swap:
md=md2 mismatch=0
Oct 14 11:13:34 hostname enas_raid_hot_swap[9431]: main (/sbin/enas_raid_hot_swap:2417): enas_raid_hot_swap:
md=md3 mismatch=0
Oct 14 11:18:28 hostname hsgui_export[11802]: HSGUI configuration export end. (export file=/tmp/hsgui_db)
Oct 14 11:18:37 hostname kernel: nfsd_mig_param_handler: start
```

Figure 8.10-4 Example of [Contents] frame on the “List of RAS Information” window

(f) If the LU name (part of *xxx*) which confirming step (e) is shown “md1”, it is clarified that the invalid data is in the OS area. If it is shown something except “md1”, it is clarified that the invalid data is not in the OS area.

(g) Click the [Close] button on the upper right of “Check for Errors” window, and close the window.

(h) Click the [Logout] button on the upper right of “Resources” tab window, and logout from GUI.

(2) Return to step (3) of Chapter 8 “When finding an invalid data - Execution procedure” with the result of the log analysis.

Copyright © 2017, Hitachi, Ltd.

Chapter 9. *Replacement*

Procedure of a node replacement is required

If a node replacement is required according to the failure determination process, HCP-AW administrator should ask the Depot administrator to ship and recall a node.

When replacing a node, follow the following procedures.

- Disconnect an older node from the environment
- Operation for node replacement
  (The replacement that indicate the node of the same serial number cannot to be operated in the management console of HCP-AW. If the new node has the same serial number as the node to be replaced, perform procedure of Chapter.9 “Node replacement - Replacing the same node”.)

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.

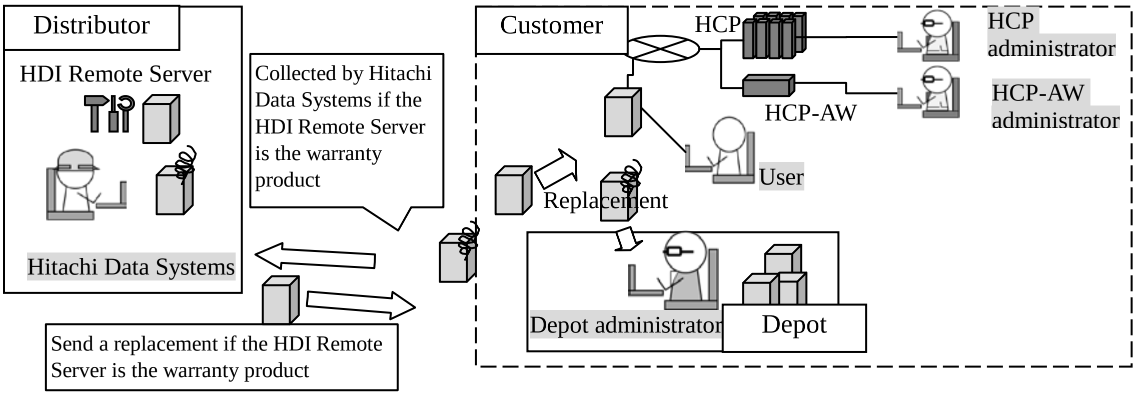

Distributor
HDI Remote Server
Hitachi Data Systems
Collected by Hitachi Data Systems if the HDI Remote Server is the warranty product
Send a replacement if the HDI Remote Server is the warranty product
Customer
HCP
HCP administrator
HCP-AW
HCP-AW administrator
User
Replacement
Depot administrator
Depot

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) Ask a user to send the replaceable HDI Remote Server to the Depot administrator.

Copyright © 2017, Hitachi, Ltd.

Note:
- HCP-AW administrator should confirm a new HDI Remote Server serial number before shipping to a use site.
- If the node to be replaced is using the fixed IP address, HCP-AW administrator needs to set the IP address. User should confirm that expected IP address has been set to a node.

(1) HCP-AW administrator confirms 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) HCP-AW administrator should perform the HDI Remote Server replacement by operating “Replace control” in the HCP-AW management console referring to the HCP-AW manual.

Note: Entered password used to register the new serial number is needed for the Provisioning. Let a user know about this.

(3) If the fixed IP address is being used, HCP-AW administrator should distribute after setting IP address to the new HDI Remote Server. For the details of the IP address setting method, see Chapter 6 Initial setting - Performing initial setting (2) (a)-(j) or Chapter6 Initial setting - Performing initial setting (3).

(4) Once HDI Remote Server arrived at the user`s site, ask a user to confirm a label and serial number and make sure that they are same as the ones the HCP-AW administrator is understanding.

(5) Ask a user to connect new HDI Remote Server to the network environment referring Quick Reference Card.

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

(6) HCP-AW administrator asks a user to execute the Provisioning.
If DHCP is being used, ask a user to execute Chapter 6 “Performing initial setting” (1). In case of using the fixed IP address, ask a user to execute the procedure following Chapter 6 “Performing initial setting” (2) (*l*).
Then, the data migrated on the HCP is restored on the HDI Remote Server automatically.

(7) After the HCP-AW administrator confirmed that Report is delivered, ask a user to execute the OS update installation if necessary (-> see the Chapter10 “Updating software according to the request from a distributor”).

(8) HCP-AW 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 the local user was registered before replacement, the local user needs to be registered again.

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

Node replacement - 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) HCP-AW administrator registers the dummy HDI Remote Server (serial number) and changes the status “Available” referring to the HCP-AW manual.

(2) HCP-AW administrator operates the management console of HCP-AW (“Replace control”) and replaces the original node with the dummy node referring to the HCP-AW manual.

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

(3) HCP-AW administrator instructs a user to open the management GUI of the original node. Ask the user to move the cursor focus to Password input fields in the login screen, and to start the restoration of “factory settings” (Press <Ctrl+ Alt+ J >). In accordance with the execution confirmation window, execute the restoration of “factory settings”, Power of HDI Remote Server will be turned off when the restoration of “factory settings” is finished.

Note : The customer needs to input user ID and password to execute “restoration of factory settings” in execution confirmation window when the OS version is 6.0.3-XX or later. The user ID and password is the one changed by Provisioning Wizard. If you lost user ID and password, call Hitachi Data Systems.

(4) HCP-AW administrator executes the operation to move the original console to the Inventory tub on the management console of HCP-AW. Additionally, replaces the dummy HDI Remoter Server with the original node.

Note: Password which was issued this time will be required for Provisioning. Therefore let a user know the password.

(5) HCP-AW administrator instructs a user to turn on the power of HDI Remote Server. Once the power is turned on, ask a user to login using the simplified GUI and perform Provisioning by entering the URL of HCP-AW and the temporary password obtained in (4) of above procedure.

(6) HCP-AW administrator deletes the HDI Remote Server (serial number) of the dummy node from the management console of HCP-AW once confirmed that Report of the original node is reached.

Note:
- For the client which is 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.

Copyright © 2017, Hitachi, Ltd.

HDD replacement procedure

If a HDD failure message was included in a report, HCP-AW administrator should contact a user and instruct to 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 node is powered on. If not, rebuilding is not executed.
- Do not reinstall the same HDD which has been removed.

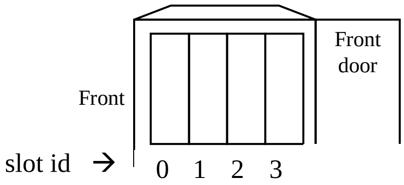
(1) HCP-AW administrator should confirm with a user that the OS status is up (determine it by checking whether a user can access to HDI Remote Server) and check the following messages which indicate HDD failure in the report.

In the following cases, a node needs to be replaced. (-> See the Chapter 9 “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) HCP-AW administrator informs a user that HDD replacement is required and contact Depot administrator to send HDD.

(3) HCP-AW administrator specifies which HDD has a failure according to the message.

```
KAQX10001 Internal disk error. (slot id =XX, status=xxxxx)
```



* 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・・・.
HCP-AW administrator should report it to a user.

Figure 9.2-1 HDD Installation Example

(4) HCP-AW administrator should confirm that a status of failed HDD is [removed] in Report. If the status [removed] is confirmed, notify a user about the location of failed HDD and instruct to replace HDD.

Note: When replacing HDD, ask a user to 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) HCP-AW administrator should confirm a Report and make sure that the HDD status is “normal”. If the status is included “failed”, 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 HCP-AW administrator for the software update.

HCP-AW administrator should store the OS image which requires the update in HCP and ask a user to execute the installation.
Software is give from a distributor to HCP-AW 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 are needed 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 (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).

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=xxxxxxxxxxxxxxxxxxxxxxxxxxx
```

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
```

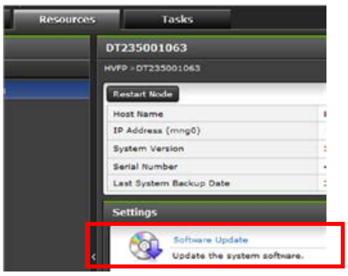
Copyright © 2017, Hitachi, Ltd.

(2) HCP-AW administrator should ask a user to perform the following procedure.
Note that the procedure shown below is performed by users.

NOTE: 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 Chapter8 “Confirming Report - Message confirmation table”.

(a) Start management GUI and login (-> see Chapter 7 “Basic function of HDI Remote Server - Starting management GUI”).

(b) Select [Software Update] tub from [Resources] tub in management GUI.



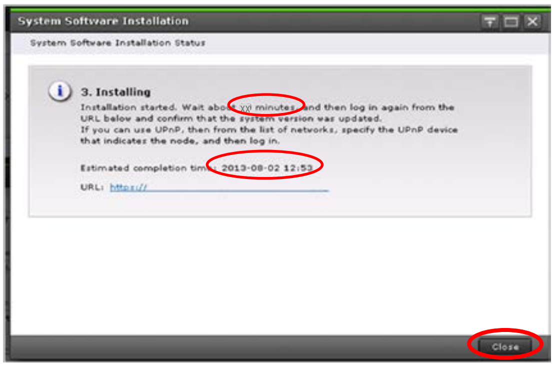
Fogure10-1 Software Update

(c) Installed OS version and the OS version can be updated are displayed. If “The latest system software is installed” is displayed, software update is not required.
If a few versions are displayed, select the version specified by a HCP-AW administrator and check the confirmation message box.

(d) When you click [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, 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 to the management GUI are not available during the installation.
Since the approximate installation time is displayed on the Install window, log into management GUI window again after passing the approximate installation time
Click [Close] button to start the installation.


System Software Installation
System Software Installation Status
Close

3. Installing
Installation started. Wait about xx minutes, and then log in again from the URL below and confirm that the system version was updated.
If you can use UPnP, then from the list of networks, specify the UPnP device that indicates the node, and then log in.

Estimated completion time: 2013-08-02 12:53
URL: https://

Figure 10-2 Install window

Note: 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.

Copyright © 2017, Hitachi, Ltd.

(f) When the approximate time has passed, confirm that you can access to management GUI of 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 could access to management GUI of HDI Remote Server successfully, go to (g). If icon is not visible or you cannot access to 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 could access to management GUI successfully, go to (g). If icon is not visible or you cannot access to management GUI, go to (ii).

(ii) Check HDI Remote Server power status. If the power is OFF, switch to ON and wait for around 15 minutes. Then try to access again. If you could access to management GUI, go to (g). If icon is not visible or you cannot access to management GUI, go to (h).

(g) Log into management GUI and confirm the OS version stated in [System Version] of [System Information] in the **Dashboard** tub.
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 be 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 phenomenon, execute the installation procedure again. If the installation has failed 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 that the power is OFF, management GUI icon is invisible or you cannot access to management GUI despite the power is ON, a version is still not updated to the installation specified version after the reboot, contact the distributor.

(3) HCP-AW administrator should check the firmware information in a Report and confirm that the OS version is updated, after the installation work by a user.

Copyright © 2017, Hitachi, Ltd.

Chapter 11. *Procedure to use HDI Remote Server on another site*

Note:• Confirm that HDI Remote Server is powered on before executing the following procedure.
• Instruct not to power off during the restoration of “factory settings”.

(1) HCP-AW administrator should set the HDI Remote Server to be moved to the “Decommissioned” status.

(2) HDI Remote Server deletes the user data, setting information and logs automatically when detected that the HDI Remoter Server was operated in the “Decommissioned” status on the HCP-AW console at the time of reporting.

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

(3) HCP-AW administrator should ask a user to confirm the power LED of a node more than 15 minutes later (Reporting interval and 15 minutes).
If the power LED is off, go to the step (4) to confirm that the restoration of “factory settings” has been completed successfully.
If the power LED is still on, this means that Factory Reset may have been failed. Then go to the step (5).

(4) HCP-AW administrator asks a user to turn on the node and start the management GUI. Log into the management GUI and confirm that Provisioning Wizard will start (Introduction window is displayed).
If the start of Provisioning Wizard was confirmed, ask a user to press “x” mark on the upper right side of the window to close the window and turn off (see Chapter 5 How to switch off the power). Then go to the step (6).
If Provisioning Wizard did not boot, go to the step (5).

(5) Sometimes the power LED may not be powered on even the reporting interval and 15 minutes elapsed or Provisioning may not start even logged into the management log after turning on in (4) stated above.

Sometimes the Provisioning may not start after the redistribution. It may occur when the fact that HCP-AW administrator performed “Decommissioned” on the HCP-AW console was not reported to the HDI Remote Server, or it may be a hardware failure. As for the failure cause determination, please see below.

(a) Ask a user to boot the management GUI.

(b) Ask a user to move the cursor focus to Password input fields in the management login screen and press <Ctrl+ Alt+ J>. If the execution confirmation widow is displayed, ask a user to follow the instruction. Then the restoration of “factory settings” (removal and initialization of each setting such as user data and log etc.) will start.

Note : The customer needs to input user ID and password to execute “restoration of factory settings” in execution confirmation window when the OS version is 6.0.3-XX or later. The user ID and password is the one changed by Provisioning Wizard. If you lost user ID and password, call Hitachi Data Systems.

(c) Ask a user to check the power LED status after 15 minutes. If the power LED is turned off.
If the power LED is turned off, ask a user to power on and login to the management GUI. Also ask a user to check whether Provisioning Wizard boots. If the boot of Provisioning Wizard can be confirmed, this means that the restoration of “factory settings” has been completed successfully. In this case, go to the step (6).

If the power LED is being turned on or Provisioning Wizard does not boot, this means that the restoration of “factory settings” has been failed. Since it is highly caused by the hardware failure, HDI Remote Server cannot be distributed to use. In this case, see switch off the node forcibly (see Chapter 5 “How to switch off the power forcibly”).

(6) HCP-AW administrator collects HDI Remoter Server and distributes HDI Remote Server to the different site.

Chapter 12. *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 to take measures such as providing an alternative HDI Remote Server to a user.

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

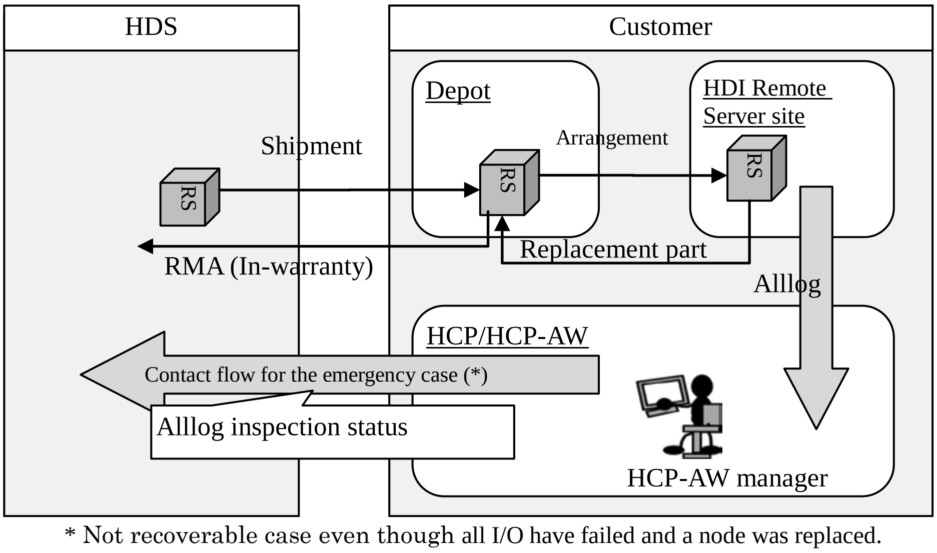


Figure 12-1 Escalation Route

Copyright © 2017, Hitachi, Ltd.

Chapter 13. *Miscellaneous*

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.). HCP-AW administrator builds and monitors several nodes in remote. HCP-AW 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 migration.
5	Migration	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 that files 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.
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 settings	System settings at the time of shipping from a factory If “factory settings” have been restored, user data and configuration information are removed from HDI device, and the system becomes the factory default settings (OS version is not restored).
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.

Copyright © 2017, Hitachi, Ltd.

Precautions

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

Table 13-3 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 unchanging IP address for the NFS client as well.
3	Configuration plan <Precaution when registering the HDI Remote Server configuration information> Setting migration policy	In case of creating multiple file systems in one node, HCP-AW administrator should disperse the starting time of the migration policy. If the multiple migration 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.

Copyright © 2017, Hitachi, Ltd.

Table 13-3 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 registers 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.

Copyright © 2017, Hitachi, Ltd.

Hitachi Data Systems

Corporate Headquarters
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

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

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

Hitachi Data Systems