Hitachi Global Link Manager

8.7.6

Installation and Configuration Guide

This manual describes how to install and set up the Hitachi Global Link Manager program, and how to operate the server. The manual is intended for system administrators who build and operate Hitachi Global Link Manager systems. This manual assumes that administrators know how to configure an environment for Hitachi Dynamic Link Manager, know how to use Hitachi Dynamic Link Manager, and are knowledgeable about the server OS (Windows).

MK-95HC107-37

February 2021

Contents

Preface

This manual describes the installation, setup, and server operation of the Hitachi Global Link Manager program (abbreviated hereafter to *Global Link Manager*).

Intended audience

This document is intended for storage administrators who use Global Link Manager to operate and manage storage systems, and assumes that readers have:

- Knowledge of how to set up an environment for HDLM and how to operate it
- Knowledge of the server OS (Windows)

Product version

This document revision applies to Hitachi Global Link Manager v8.7.6 or later.

Release notes

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

Document organization

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

Chapter/Appendix	Description
Chapter 1, Global Link Manager system configuration and requirements on page 1-1	Describes the Global Link Manager system configuration and requirements.
Chapter 2, Installing Global Link Manager on page 2-1	Describes how to install Global Link Manager.
Chapter 3, Setting up Global Link Manager on page 3-1	Describes how to set up Global Link Manager, including how to start and stop Global Link Manager, and how to back up and restore the Global Link Manager databases.
Chapter 4, Installing Global Link Manager clusters on page 4-1	Describes the settings for clustering servers.
Chapter 5, Security settings for communication on page 5-1	Describes the communication security settings that can be used to operate Global Link Manager.
Chapter 6, Using Global Link Manager with other products on page 6-1	Describes the settings for linking Global Link Manager with other products.

Chapter/Appendix	Description
Chapter 7, Troubleshooting Global Link Manager on page 7-1	Describes how to troubleshoot problems occurring during Global Link Manager operation.
Appendix A, The settings of Hitachi Command Suite Common Agent Component on page A-1	Provides information that is necessary to use Hitachi Command Suite Common Agent Component on a host, such as relevant settings and the procedure for starting the component.

Related documents

The following Hitachi referenced documents are also available for download from the Hitachi Vantara Support Connect: https://knowledge.hitachivantara.com/Documents.

- *Hitachi Global Link Manager User Guide*, MK-92HC214
- *Hitachi Global Link Manager Messages*, MK-95HC108
- *Hitachi Dynamic Link Manager (for AIX) User Guide*, MK-92DLM111
- *Hitachi Dynamic Link Manager (for Linux®) User Guide*, MK-92DLM113
- *Hitachi Dynamic Link Manager (for Solaris) User Guide*, MK-92DLM114
- *Hitachi Dynamic Link Manager (for Windows®) User Guide*, MK-92DLM129
- *Hitachi Dynamic Link Manager (for VMware®) User Guide*, MK-92DLM130
- *Hitachi Command Suite Installation and Configuration Guide*, MK-90HC173
- *Hitachi Command Suite Administrator Guide*, MK-90HC175
- *Hitachi Command Suite Tuning Manager Server Administration Guide*, MK-92HC021
- *Hitachi Command Suite System Requirements*, MK-92HC209

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	• Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. • Indicates a emphasized words in list items.
Italic	• Indicates a document title or emphasized words in text. • Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example:

Convention	Description
	`pairdisplay -g group` (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`
< > angled brackets	Indicates a variable in the following scenarios: • Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<report-name><file-version>.csv` • Variables in headings.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.

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

Icon	Label	Description
	Note	Calls attention to important or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes

Physical capacity unit	Value
1 megabyte (MB)	1,000 KB or $1,000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1,000^3$ bytes
1 terabyte (TB)	1,000 GB or $1,000^4$ bytes
1 petabyte (PB)	1,000 TB or $1,000^5$ bytes
1 exabyte (EB)	1,000 PB or $1,000^6$ bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: • OPEN-V: 960 KB • Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1,024^2$ bytes
1 GB	1,024 MB or $1,024^3$ bytes
1 TB	1,024 GB or $1,024^4$ bytes
1 PB	1,024 TB or $1,024^5$ bytes
1 EB	1,024 PB or $1,024^6$ bytes

Accessing product documentation

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

Getting help

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

Hitachi Vantara Community is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make

connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

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

Thank you!

1

Global Link Manager system configuration and requirements

This chapter describes the Global Link Manager system configuration and requirements.

Global Link Manager overview

Global Link Manager uses Hitachi Dynamic Link Manager (HDLM) path control functionality to provide integrated path management for large-sized system configurations. While HDLM manages paths for a host, Global Link Manager batch-manages paths for multiple hosts.

When you use a large-sized system configuration containing many hosts, the workload for managing paths from each host grows in proportion to the size of the system. Global Link Manager enables you to reduce the workload by providing unified management of the path information for multiple hosts. Global Link Manager also helps you to improve system reliability, by switching path statuses while taking into account the balancing of workloads in the whole system, by enabling the reporting of error information (alerts) from each host, and by enabling you to quickly solve problems.

Global Link Manager collects information about paths from multiple hosts on which HDLM is installed, and the Global Link Manager server collectively manages this information. Collected information can be viewed and controlled by multiple users who manage the hosts from client machines. The following figure shows an example of a Global Link Manager system configuration.

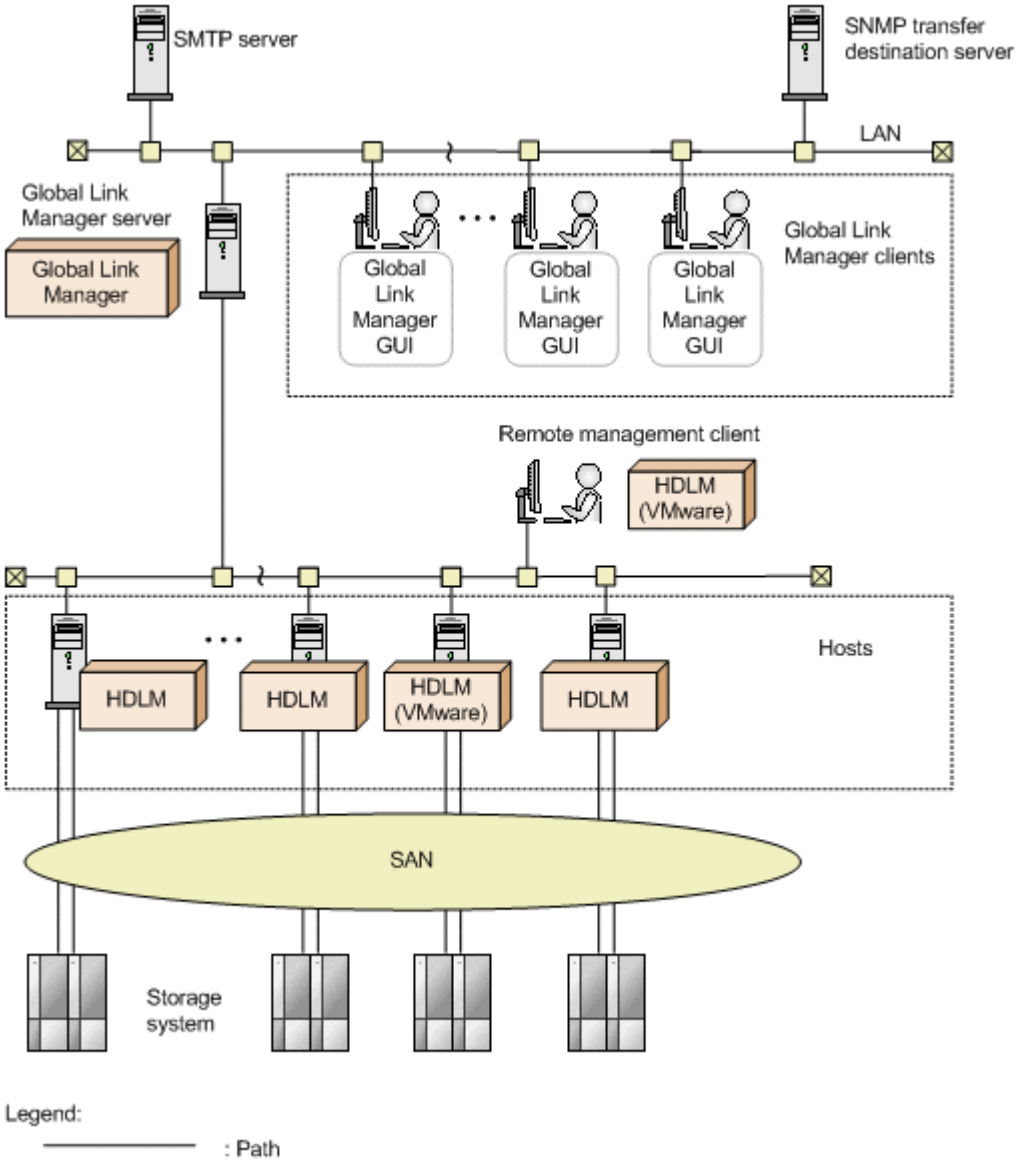

Figure 1-1 Example of a Global Link Manager system configuration

Global Link Manager includes the following features:

Collective management of path information of multiple hosts

By using remote operations from the Global Link Manager GUI, you can collectively set up multiple hosts and collect information from HDLM on multiple hosts. Operations can be managed from one console without having to log in to each host. Since multiple hosts can be managed collectively, the user can view the path information for hosts, HBA ports, storage systems, CHA ports, or by path status.

Summarizing the path statuses for the whole system

Global Link Manager can also display a summary of path statuses (the number of paths in each status). You can check path availability in the entire system without having to check the status of each host individually.

Support for path bandwidth control

Global Link Manager enables you to specify the format for viewing path information, such as by storage system or by CHA port. You can also use Global Link Manager to adjust the bandwidth of paths (the actual number of online paths) among multiple user applications or hosts.

Collective management of error information from multiple hosts

To quickly detect an error that occurs on a host in a multi host system and take appropriate action, you need to set up the environment to inform you about the error cause and location. To facilitate collective management, you can set up Global Link Manager so that path error information (detected by HDLM on each host) is reported to you as alerts. You can use any application to manage the alert information that is transferred from the Global Link Manager server to another server (SNMP transfer destination server).

Global Link Manager system configuration

Global Link Manager performs path management in a medium-scale or large-scale SAN environment that consists of multiple storage systems and multiple hosts. The following figure illustrates a basic Global Link Manager system configuration.

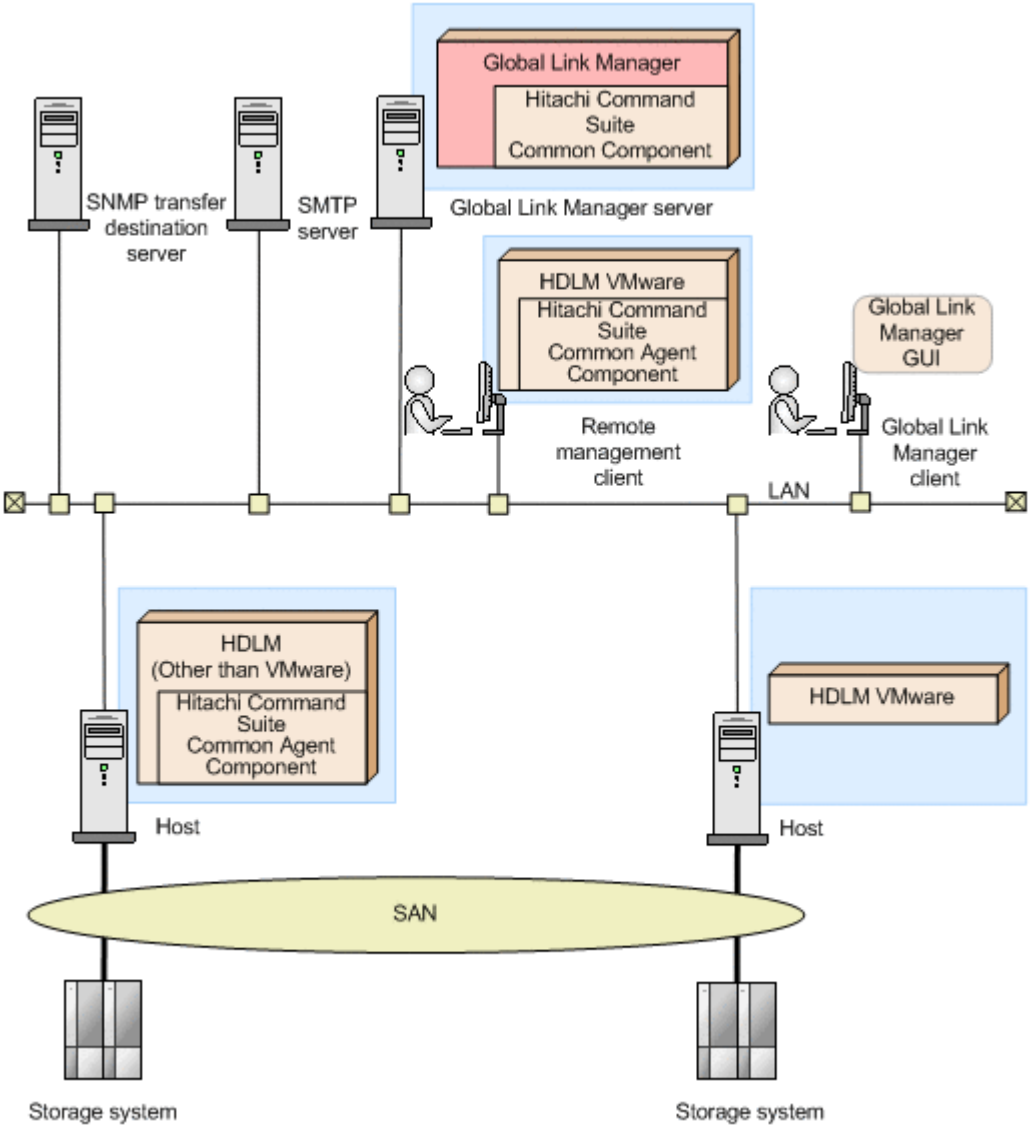

Figure 1-2 Basic Global Link Manager system configuration

The system components in this figure are explained below.

Global Link Manager server

The machine on which the Global Link Manager program is installed. The Global Link Manager server collects system configuration information from each host and then provides the information to the Global Link Manager client.

Global Link Manager receives requests from the Global Link Manager GUI and then performs the appropriate operations, such as collecting information from hosts and setting up hosts.

Hitachi Command Suite Common Component provides Hitachi Command Suite server functionality and the basic functionality of the GUI. Hitachi Command Suite Common Component is installed as part of Global Link

Manager, Device Manager, Tuning Manager, and other Hitachi Command Suite server products, and is always updated to the latest version.

Global Link Manager client

A machine on which the Global Link Manager GUI is used. The Global Link Manager GUI provides a user interface for managing hosts by using Global Link Manager.

Remote management client

A Hitachi Command Suite Common Agent Component instance or the computer the instance is installed on that connects to and controls a host via a LAN. A remote management client is required for and can only be used to manage HDLM instances installed on hosts running VMware without an underlying OS (hereafter referred to as the *VMware-version of HDLM*).

Host

A machine on which application programs are installed. In the system in which Global Link Manager is used, each host uses storage systems as external storage devices, and HDLM manages the paths between hosts and storage systems. When an ESXi hypervisor is running on a server without an underlying OS (in other words, VMware is used as the OS), the server is referred to as a *host*.

HDLM manages the paths between hosts and storage systems. HDLM improves the reliability of the system by balancing the load on paths and switching paths when a problem occurs.

For communication between the Global Link Manager server and hosts, Hitachi Command Suite Common Agent Component is required.

Hitachi Command Suite Common Agent Component refers to the component included in HDLM.

Storage system

An external storage device connected to hosts. The storage systems whose paths are managed by HDLM are subject to Global Link Manager management.

SNMP transfer destination server

A machine that receives alert information transferred from the Global Link Manager server by means of SNMP traps. You must set up the Global Link Manager server to transfer alert information to the SNMP transfer destination server. For details about the setup for transferring alert information, see Setting up alert transfer on page 3-85.

SMTP server

A machine that sends email about alert information received by the Global Link Manager server. The SMTP server is used as a mail server.

The Global Link Manager system configuration is also explained in the following locations. See the appropriate section for your environment.

- System configuration in a cluster environment: Global Link Manager cluster system configuration on page 4-2
- System configurations where Global Link Manager links with other Hitachi Command Suite products: Overview of single sign-on and user management integration for Hitachi Command Suite products on page 6-2

Global Link Manager system requirements

This section describes the Global Link Manager system requirements.

Global Link Manager server requirements

The following table describes the requirements for the machine on which the Global Link Manager server program is installed.

Table 1-1 Requirements for the machine on which the Global Link Manager server program is installed

Item	Requirements
Applicable OSs#1	• Windows Server 2012 (x64) #2 (Datacenter, Essentials, Standard) • Windows Server 2012 R2#2 (Datacenter, Essentials, Standard) • Windows Server 2016 (x64) #2 (Datacenter, Standard) • Windows Server 2019 (x64) #2 (Datacenter, Standard)
Free disk space (for a new installation)	6.5 GB or more#3 #4
Cluster software (when a cluster system is to be created)	One of the cluster services of the following OSs: • Windows Server 2012 (x64) #2 (Datacenter, Standard) • Windows Server 2012 R2#2 (Datacenter, Standard) • Windows Server 2016 (x64) #2 (Datacenter, Standard) • Windows Server 2019 (x64) #2

Item	Requirements
	(Datacenter, Standard)
Combinations of supported virtualization platforms and OSs	• VMware ESX/ESXi Server 5 (Windows Server 2012 (x64) (no SP)) • VMware ESX/ESXi Server 5 (Windows Server 2012 R2 (no SP)) • VMware ESX/ESXi Server 6 (Windows Server 2012 (x64) (no SP)) • VMware ESX/ESXi Server 6 (Windows Server 2012 R2 (no SP)) • Windows Server 2012 Hyper-V 3 (Windows Server 2012 (x64) (no SP)) • Windows Server 2012 R2 Hyper-V 3 (Windows Server 2012 R2 (no SP)) • Windows Server 2016 Hyper-V (Windows Server 2016 (x64) (no SP)) • Windows Server 2019 Hyper-V (Windows Server 2019 (x64) (no SP))

#1

To run Global Link Manager on a Hyper-V virtual machine, configure the virtual machine so that it has the same amount of memory (1 GB) as the recommended configuration.

#2

Global Link Manager installed in this OS can operate in an IPv4 or IPv6 environment.

#3

If you want to specify different drives as the installation location of Global Link Manager and the storage location of the database files, the following free space is required:

Disk on which Global Link Manager is to be installed: 3 GB or more (To enable the function for downloading the HDLM installer, an extra 1 GB of space is required.)

Disk on which the database files are to be stored: 4 GB or more

#4

To enable the function for downloading the HDLM installer, an extra 1 GB of space is required.

The guidelines for the maximum number of hosts, multipath LUs, and paths that can be managed are described in the following table.

Table 1-2 Guide to maximum numbers for Global Link Manager management targets

Management target type	Maximum number
Hosts	1500
Multipath LUs#1	15000
Paths#1#2	60000

#1

For the maximum numbers of multipath LUs and paths per host, use the following formula:

Maximum-number-of-multipath-LUs-or-paths / *Number-of-management-target-hosts*

#2

If acquisition of path availability information (path status log) for the host is enabled to output reports on path availability information, set approximately 1000 for the maximum number of paths per host on which HDLM version 5.9 or later is running.

By default, acquisition of path availability information (path status log) is disabled. To enable or disable the acquisition, use the `server.pathreport.enable` property in the property file (`server.properties`). For details on how to set the property file, see Changing Global Link Manager environment settings on page 3-33.

For details on how to output reports on path availability information, see the manual *Global Link Manager User Guide*.

Notes

- If the Global Link Manager version is 8.0 or later, Global Link Manager cannot coexist with a Hitachi Command Suite product whose version is earlier than 8.0. Therefore, make sure that the version of each Hitachi Command Suite product to be installed or upgraded is 8.0 or later.
- Global Link Manager cannot coexist with the HiRDB products listed below. Therefore, do not install Global Link Manager on a machine in which any of the following HiRDB products is already installed. Also, do not install any of the following HiRDB products on a machine in which Global Link Manager is already installed.
  - HiRDB/Single Server
  - HiRDB/Parallel Server
  - HiRDB/Workgroup Server
  - HiRDB/Run Time
  - HiRDB/Developer's Kit
  - HiRDB SQL Executor

- A static IP address must be set for the Global Link Manager server. Do not use DHCP. Connections using the IPv4 and IPv6 protocols are supported. When the IPv6 protocol is used, both IPv4 and IPv6 need to be enabled on the management server. Only global IPv6 addresses can be used.
- Before installing Global Link Manager, make sure that you set the current time for the local time of the machine on which you are going to install Global Link Manager. If the current time is not set, path availability information (path status log) might not be acquired correctly. If you want to change the time either after installing Global Link Manager or in an environment in which other Hitachi Command Suite products have been installed, see Changing the time of the machine on which Global Link Manager is installed on page 3-5.

Global Link Manager client requirements

The following table describes the system requirements for using the Global Link Manager GUI.

Table 1-3 Requirements of the client system for using the Global Link Manager GUI

Applicable OSs and other items		Applicable web browsers and requirements
Windows	Windows Server 2012 (x64) #1 (Datacenter, Essentials, Standard)	• Internet Explorer 11.0
	Windows Server 2012 R2#1 (Datacenter, Essentials, Standard)	• Internet Explorer 11.0#2
	Windows Server 2016 (x64) #1 (Datacenter, Standard)	• Internet Explorer 11.0#2
	Windows Server 2019 (x64) #1 (Datacenter, Standard)	• Internet Explorer 11.0#2
	• Windows 8.1 (32-bit)#1 (Windows 8.1, Windows 8.1 Enterprise Edition, Windows 8.1 Pro Edition) • Windows 8.1 (64-bit)#1 (Windows 8.1, Windows 8.1 Enterprise Edition, Windows 8.1 Pro Edition)	• Internet Explorer 11.0#2 • Chrome Browser for enterprise (Latest version of stable channel)
	• Windows 10 (32-bit)#1 (Windows 10 Pro, Windows 10 Education, Windows 10 Enterprise) • Windows 10 (64-bit)#1 (Windows 10 Pro, Windows 10 Education, Windows 10 Enterprise)	• Internet Explorer 11.0#2 • Chrome Browser for enterprise (Latest version of stable channel)

Applicable OSs and other items		Applicable web browsers and requirements
Linux	Red Hat Enterprise Linux 6.2	• FireFox ESR 45.x
	Red Hat Enterprise Linux 6.4	• FireFox ESR 45.x
	Red Hat Enterprise Linux 6.5	• FireFox ESR 45.x
	Red Hat Enterprise Linux 6.7	• FireFox ESR 45.x
	Red Hat Enterprise Linux 6.8	• FireFox ESR 45.x
	Red Hat Enterprise Linux 7	• FireFox ESR 68.x
	Red Hat Enterprise Linux 7.1	• FireFox ESR 68.x
	Red Hat Enterprise Linux 7.2	• FireFox ESR 68.x
	Red Hat Enterprise Linux 7.3	• FireFox ESR 68.x
	Red Hat Enterprise Linux 7.4	• FireFox ESR 68.x
	Red Hat Enterprise Linux 7.5	• FireFox ESR 68.x
	Red Hat Enterprise Linux 7.6	• FireFox ESR 68.x
	Red Hat Enterprise Linux 7.7	• FireFox ESR 68.x
	Red Hat Enterprise Linux 7.8	• FireFox ESR 68.x • FireFox ESR 78.x
	Red Hat Enterprise Linux 8	• FireFox ESR 68.x
	Red Hat Enterprise Linux 8.1	• FireFox ESR 68.x
	Red Hat Enterprise Linux 8.2	• FireFox ESR 68.x • FireFox ESR 78.x
	SUSE LINUX Enterprise Server 11 (x86) (SP4)	• FireFox ESR 45.x
Monitor resolution		SVGA (800 *x* 600) or higher

#1

Global Link Manager installed in this OS can operate in an IPv4 or IPv6 environment.

#2

If you use Internet Explorer as the web browser, do not operate the browser as an Administrator user. Operate the browser as a user who is not an Administrator user.

Note

If you are using Internet Explorer, do not enable ActiveX Filtering.

Host requirements

To use Global Link Manager to manage hosts, installation and environment setup of HDLM must be completed on the hosts.

You can use IPv4 or IPv6 to connect to Global Link Manager if the host HDLM version is 6.0 or later.

Notes

- If multiple NICs are installed, you must specify the IP address of one of them for the `server.http.socket.agentAddress` and `server.http.socket.bindAddress` properties# in Hitachi Command Suite Common Agent Component `server.properties` file on each host. If these settings are not performed, it might not be possible to add a host.

  To add a host by specifying a host name, you must have configured the network in such a way that the host name can be resolved from the IP address specified in the `server.http.socket.agentAddress` property and `server.http.socket.bindAddress` property.

  #:

  For details about the `server.http.socket.agentAddress` property and `server.http.socket.bindAddress` property in the `server.properties` file, see Appendix A, The settings of Hitachi Command Suite Common Agent Component on page A-1 in this manual.

  Even if you use an IPv6 address to add a host for which both IPv4 and IPv6 addresses are enabled, the host information might be added using an IPv4 address. To prevent this, specify an IPv6 address for the `server.http.socket.agentAddress` property and `server.http.socket.bindAddress` property in the `server.properties` file.
- A static IP address must be set for a host. Do not use DHCP.
- Before installing HDLM, make sure that you set the current time for the local time of the machine on which you are going to install the software. If the current time is not set, path availability information (path status log) might not be acquired correctly from the hosts using HDLM.

HDLM requirements

For details about the HDLM requirements, see the HDLM documentation. To manage a VMware version of HDLM, a remote management client is required. For more information about remote management clients, see the documentation regarding the VMware versions of HDLM.

For details about the installation and environment settings of HDLM, see the HDLM documentation and Appendix A, The settings of Hitachi Command Suite Common Agent Component on page A-1 in this manual.

Note

If the installed HDLM version is earlier than 6.0, the hosts cannot connect to Global Link Manager via IPv6. If IPv6 is enabled on a host, disable it. If IPv6 remains enabled, you cannot start the Hitachi Command Suite Common Agent Component service.

Operating in an IPv6 environment

Global Link Manager supports IPv6 environments. For details about the OSs on which Global Link Manager supports IPv6 environments, see Global Link Manager system requirements on page 1-7.

Limitations on operations in an IPv6 environment

Note the following limitations when you use Global Link Manager in an IPv6 environment:

- Global Link Manager does not support IPv6-only environments. Set up the OS such that both IPv4 and IPv6 can be used.
- You can only use global addresses as IPv6 addresses. Global-unique local addresses (site-local addresses), and link-local addresses cannot be used.
- When specifying the IP address or host name of the Global Link Manager server, we recommend that you use the host name. If you specify an IPv6 address, you might not be able to move from one window to another.
- In the list of hosts in the Global Link Manager GUI, hosts are managed for each IP address. Therefore, a host that has both an IPv4 address and an IPv6 address is registered as two hosts. After you migrate a host to an IPv6 environment, manually delete the IPv4 address of the host from the list of hosts. For details about the list of hosts in the Global Link Manager GUI, see the manual *Global Link Manager User Guide*.
- Because the path availability information (path status log) for a host is managed for each IP address, this information cannot be migrated even if the connection method to the host is changed from IPv4 to IPv6.

Settings for operations in an IPv6 environment

If you use Global Link Manager that has been used in an IPv4 environment in an IPv6 environment, edit the `user_httpsd.conf` file. The `user_httpsd.conf` file is stored one of the following locations:

Hitachi-Command-Suite-Common-Component-installation-folder`\uCPSB\httpsd\conf\user_httpsd.conf`

Caution

Stop Global Link Manager and Hitachi Command Suite Common Component, and then edit the `user_httpsd.conf` file. After editing the file, start Global Link Manager and Hitachi Command Suite Common Component to apply the changes.

If you want to send an SNMP trap to the management server via IPv6, you need to specify the properties in the `server.properties` file. For details about how to specify the properties, see Changing Global Link Manager environment settings on page 3-33.

Note

During a new installation of Global Link Manage in an IPv6 environment, the installer automatically sets the `Listen` line in the `httpsd.conf` file as described below.

Settings for IPv6

Remove the hash mark (`#`) at the beginning of the line `Listen [::]:22015` (when the default setting is used). Specify the same port number as specified in the `Listen` line for IPv4. The default value for the port number is `22015`.

The following shows an example of how to specify these settings:

```
Listen [::]:22015
Listen 22015
```

Caution

Do not delete or edit the existing `Listen` line. If you do this, communication using IPv4 will no longer be available.

Settings when establishing SSL communication

Remove the hash mark (`#`) at the beginning of the line `Listen [::]:22016` (when the default setting is used). Specify the same port number as specified in the `Listen` line for IPv4. The default value for the port number for SSL communication is `22016`. For details on the settings for SSL communication, see Chapter 5, Security settings for communication on page 5-1.

The following shows an example of how to specify these settings:

```
Listen [::]:22016
Listen 22016
<VirtualHost * :22016>
```

Caution

Do not delete or edit the existing `Listen` line. If you do this, communication using IPv4 will no longer be available.

Global Link Manager operation overview

This section describes the overall flow of tasks for Global Link Manager, from setup to operations. In addition, the settings necessary to start the operations and the procedures for logging in to Global Link Manager are described.

The following figure shows the flow of tasks for operating Global Link Manager.

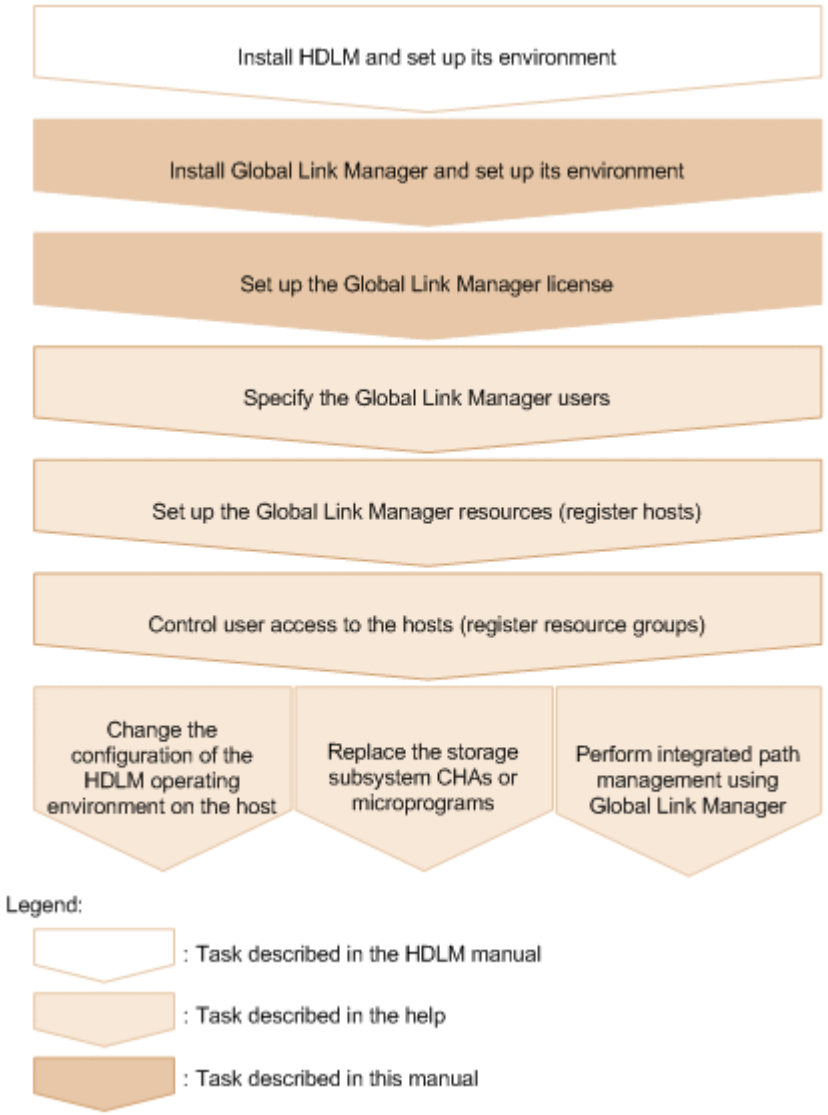

Figure 1-3 Flow of Global Link Manager tasks

Installing HDLM and setting up its environment

Set up HDLM on all hosts that are integrated and managed by Global Link Manager. For details about the requirements for installing HDLM, see Host requirements on page 1-11. For details on how to install HDLM and set up its environment on each host, see the HDLM documentation.

To use Global Link Manager to manage HDLM, you have to configure the settings to use Hitachi Command Suite Common Agent Component after setting up HDLM. For details about how to configure the settings, see Appendix A, The settings of Hitachi Command Suite Common Agent Component on page A-1.

Installing Global Link Manager and setting up its environment

Set up Global Link Manager and start the Global Link Manager server. For details about the installation and environment setup of the Global Link Manager server, see Chapter 2, Installing Global Link Manager on page

2-1 through Chapter 6, Using Global Link Manager with other products on page 6-1 for the appropriate server environment.

Setting up Global Link Manager license information during initial login

After setting up Global Link Manager, in the Global Link Manager GUI, specify the initial license. For details about how to specify the initial license, see Setting up license information during initial login on page 2-30.

For details about the flow of operations of other tasks, description of functions, and procedure details, see the manual *Global Link Manager User Guide*.

Settings required when Global Link Manager is installed

This section describes the settings that are required when Global Link Manager is installed.

Notes on using a virus scan program in the host in which a Hitachi Command Suite product operates

If a third-party software accesses the database of a Hitachi Command Suite product during server operation, server performance might go down or server failure might occur. To prevent this problem, register the following folders or directories as exemptions of virus scan in the virus scan program you are going to use.

- *HCS-installation-folder*\Base64\HDB
- *HCS-installation-folder*\HGLAM\database

HCS-installation-folder and HCS-installation-directory refer to the installation folder or directory you specify during the installation.

Note on using backup program

If a third-party software accesses the database of a Hitachi Command Suite product during server operation, server performance might go down or server failure might occur. To prevent this problem, if you are going to take backup of a drive, in which a Hitachi Command Suite product is installed, using a third-party software, stop all Hitachi Command Suite product services before performing backup.

2

Installing Global Link Manager

This chapter describes Global Link Manager installation. When installing Global Link Manager in a cluster environment, see Chapter 4, Installing Global Link Manager clusters on page 4-1.

Types of Global Link Manager installations

This section explains how to install Global Link Manager. The following types of installation are available:

- New installation#
- Reinstallation#
- Upgrade installation#
- Removal

#

An unattended installation is also available. An unattended installation allows a user to install Global Link Manager without needing to respond to instructions in dialog boxes.

After checking the items described in Preparing to install Global Link Manager on page 2-3, follow the installation procedure.

Note that the machine on which Global Link Manager version 8.2.1 or later is to be installed uses Hitachi Command Suite products version 8.0.1 or later.

Note

Note the following when performing a new installation or an upgrade installation:

- If you are using Oracle JDK 7 in the Hitachi Command Suite products and install Global Link Manager version 8.2.1 or later, the JDK being used will be changed to the JDK that is bundled with Global Link Manager.

  If SSL communication is used, you need to import the server certificate to the management server again after installing Global Link Manager. Note that, if you are using an Oracle JDK after installing Global Link Manager, use the `hcmds64chgjdk` command to change the JDK to be used, and then import the server certificate again.
- When upgrading an OS, uninstall Hitachi Command Suite before performing the upgrade. For example, uninstall Hitachi Command Suite before upgrading an OS from Windows Server 2012 to Windows Server 2012 R2.

  After upgrading the OS, install a version of Hitachi Command Suite supported by the upgraded OS, and then migrate the Hitachi Command Suite database.
- When performing an upgrade installation of Global Link Manager from a version earlier than 8 to version 8 or later, a copy of the data is always stored when migrating data from a 32-bit program to a 64-bit program. To continue using this data in products other than Global Link Manager, do not delete the data until you have upgraded all of the following products to v8 or later:
  - Device Manager
  - Tiered Storage Manager
  - Replication Manager

    - Tuning Manager
    - Compute Systems Manager

    After you have upgraded all of the above products to v8 or later, you can safely delete the copy of the data that was stored.

  - When performing an upgrade installation of Global Link Manager from a version earlier than version 8 to version 8 or later, confirm that the following services are running in the **Services** window in Windows. If both or one of them is not running, start them.

    - HiRDB/EmbeddedEdition _HD0
    - HiRDB/EmbeddedEdition _HD1

  - If you install v8.7.1 or an earlier version of Global Link Manager, the Microsoft Visual C++ 2008 Redistributable Package (x86) and the Microsoft Visual C++ 2008 Redistributable Package (x64) are also installed at the same time.
  - If you install v8.7.2 or a later version of Global Link Manager, the Microsoft Visual C++ 2013 Redistributable Package (x86) and the Microsoft Visual C++ 2013 Redistributable Package (x64) are also installed at the same time.

Reference:

  - A service pack for Global Link Manager is provided. For details on how to install a service pack, see the documentation provided with the service pack.
  - You cannot downgrade an existing installation (install a version earlier than the installed version).

Note

Precautions when uninstalling Global Link Manager:

  - When you uninstall Global Link Manager, the Microsoft Visual C++ 2008 Redistributable Package (x86) and the Microsoft Visual C++ 2008 Redistributable Package (x64) are not uninstalled. If the Microsoft Visual C++ 2008 Redistributable Package is not being used by any other product, you can uninstall it from **Programs and Features** on **Control Panel**.
  - When you uninstall Global Link Manager, the Microsoft Visual C++ 2013 Redistributable Package (x86) and the Microsoft Visual C++ 2013 Redistributable Package (x64) are not uninstalled. If the Microsoft Visual C++ 2013 Redistributable Package is not being used by any other product, you can uninstall it from **Programs and Features** on **Control Panel**.

Preparing to install Global Link Manager

Make sure of the following on the server on which Global Link Manager is to be installed before starting installation:

- You are logged on to Windows as an Administrator or a member of the Administrators group.

- The following programs are not installed:
  - Device Manager or Tuning Manager whose version is earlier than version 8.0
  - HiRDB products (HiRDB/Single Server, HiRDB/Parallel Server, HiRDB/Workgroup Server, HiRDB/Run Time, HiRDB/Developer's Kit, and HiRDB SQL Executer)
- Port number 22620 is not being used by another product.

  In Global Link Manager, the default value for the port number for receiving SNMP traps is set to 22620. If this port number is already used by another product, specify a different port number when installing Global Link Manager. If the same port number is shared by Global Link Manager and another product, even if the installation of Global Link Manager has finished successfully, you will not be able to start Global Link Manager. In such a case, in the property file (`server.properties`), disable the reception of SNMP traps or change the port number settings. For details on how to set up the property file, see Changing Global Link Manager environment settings on page 3-33.
- Products other than Hitachi Command Suite products are not using port numbers 22015, 22016, 22031, 22032, 22035, 22036, 22037, 22038, 22125, 22126, 22127, and 22128.

  If other products are using these ports, you cannot start Global Link Manager, even if the installation of Global Link Manager has finished normally. Make sure that no other products are using these ports, and then begin the installation. You can change these port numbers after the installation. For details on how to change a port number, see Changing Hitachi Command Suite Common Component port numbers on page 3-58. If these port numbers have already been changed and used in an environment where Hitachi Command Suite Common Component is installed, you can use the changed port numbers to install Global Link Manager. You do not have to change the port numbers back to the default.
- Make sure that the firewall has been set up such that socket communication within the local host is not prevented.

  Some of the firewall functions provided by the OS might terminate socket connections in the local host. You cannot install and operate Hitachi Command Suite products in an environment in which socket connections are terminated in the local host. When setting up the firewall provided by the OS, configure the settings so that socket connections cannot be terminated in the local host.
- Check whether security-monitoring programs or virus detection programs are installed.

  If security-monitoring programs or virus detection programs are installed, stop them.
- Check whether process-monitoring programs are installed.

  If process-monitoring programs are installed, stop them, or change the settings so that the services of Hitachi Command Suite Common Component and Hitachi Command Suite products (process) are not monitored.

- When using the Remote Desktop functionality, make sure that you are connected to a console session.

  Hitachi Command Suite products for Windows support the Windows Remote Desktop functionality. Note that the Microsoft terms used for this functionality differ depending on the Windows OS. The following terms can refer to the same functionality:

  - Remote Desktop for Administration
  - Remote Desktop connection

  When using the Remote Desktop functionality to perform a Hitachi Command Suite product operation (including installation or removal), you need to connect to the console session of the target server in advance. However, even if you have successfully connected to the console session, the product might not work properly if another user connects to the console session.
- Dialog boxes used for operating Windows services, such as Computer Management or Services, are not displayed.
- If a Hitachi Command Suite product has already been installed, HiRDB/EmbeddedEdition _HD1 is already running.

  To use Hitachi Command Suite products, HiRDB/EmbeddedEdition _HD1 must be always running. In the list in the Services panel, make sure that HiRDB/EmbeddedEdition _HD1 is running. If it is not running, start HiRDB/EmbeddedEdition _HD1.
- You have already set the current time of the machine on which you are going to install Global Link Manager to the local time.

Notes

- Before installing Global Link Manager on a machine in which another Hitachi Command Suite product has already been installed, back up the database. For details about how to do this, see Backing up the Global Link Manager database on page 3-8.
- You cannot install Global Link Manager when Hitachi Command Suite Common Component is installed directly under a drive letter (such as `C:\` or `D:\`).
- If you want to install Global Link Manager on the computer where Tuning Manager - Agent for SAN Switch whose version is earlier than 6.3 has been installed, you must first stop the Tuning Manager - Agent for SAN Switch services. To stop the Tuning Manager - Agent for SAN Switch services, execute the following command:

  Tuning-Manager-Agent-installation-folder`\tools\jpcstop agtw`

  Note that the Tuning Manager - Agent for SAN Switch services will not stop even if you execute the `hcmds64srv /stop` command that is used to stop Hitachi Command Suite product services.

If you use Data Execution Prevention, specify the following settings.

Settings when data execution prevention is enabled

If Data Execution Prevention (DEP) is enabled in Windows, sometimes installation cannot start. In this case, use the following procedure to disable DEP and then re-execute the installation operation.

To disable DEP:

1. Choose **Start**, **Control Panel**, and then **System**.
   The **System Properties** dialog box appears.
2. Select the **Advanced** tab, and under **Performance** click the **Settings** button.
   The **Performance Options** dialog box appears.
3. Select the **Data Execution Prevention** tab, and then select the **Turn on DEP for all programs and services except those I select** radio button.
4. Click the **Add** button, and then specify the Global Link Manager installer (`setup.exe`).
   The Global Link Manager installer (`setup.exe`) is added to the list.
5. Select the check box next to the Global Link Manager installer (`setup.exe`), and then click the **OK** button.

Installing Global Link Manager for the first time

You need to specify the following items when installing Global Link Manager for the first time. Check these items before the installation.

Table 2-1 Items you need to check before installation

Item	Description
IP address or host name of the server	Information required for setting the URL used to log in to Global Link Manager. Check the IP address or host name of the server on which Global Link Manager is to be installed, and check the port number for HBase 64 Storage Mgmt Web Service. The default value for the port number is 22015. This information is not required when another Hitachi Command Suite product has been installed.
Number of the port for HBase 64 Storage Mgmt Web Service	
Whether to receive SNMP traps	Determine in advance whether to use the function that notifies Global Link Manager of error information by using SNMP traps if an error occurs on the path to the host.
IP address for receiving SNMP traps	If you intend to use the SNMP trap receiving function, check the IP address of the SNMP trap destination. The default IP address is the IP address of the Global Link Manager server.
Number of the port for receiving SNMP traps	When you use the SNMP trap receiving function, check the port number to be used exclusively by SNMP traps. The default value for the port number is22620. If port number 22620 is already used by another program, use another port number.

To perform a new installation:

1. Insert the Global Link Manager installation DVD-ROM.

   In the displayed window, click the **Install** button next to **Hitachi Global Link Manager Software**.

   If the window does not appear, directly execute the installer (`setup.exe`).

   The installer is stored in *drive-where-installation-DVD-ROM-is-set*`:\HGLM`.

   When the installer starts, the Microsoft Visual C++ 2013 Redistributable Package (x86) and the Microsoft Visual C++ 2013 Redistributable Package (x64) are automatically installed,

   - When the installation of the redistributable package is complete, you might be prompted to restart your computer. If you are prompted to do so, restart your computer before starting the installation of Global Link Manager.
   - If the same version or a later version of the Microsoft Visual C++ 2013 Redistributable Package is already installed in the installation-destination environment, this processing is skipped.

   When this processing is complete, the **Welcome to the Installation of Hitachi Global Link Manager (New)** dialog box appears.

2. Click the **Next** button.

   The **Dynamic Link Manager Installer File Download** dialog box appears.

   Select the check box to enable the function for downloading the HDLM installer. If the download functionality is enabled, the HDLM installer file can be stored on the Global Link Manager server, and then you will be able to download the HDLM installer by using the client Web browser.

3. Click the **Next** button.

   If any services of Hitachi Command Suite Common Component or of another Hitachi Command Suite product are running, the **Stopping the Services of Hitachi Command Suite Products** dialog box appears. Click the **Next** button to stop those services.

4. Click the **Next** button.

   The **Setup of the Installation Folder** dialog box appears.

   If you do not want to accept the default installation folder, specify another installation folder. The rules for specifying an installation folder are as follows:

   - Do not specify an installation folder that is directly under a drive letter (such as `C:\` or `D:\`).
   - The maximum length of an absolute path is 64 bytes.
   - Only the following characters can be used:

     `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), underscore (_), and the space character.

     Note that you cannot specify a space character or a period at the beginning or end of a folder name.

     Furthermore, you cannot specify two or more space characters in a row.

- The path name must not contain any names reserved by the OS (`CON`, `AUX`, `NUL`, `PRN`, `CLOCK$`, `COM1` to `COM9`, and `LPT1` to `LPT9`).

You cannot install Global Link Manager under any of the following folders:

- `%ProgramFiles(x86)%\`
- `%CommonProgramFiles(x86)%\`
- `%SystemRoot%\SysWOW64\`
- `%SystemRoot%\system32\`
- `%ProgramFiles%\WindowsApps\`

The default installation folder for Global Link Manager is as follows:

system-drive`:\Program Files\HiCommand`

The default installation folder for Hitachi Command Suite Common Component is as follows:

system-drive`:\Program Files\HiCommand\Base64`

If you install Global Link Manager on a server on which other Hitachi Command Suite products are not installed, Global Link Manager and Hitachi Command Suite Common Component will be installed in the folder that is specified in the **Setup of the Installation Folder** dialog box. If you install Global Link Manager on a server on which other Hitachi Command Suite products are installed, Global Link Manager will be installed in the folder that is specified in the **Setup of the Installation Folder** dialog box, but Hitachi Command Suite Common Component will be installed in the folder that contains the existing Hitachi Command Suite Common Component, and overwrites it. If you want to check the installation folder for Hitachi Command Suite Common Component, check the following registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Hitachi\HiCommand Base 64\InstallPath`

5. Click the **Next** button.

   The **Setup of the Storage Destination for Database Files of Hitachi Global Link Manager** dialog box appears.

   If you do not want to accept the default folder, specify another folder. The rules for specifying a folder are as follows:

   - Do not specify a storage destination folder for database files that is directly under a drive letter (such as `C:\` or `D:\`).
   - The maximum length of an absolute path is 64 bytes.
   - Only the following characters can be used:

     `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), underscore (`_`), and the space character.

     Note that you cannot specify a space character or a period at the beginning or end of a folder name.

     Furthermore, you cannot specify two or more space characters in a row.
   - The path name must not contain any names reserved by the OS (`CON`, `AUX`, `NUL`, `PRN`, `CLOCK$`, `COM1` to `COM9`, and `LPT1` to `LPT9`).

   You cannot install Global Link Manager under any of the following folders:

- `%ProgramFiles(x86)%\`
- `%CommonProgramFiles(x86)%\`
- `%SystemRoot%\SysWOW64\`
- `%SystemRoot%\system32\`
- `%ProgramFiles%\WindowsApps\`

Note

The database files of Hitachi Global Link Manager are created under the *specified-storage-destination*`\x64` folder.

6. Click the **Next** button.

   If this installation will install the 64-bit version of Hitachi Command Suite Common Component for the first time in an environment where the 32-bit version of Hitachi Command Suite Common Component exists, the **Setup of the data backup storage folder for database files** of Hitachi Command Suite dialog box appears.

   To upgrade the Hitachi Command Suite products from v7 or earlier to v8, specify a storage destination for the database files of Hitachi Command Suite products. If you want to use a folder different from the default, follow the rules below to specify the folder:

   - Absolute paths must be 150 bytes or less.
   - Only the following characters can be used:

     `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), underscore (_), and the space character.

     Note that you cannot specify a space character or a period at the beginning or end of a folder name.

     Furthermore, you cannot specify two or more space characters in a row.
   - The path name must not contain any names reserved by the OS (`CON`, `AUX`, `NUL`, `PRN`, `CLOCK$`, `COM1` to `COM9`, and `LPT1` to `LPT9`).

   The following is the default database storage destination for the Hitachi Command Suite products:

   specified-installation-folder-for-Hitachi-Global-Link-Manager`\databackup`

7. Click the **Next** button.

   The **Setup of Information about the Server of Hitachi Global Link Manager** dialog box appears.

   Specify the following information (confirm the information before you start installation):

   - IP address or host name of the server
   - Port number for HBase 64 Storage Mgmt Web Service
   - Enabling or disabling reception of an SNMP trap

   When you install Global Link Manager in an environment in which no other Hitachi Command Suite product has been installed, the automatically detected IP address is displayed as the IP address or host name of the server. If nothing is displayed, enter the IP address or host

name of the server. When specifying an IPv6 address, enclose the IP address in square brackets ([ ]).

If another Hitachi Command Suite product has already been installed, the fields for the following information are disabled:

- IP address or host name of the server
- Port number for HBase 64 Storage Mgmt Web Service

Notes

- In some network environments, the host might have multiple IP addresses. If the host has multiple IP addresses, the first detected IP address is displayed. Make sure that the detected IP address is correct.
- The host name must be no more than 128 bytes. You can use the following characters:

  A to Z, a to z, 0 to 9, period (.), -

  Note that the host name cannot start or end with a hyphen (-).

8. Click the **Next** button.

   If you have enabled the SNMP trap receiving function, the **SNMP Trap Connection Settings for Hitachi Global Link Manager** dialog box appears. If you have disabled this function, go to step 9.

   Specify the following information (check the information before you start installation):

   - IP address for receiving SNMP traps (IPv4 address or IPv6 address)
   - Port number for receiving SNMP traps

   The IP address of the Global Link Manager server is displayed as the IP address for receiving SNMP traps. If nothing is displayed, enter the IP address of the server.

   When specifying an IPv6 address, enclose the IP address in square brackets ([ ]).

   Note

   When you install Global Link Manager on a server on which Device Manager is installed, specify a port number other than 162 for the port that receives SNMP traps. When the reception of SNMP traps is being used in Device Manager, if you specify 162 for the port that receives SNMP traps during the installation of Global Link Manager, you will no longer be able to start Device Manager.

9. Click the **Next** button.

   If Windows Firewall is installed, the **Windows Firewall** dialog box appears. Check the information on the **Exceptions** tab, and then click the **Next** button. Hitachi Command Suite Common Component and the port that receives SNMP traps will be added to the Windows Firewall exceptions list.

   Note

   If you register Global Link Manager as an exception in the Windows Firewall exceptions list, it might take approximately 15 minutes more

to install Global Link Manager. If you enabled Windows Firewall after installing Global Link Manager, you must manually add Global Link Manager to the exceptions list. For details on how to manually add Global Link Manager to the exception list, see Settings for Windows firewalls on page 3-67.

10. After installation, select whether to start the services of Hitachi Command Suite products.

    A dialog box appears, asking you whether you want to start the services of Hitachi Command Suite products after installation. If you want to enter the license key after installation, we recommend that you click the **Yes** button.

    When you click the **Yes** or **No** button, the **Confirmation Before Installation** dialog box appears.

11. Confirm that the displayed installation settings are correct, and then click the **Install** button.

    Installation starts. During the installation, dialog boxes indicating the processing status appear. When the **HGLM Settings Complete** dialog box appears, confirm the settings you specified during installation.

    If a value specified for **URL for the HGLM login window** does not match the information on the server on which Global Link Manager is installed, see the appropriate reference below and change the value:

    - For details on how to change the IP address, see Changing the Global Link Manager login URL on page 3-64.
    - For details on how to change the host name, see Changing the Global Link Manager server host name on page 3-56.
    - For details on how to change the port number of HBase 64 Storage Mgmt Web Service, see Changing port numbers for accessing the HBase 64 Storage Mgmt Web Service on page 3-60.

12. Click the **Next** button.

    When installation has been completed normally, the **Installation Complete** dialog box appears.

13. Click the **Finish** button to finish the installation.

    The operating status of the Hitachi Command Suite Common Component services varies depending on the setup status specified during installation.

    To log in to Global Link Manager and start operations, you must set up the initial license information. See Setting up license information during initial login on page 2-30.

When using report output of path availability information

For the hosts running HDLM version 5.9 or later, you can output path availability information as a report. To use the function to output reports on path availability information, you need to modify the `server.pathreport.enable` property in the property file (`server.properties`). For details on how to set the property file, see Changing Global Link Manager environment settings on page 3-33.

Reinstalling Global Link Manager

If files of the installed Global Link Manager program are damaged, they can be restored by performing an overwrite installation (reinstallation), using the same Global Link Manager program version as the one already installed.

Before starting a reinstallation, make sure that the preparation for installation described in Preparing to install Global Link Manager on page 2-3 has been completed.

To perform a reinstallation:

1. Insert the Global Link Manager installation DVD-ROM.

   In the displayed window, click the **Install** button next to **Hitachi Global Link Manager Software**.

   If the window does not appear, directly execute the installer (`setup.exe`).

   The installer is stored in *drive-where-installation-DVD-ROM-is-set*`:\HGLM`.

   When the installer starts, the Microsoft Visual C++ 2013 Redistributable Package (x86) and the Microsoft Visual C++ 2013 Redistributable Package (x64) are automatically installed,

   - When the installation of the redistributable package is complete, you might be prompted to restart your computer. If you are prompted to do so, restart your computer before starting the installation of Global Link Manager.
   - If the same version or a later version of the Microsoft Visual C++ 2013 Redistributable Package is already installed in the installation-destination environment, this processing is skipped.

   When this processing is complete, the **Welcome to the Installation of Hitachi Global Link Manager (Overwrite)** dialog box appears.

2. Click the **Next** button.

   The **Dynamic Link Manager Installer File Download** dialog box appears.

   Select the check box to enable the function for downloading the HDLM installer. If the download functionality is enabled, the HDLM installer file can be stored on the Global Link Manager server, and then you will be able to download the HDLM installer by using the client Web browser.

   If the HDLM installer is already installed with the download function enabled, this dialog box is not displayed.

3. Click the **Next** button.

   If any services of Hitachi Command Suite Common Component or of another Hitachi Command Suite product are running, either of the following dialog boxes will appear:

   - The **Stopping the Services of Hitachi Command Suite Products** dialog box appears. Click the **Next** button to stop those services.

4. Click the **Next** button.

   If Windows Firewall is installed, the **Windows Firewall** dialog box appears. Check the settings in the dialog box, and then click the **Next**

button. Hitachi Command Suite Common Component and the port that receives SNMP traps will be added to the Windows Firewall exceptions list.

Note

If you register Global Link Manager as an exception in the Windows Firewall exceptions list, it might take approximately 15 minutes more to install Global Link Manager. If you enabled Windows Firewall after installing Global Link Manager, you must manually add Global Link Manager to the exceptions list. For details on how to manually add Global Link Manager to the exception list, see Settings for Windows firewalls on page 3-67.

5. After installation, select whether to start the services of Hitachi Command Suite products.

   A dialog box appears, asking you whether you want to start the services of Hitachi Command Suite products after installation.

   - Select whether to start the services after installation (optional).

   When you click the **Yes** or **No** button, the **Confirmation Before Installation** dialog box appears.

6. Confirm that the displayed installation settings are correct, and then click the **Install** button.

   Installation starts. During the installation, dialog boxes indicating the processing status appear. The Global Link Manager database is not initialized by an overwrite installation (except when the database files are damaged). When the **HGLM Settings Complete** dialog box appears, confirm the settings you specified during installation.

   If a value specified for **URL for the HGLM login window** does not match the information on the server on which Global Link Manager is installed, see the appropriate reference below and change the value:

   - For details on how to change the IP address, see Changing the Global Link Manager login URL on page 3-64.
   - For details on how to change the host name, see Changing the Global Link Manager server host name on page 3-56.
   - For details on how to change the port number of HBase 64 Storage Mgmt Web Service, see Changing port numbers for accessing the HBase 64 Storage Mgmt Web Service on page 3-60.

7. Click the **Next** button.

   When installation has been completed normally, the **Installation Complete** dialog box appears.

8. Click the **Finish** button to finish the installation.

   The operating status of the Hitachi Command Suite Common Component service varies depending on the setup status specified during installation. When Global Link Manager is installed on a standby node in a cluster configuration, the services will not start. Specify the settings for operating Global Link Manager in a cluster configuration.

Upgrade installation of Global Link Manager

When you want to update the version of the instance of Global Link Manager that is already installed, perform an upgrade installation.

Before starting an upgrade installation, make sure that the preparation for installation described in Preparing to install Global Link Manager on page 2-3 has been completed.

Notes

- Before you upgrade Global Link Manager, secure sufficient free disk space. The required free space on the disk where the database files are to be stored is 4 GB.
- If you perform an upgrade installation of Hitachi Global Link Manager from a version earlier than v8 to v8 or later:
  - The URL for activating the Global Link Manager GUI changes to `http://`*server-IP-address-or-host-name*`:22015/GlobalLinkAvailabilityManager/`.
  - Command names for Hitachi Command Suite Common Components change from `hcmds`*XXXX* to `hcmds64`*XXXX*.
  - If the version of Hitachi Global Link Manager is earlier than v8, and it is installed in a 32-bit folder on Windows, the installation destination changes as follows.

Table 2-2 Changes in installation destination when upgrading

Before upgrade installation	After upgrade installation
`%SystemRoot%\SysWOW64`	`%ProgramFiles%`
`%ProgramFiles(x86)%`	`%ProgramFiles%`
`%CommonProgramFiles(x86)%`	`%CommonProgramFiles%`

  - The default (22032) is set to the port number that HiRDB uses. Therefore, if you are using a port number other than the default to perform operations, you need to reset the port number later. Write down the port number you are using so that you can set the port number again.
- If you performed an upgrade installation of Global Link Manager from a version earlier than v7.5.0, change the `server.agent.max_retry_count` property in the `server.properties` file according to the following procedure:

  a. Open the following file with a text editor:
  Global-Link-Manager-installation-folder`\conf\server.properties`

  b. Set the server.agent.max_retry_count property to 110 as follows:

```
server.agent.max_retry_count=110
```

  c. Save the file, and then restart Global Link Manager.

- If the following settings have been specified in a version of Global Link Manager prior to v8, you must specify the settings again after an upgrade installation:
  - Changing the Global Link Manager database password
  - Security Settings for Communication

The procedure for each of the following upgrade installations is explained:

- Upgrading to a later release of the same major version
- Upgrading from version 6 or version 7 to version 8.0 or later
- Migrating the data of the currently-installed Global Link Manager to a different server and then upgrading to version 8.0 or later
  - Using Global Link Manager version 6 or 7 on an OS that is not supported by Global Link Manager version 8.0 or later
  - Using Global Link Manager version 5

Upgrading to a later release of the same major version

To perform an upgrade installation to a later release of the same major version, perform the following steps:

1. Insert the Global Link Manager installation DVD-ROM.

   In the displayed window, click the **Install** button next to **Hitachi Global Link Manager Software**.

   If the window does not appear, directly execute the installer (`setup.exe`).

   The installer is stored in *drive-where-installation-DVD-ROM-is-set*`:\HGLM`.

   When the installer starts, the Microsoft Visual C++ 2013 Redistributable Package (x86) and the Microsoft Visual C++ 2013 Redistributable Package (x64) are automatically installed,

   - When the installation of the redistributable package is complete, you might be prompted to restart your computer. If you are prompted to do so, restart your computer before starting the installation of Global Link Manager.
   - If the same version or a later version of the Microsoft Visual C++ 2013 Redistributable Package is already installed in the installation-destination environment, this processing is skipped.

   When this processing is complete, the **Welcome to the Installation of Hitachi Global Link Manager (Upgrade)** dialog box appears.

2. Click the **Next** button.

   The **Dynamic Link Manager Installer File Download** dialog box appears.

   Select the check box to enable the function for downloading the HDLM installer. If the download functionality is enabled, the HDLM installer file can be stored on the Global Link Manager server, and then you will be able to download the HDLM installer by using the client Web browser.

   If the HDLM installer is already installed with the download function enabled, this dialog box is not displayed.

3. Click the **Next** button.

   If any services of Hitachi Command Suite Common Component or of another Hitachi Command Suite product are running, either of the following dialog boxes will appear:

   - The **Stopping the Services of Hitachi Command Suite Products** dialog box appears. Click the **Next** button to stop those services.

4. Click the **Next** button.

   If Windows Firewall is installed, the **Windows Firewall** dialog box appears. Check the settings in the dialog box, and then click the **Next** button. Hitachi Command Suite Common Component and the port that receives SNMP traps will be added to the Windows Firewall exceptions list.

   Note

   If you register Global Link Manager as an exception in the Windows Firewall exceptions list, it might take approximately 15 minutes more to install Global Link Manager. If you enabled Windows Firewall after installing Global Link Manager, you must manually add Global Link Manager to the exceptions list. For details on how to manually add Global Link Manager to the exception list, see Settings for Windows firewalls on page 3-67.

5. After installation, select whether to start the services of Hitachi Command Suite products.

   A dialog box appears, asking you whether you want to start the services of Hitachi Command Suite products after installation.

   - Select whether to start the services after installation (optional).

   When you click the **Yes** or **No** button, the **Confirmation Before Installation** dialog box appears.

6. Confirm that the displayed installation settings are correct, and then click the **Install** button.

   Installation starts. During the installation, dialog boxes indicating the processing status appear. The Global Link Manager database is updated by running an upgrade installation (except when the database files are damaged). When the **HGLM Settings Complete** dialog box appears, confirm the settings you specified during installation.

   If a value specified for **URL for the HGLM login window** does not match the information on the server on which Global Link Manager is installed, see the appropriate reference below and change the value:

   - For details on how to change the IP address, see Changing the Global Link Manager login URL on page 3-64.
   - For details on how to change the host name, see Changing the Global Link Manager server host name on page 3-56.
   - For details on how to change the port number of HBase 64 Storage Mgmt Web Service, see Changing port numbers for accessing the HBase 64 Storage Mgmt Web Service on page 3-60.

7. Click the **Next** button.

   When installation has been completed normally, the **Installation Complete** dialog box appears.

8. Click the **Finish** button to finish the installation.

   The operating status of the Hitachi Command Suite Common Component service varies depending on the setup status specified during installation. When Global Link Manager is installed on a standby node in a cluster configuration, the services will not start. Specify the settings for operating Global Link Manager in a cluster configuration.

Upgrading from version 6 or version 7 to version 8.0 or later

To upgrade from version v6 or v7 to v8.0 or later, perform the following steps:

1. Insert the Global Link Manager installation DVD-ROM.

   In the displayed window, click the **Install** button next to **Hitachi Global Link Manager Software**.

   If the window does not appear, directly execute the installer (`setup.exe`).

   The installer is stored in *drive-where-installation-DVD-ROM-is-set*`:\HGLM`.

   When the installer starts, the Microsoft Visual C++ 2013 Redistributable Package (x86) and the Microsoft Visual C++ 2013 Redistributable Package (x64) are automatically installed,

   - When the installation of the redistributable package is complete, you might be prompted to restart your computer. If you are prompted to do so, restart your computer before starting the installation of Global Link Manager.
   - If the same version or a later version of the Microsoft Visual C++ 2013 Redistributable Package is already installed in the installation-destination environment, this processing is skipped.

   When this processing is complete, the **Welcome to the Installation of Hitachi Global Link Manager (Upgrade)** dialog box appears.

2. Click the **Next** button.

   The **Dynamic Link Manager Installer File Download** dialog box appears.

   Select the check box to enable the function for downloading the HDLM installer. If the download functionality is enabled, the HDLM installer file can be stored on the Global Link Manager server, and then you will be able to download the HDLM installer by using the client Web browser.

3. Click the **Next** button.

   If any services of Hitachi Command Suite Common Component or of another Hitachi Command Suite product are running, either of the following dialog boxes will appear:

   - The **Stopping the Services of Hitachi Command Suite Products** dialog box appears. Click the **Next** button to stop those services.

4. Click the **Next** button.

   If this installation will install the 64-bit version of Hitachi Command Suite Common Component for the first time in an environment where the 32-bit version of Hitachi Command Suite Common Component exists, the **Setup**

of the data backup storage folder for database files of Hitachi Command Suite dialog box appears.

To upgrade the Hitachi Command Suite products from v7 or earlier to v8, specify a storage destination for the database files of Hitachi Command Suite products. If you want to use a folder different from the default, follow the rules below to specify the folder:

- Absolute paths must be 150 bytes or less.
- Only the following characters can be used:

  `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), underscore (`_`), and the space character.

  Note that you cannot specify a space character or a period at the beginning or end of a folder name.

  Furthermore, you cannot specify two or more space characters in a row.
- The path name must not contain any names reserved by the OS (`CON`, `AUX`, `NUL`, `PRN`, `CLOCK$`, `COM1` to `COM9`, and `LPT1` to `LPT9`).

The following is the default database storage destination for the Hitachi Command Suite products:

specified-installation-folder-for-Hitachi-Global-Link-Manager`\databackup`

5. Click the **Next** button.

   The property files of Hitachi Global Link Manager and the **Setup of the data backup storage folder for path status log and property files of Hitachi Global Link Manager** dialog box appear. If you want to use a folder different from the default, follow the rules below to specify the folder:

   - Absolute paths must be 140 bytes or less.
   - Only the following characters can be used:

     `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), underscore (`_`), and the space character.

     Note that you cannot specify a space character or a period at the beginning or end of a folder name.

     Furthermore, you cannot specify two or more space characters in a row.
   - The path name must not contain any names reserved by the OS (`CON`, `AUX`, `NUL`, `PRN`, `CLOCK$`, `COM1` to `COM9`, and `LPT1` to `LPT9`).

   The following is the default storage destination for the property files of Hitachi Global Link Manager and the path availability information:

   specified-installation-folder-for-Hitachi-Global-Link-Manager`\databackup`

6. Click the **Next** button.

   If Windows Firewall is installed, the **Windows Firewall** dialog box appears. Check the settings in the dialog box, and then click the **Next** button. Hitachi Command Suite Common Component and the port that receives SNMP traps will be added to the Windows Firewall exceptions list.

   Note

If you register Global Link Manager as an exception in the Windows Firewall exceptions list, it might take approximately 15 minutes more to install Global Link Manager. If you enabled Windows Firewall after installing Global Link Manager, you must manually add Global Link Manager to the exceptions list. For details on how to manually add Global Link Manager to the exception list, see Settings for Windows firewalls on page 3-67.

7. After installation, select whether to start the services of Hitachi Command Suite products.

   A dialog box appears, asking you whether you want to start the services of Hitachi Command Suite products after installation. However, this dialog box does not appear when Global Link Manager is installed on a standby node in a cluster configuration. In this case, go to step 8.

   - Select whether to start the services after installation (optional).

   When you click the **Yes** or **No** button, the **Confirmation Before Installation** dialog box appears.

8. Confirm that the displayed installation settings are correct, and then click the **Install** button.

   Installation starts. During the installation, dialog boxes indicating the processing status appear. The Global Link Manager database is updated by running an upgrade installation (except when the database files are damaged). When the **HGLM Settings Complete** dialog box appears, confirm the settings you specified during installation.

   If a value specified for **URL for the HGLM login window** does not match the information on the server on which Global Link Manager is installed, see the appropriate reference below and change the value:

   - For details on how to change the IP address, see Changing the Global Link Manager login URL on page 3-64.
   - For details on how to change the host name, see Changing the Global Link Manager server host name on page 3-56.
   - For details on how to change the port number of HBase 64 Storage Mgmt Web Service, see Changing port numbers for accessing the HBase 64 Storage Mgmt Web Service on page 3-60.

9. Click the **Next** button.

   When installation has been completed normally, the **Installation Complete** dialog box appears.

10. Click the **Finish** button to finish the installation.

    The operating status of the Hitachi Command Suite Common Component service varies depending on the setup status specified during installation.

Notes

- The following settings are not inherited after upgrade installations from v6 or v7. Configure these settings again after the upgrade installation.

  - SSL settings

- JDK settings if you have performed a procedure to directly change the JDK configuration file

- After an upgrade installation, the port for the Hitachi Command Suite Common Component services changes to `22015`. Accordingly, the port number that is specified in the server access URL for Hitachi Global Link also changes to `22015`.

  For details on how to change the URL, see Changing the Global Link Manager login URL on page 3-64 after the upgrade installation.

- When you upgrade Hitachi Global Link Manager to v8, Hitachi Global Link Manager and other Hitachi Command Suite products might not work properly if Hitachi Command Suite v6 or v7 products exist on the same machine and you start operating the updated Hitachi Global Link Manager. Therefore, upgrade all Hitachi Command Suite products, including Hitachi Link Manager, to v8 before you start operating them.

- The storage destination for the database files changes to the following:

  original-storage-destination-path-for-database-files`\x64`

- If you upgrade from v6 or v7 to v8, maintenance information is deleted. Therefore, collect any necessary maintenance information before upgrading to v8. For details on how to collect maintenance information, see the manual *Global Link Manager User Guide* for the version that will be upgraded.

Migrating the data of the currently-installed Global Link Manager to a different server and then upgrading to version 8.0 or later

To migrate the data of the currently-installed Global Link Manager to a different server and to then upgrade to v8.0 or later, perform the following steps:

1. Export the database of the host at the migration source.
2. At the migration destination, perform a new installation of Global Link Manager version 6 or 7.
3. Import the database to Global Link Manager version 6 or 7 of the migration destination.
4. At the migration destination, upgrade Global Link Manager to version 8.

For details about each step, see the manual for the Global Link Manager version.

When using report output of path availability information

For the hosts running HDLM version 5.9 or later, you can output path availability information as a report. To use the function to output reports on path availability information, you need to modify the `server.pathreport.enable` property in the property file (`server.properties`). For details on how to set the property file, see Changing Global Link Manager environment settings on page 3-33.

When an attempt to update the database has failed

If message KAIF40094-E appears indicating that the database could not be updated, you must manually update the database.

To update the Global Link Manager database:

1. Execute the following command to make sure that Hitachi Command Suite Common Component is running:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /status

   If it is running, execute the following command:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /stop

2. Execute the following command to start HiRDB:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64dbsrv /start

3. Execute the following command to update the Global Link Manager database:

   Global-Link-Manager-installation-folder\bin\hglamdbupdate

   The following confirmation message appears. Enter Y to continue.

   "Are you sure to execute the database update command? (Y/N)"

   You can specify the following options in the hglamdbupdate command.

Table 2-3 hglamdbupdate command options

Item	Description
-x	Specify this option to suppress the output of messages and error messages during updating of the database. Note, however, that option error messages will be displayed even though you specify this option.
-f *message-output-file*	Specify this option to save messages and error messages output during updating of the database in a file. You can specify a relative path or an absolute path. Specify a path by using 255 bytes or less. Only the following characters can be used: A to Z, a to z, 0 to 9, period (.), and underscore (_). You can also use a backslash (\), and colon (:) as the path delimiter.
-s	Specify this option to suppress the output of a message asking for confirmation of the requested operation.

4. Execute the following command to stop HiRDB:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64dbsrv /stop

5. Execute the following command to start Hitachi Command Suite Common Component:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64srv /start
```

Performing an unattended installation of Global Link Manager

An unattended installation is an installation in which Global Link Manager is installed based on the responses predefined in the installation-information settings file instead of user responses. The following shows the processing flow of unattended installation:

1. Define information necessary for installing Global Link Manager in the installation-information settings file. You can also install Global Link Manager without defining any information in this file. For details on this file, see Contents of the installation-information settings file on page 2-24.
2. Execute the installation command (`installhglm`)# to start the installation.
3. The necessary responses are automatically determined based on the installation-information settings file.
4. Installation is completed. Log data about the progress and result of installation is output.

#

If the UAC feature is enabled in a Windows OS, when you execute a command, you might be asked to elevate your current privileges to Administrator privileges. If you are asked, execute the command with elevated privileges.

Unattended installation

To perform an unattended installation:

1. Insert the Global Link Manager installation DVD-ROM.

   In the displayed window, click the **Install** button next to **Hitachi Global Link Manager Software**.

   If the window does not appear, directly execute the installer (`setup.exe`).

   The installer is stored in *drive-where-installation-DVD-ROM-is-set*:`\HGLM`.

   When the installer starts, the Microsoft Visual C++ 2013 Redistributable Package (x86) and the Microsoft Visual C++ 2013 Redistributable Package (x64) are automatically installed,

   - When the installation of the redistributable package is complete, you might be prompted to restart your computer. If you are prompted to do so, restart your computer before starting the installation of Global Link Manager.

- If the same version or a later version of the Microsoft Visual C++ 2013 Redistributable Package is already installed in the installation-destination environment, this processing is skipped.

When this processing is complete, the **Welcome to the Installation of Hitachi Global Link Manager** dialog box appears.

2. Click the **Cancel** button.

   A dialog box appears, asking you whether you want to cancel the installation.

3. Click the **Yes** button.

   The dialog box closes.

4. Execute the following command to start an unattended installation:

   `drive-in-which-the-installation-DVD-ROM-is-set:\HGLM\GLMTools\installhglm [/f name-of-the-installation-information-settings-file] [/s]`

   You can specify the following options in the `installhglm` command.

Table 2-4 installhglm command options

Item	Description
`/f` *installation-information-settings-file*	If the installation-information settings file has been created, specify the location where that file is stored. You can specify a relative path or an absolute path. Specify a path by using 255 bytes or less. Only the following characters can be used: `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), underscore (`_`), and the space character. You can also use a backslash (`\`), and colon (`:`) as the path delimiter. If you do not specify this option, the default location for the installation-information settings file is used. For details on this file, see Contents of the installation-information settings file on page 2-24.
`/s`	Specify this option to suppress the output of a message asking for confirmation of the requested operation.

Executing the command starts the installation. You cannot stop the installation once the installation starts. Do not force the installation to terminate, for example by using **Ctrl** + **C**.

After the installation finishes successfully, the message `KAIF40111-I` will be output. If it is not output, follow the instructions provided by the messages that are output.

Also, the installation results will be output to the log file (`installhglm_`*yyyy-mm-dd_hh-mm-ss*`.log`#). For details about `installhglm.log`, see About the log file on page 2-28.

#

yyyy-mm-dd_hh-mm-ss represents year, month, date, hour, minute, and second respectively.

Contents of the installation-information settings file

Global Link Manager provides a sample file of the installation-information settings file. The following shows the path to this file:

drive-in-which-the-installation-DVD-ROM-is-set:\HGLM\GLMTools\sample_installhglm.ini

The following shows the contents of the sample file:

```
[INSTALLATION_SETTINGS]
HGLM_INSTDIR="C:\Program Files\HiCommand"
HGLM_DBDIR="C:\Program Files\HiCommand\HGLAM\database"
HGLM_IPADDRESS=
HGLM_PORT=22015
HGLM_SNMPTRAP=TRUE
HGLM_SNMPIPADDRESS=
HGLM_SNMPIPV6ADDRESS=
HGLM_SNMPTRAPPORT=22620
HGLM_RUNSERVICE=TRUE
HGLM_DBTMPDIR="C:\Program Files\HiCommand\databackup"
HGLM_DATATMPDIR="C:\Program Files\HiCommand\databackup"
HGLM_HDLMINSTALLDOWNLOAD=FALSE
[EOF]
```

If you plan to set up a cluster environment, specify a key such as `HGLM_CLUSTER_SETUP`. The following shows the contents of the definition for setting up a cluster environment:

```
[INSTALLATION_SETTINGS]
HGLM_INSTDIR="C:\Program Files\HiCommand"
HGLM_DBDIR="X:\HiCommand\HGLAM\database"
HGLM_IPADDRESS=HCSClientAccessPoint
HGLM_PORT=22015
HGLM_SNMPTRAP=TRUE
HGLM_SNMPIPADDRESS=
HGLM_SNMPIPV6ADDRESS=
HGLM_SNMPTRAPPORT=22620
HGLM_RUNSERVICE=FALSE
HGLM_DBTMPDIR="C:\Program Files\HiCommand\databackup"
HGLM_DATATMPDIR="C:\Program Files\HiCommand\databackup"
HGLM_CLUSTER_SETUP=TRUE
HGLM_CLUSTER_MODE=2
HGLM_CLUSTER_RESOURCEGROUPNAME=HCSClusterServices
HGLM_CLUSTER_HOSTNAME_ACTIVE=activenodehost
HGLM_CLUSTER_HOSTNAME_STANDBY=standbynodehost
HGLM_HDLMINSTALLDOWNLOAD=FALSE
[EOF]
```

If you want to edit the `sample_installhglm.ini` file, copy the file to another folder, and then edit the copied file.

Define the responses for an unattended installation in the `[INSTALLATION_SETTINGS]` section. Note the following when you define the responses:

- A line that begins with a hash mark (`#`) is treated as a comment line. If you specify `#` at the beginning of the section name, all the properties defined in this section will be treated as comments, and the default values will be applied.
- Any line feed is ignored.

Contents

The following table describes the keys that can be specified in the `[INSTALLATION_SETTINGS]` section, and the types of installation you can specify each key for.

Table 2-5 Keys that can be specified in the [INSTALLATION_SETTINGS] section

Key name	Description	Key is specifiable for:
`HGLM_INSTDIR`	Specify an absolute path (maximum of 64 bytes) for the installation folder. Only the following characters can be used: `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), underscore (`_`), and the space character. You can also use a backslash (`\`), and colon (`:`) as the path delimiter. The default is usually `C:\Program Files\HiCommand` . The following folders cannot be specified: • `%ProgramFiles(x86)%\` • `%CommonProgramFiles(x86)%\` • `%SystemRoot%\SysWOW64\` • `%SystemRoot%\system32\` • `%ProgramFiles%\WindowsApps\`	New installation, or upgrade installation from version 6 or version 7
`HGLM_DBDIR`	Specify an absolute path (maximum of 64 bytes) for the storage destination of the database. Only the following characters can be used: `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), underscore (`_`), and the space character. You can also use a backslash (`\`), and colon (`:`) as the path delimiter. The default is usually `C:\Program Files\HiCommand\HGLAM\database` . The following folders cannot be specified: • `%ProgramFiles(x86)%\` • `%CommonProgramFiles(x86)%\`	New installation, or upgrade installation from version 6 or version 7

Key name	Description	Key is specifiable for:
	• %SystemRoot%\SysWOW64\ • %SystemRoot%\system32\ • %ProgramFiles%\WindowsApps\	
HGLM_IPADDRESS	Specify the IP address or host name of the Global Link Manager server. When specifying an IPv6 address, enclose the IP address in square brackets ([ ]). The default is *IP-address-of-the-Global-Link-Manager-server*. When setting a cluster, specify the logical host name.	New installation
HGLM_PORT	Specify the port number of the Global Link Manager server. The default is 22015.	New installation, or upgrade installation from version 6 or version 7
HGLM_SNMPTRAP	Specify whether to receive SNMP traps. TRUE: SNMP traps will be received. FALSE: SNMP traps will not be received. The default is TRUE.	New installation
HGLM_SNMPIPADDRESS	Specify the IPv4 address for receiving SNMP traps. The default is *IP-address-of-the-Global-Link-Manager-server*.	New installation
HGLM_SNMPIPV6ADDRESS	Specify the IPv6 address for receiving SNMP traps. Enclose the IP address in square brackets ([ ]). The default is *IP-address-of-the-Global-Link-Manager-server*.	New installation
HGLM_SNMPTRAPPORT	Specify the port number for receiving SNMP traps. The default is 22620.	New installation
HGLM_RUNSERVICE	Specify whether to start the service after the installation finishes. TRUE: The service will be started. FALSE: The service will not be started. The default is TRUE. For a new, upgrade, or overwrite installation in a cluster environment, even if you specify TRUE, the service is not started after the installation finishes.	New installation, upgrade installation, or reinstallation
HGLM_DBTMPDIR	Specify an absolute path for the database-information backup folder for Hitachi Command Suite products (which include Global Link Manager).	Upgrade installation from version 6 or version 7

Key name	Description	Key is specifiable for:
	The default is usually `C:\Program Files\HiCommand\databackup` .	
`HGLM_DATATMPDIR`	Specify an absolute path for the database-information backup folder for the path status log, property files, and log files for Global Link Manager. The default is usually `C:\Program Files\HiCommand\databackup` .	Upgrade installation from version 6 or version 7
`HGLM_CLUSTER_SETUP`	If Hitachi Command Suite Common Component and HiRDB are in neither a cluster configuration nor a non-cluster configuration, specify whether to set up a cluster environment or a non-cluster environment. `TRUE`: A cluster environment will be set up. `FALSE`: A non-cluster environment will be set up. The default is `FALSE`. If you specify `TRUE` for `HGLM_CLUSTER_SETUP`, you must specify the following key names: • `HGLM_CLUSTER_RESOURCEGROUPNAME` • `HGLM_CLUSTER_HOSTNAME_ACTIVE` • `HGLM_CLUSTER_HOSTNAME_STANDBY`	New installation, upgrade installation, or reinstallation
`HGLM_CLUSTER_MODE`	If you perform the installation in a cluster configuration, specify the operation mode. `2`: Active `3`: Standby The default is `2`.	New installation, upgrade installation, or reinstallation
`HGLM_CLUSTER_RESOURCEGROUPNAME`	Specify the resource group name. In a cluster configuration, an error occurs if a user performs an unattended installation without setting this key.	New installation, upgrade installation, or reinstallation
`HGLM_CLUSTER_HOSTNAME_ACTIVE`	Specify the active host name. In a cluster configuration, an error occurs if a user performs an unattended installation without setting this key.	New installation, upgrade installation, or reinstallation
`HGLM_CLUSTER_HOSTNAME_STANDBY`	Specify the standby host name. In a cluster configuration, an error occurs if a user performs an unattended installation without setting this key.	New installation, upgrade installation, or reinstallation
`HGLM_HDLMINSTALLDOWNLOAD`	Specify whether to use the function for downloading the HDLM installer. `TRUE`: Uses the download function. `FALSE`: Does not use the download function. The default is `FALSE`.	New installation, upgrade installation, or reinstallation

Key name	Description	Key is specifiable for:
	If an upgrade installation or re-installation is being performed, and the installer has previously been installed with the download function enabled, this key will not be used. Regardless of the specified value, the download function will be enabled.	

About the log file

For an unattended installation, the results of the installation processing are output to the log file `installhglm_`*yyyy-mm-dd_hh-mm-ss*`.log`.

The `installhglm_`*yyyy-mm-dd_hh-mm-ss*`.log` file will be output to the following location:

system-drive`:\installhglm_`*yyyy-mm-dd_hh-mm-ss*`.log`

If the `KAIF40111-I` message has not been output to the log file, follow the instructions provided by the messages that were output.

Note

The `installhglm_`*yyyy-mm-dd_hh-mm-ss*`.log` file and the `setup_`*yyyy-mm-dd_hh-mm-ss*`.log` file# for an unattended installation are directly output to the system drive, and these files are not deleted when Global Link Manager is removed. Therefore, if the log files for the unattended installation are no longer necessary, delete them manually.

#

This log file is used for the internal processing.

Removing Global Link Manager

Make sure of the following before performing a removal.

- You are logged on to Windows as an Administrator or a member of the Administrators group.
- Dialog boxes used for operating Windows services, such as Computer Management or Services, are not displayed.
- If the OS has set Global Link Manager to manage VMware hosts, the OS has deleted the VMware hosts before removing Global Link Manager.#

#

For details about deleting hosts, see the *Hitachi Global Link Manager User Guide*. If Global Link Manager is removed before the OS deletes the VMware hosts, perform the following steps:

a. Log on to Windows on the remote management client as a member of the Administrators group.

b. Stop the HDLM manager.

   Choose **Start**, **Control Panel**, **Administrative Tools**, and **Services**.

   Double-click **DLMManager** from the list of services, and then click the **Stop** button.

c. Delete all folders and files in the following folder:

   HDLM-installation-folder`\host`

d. Start the HDLM manager.

   Choose **Start**, **Control Panel**, **Administrative Tools**, and **Services**.

   Double-click **DLMManager** from the list of services, and click the **Start** button.

   Note

   If Global Link Manager is used to set, for each LU, the functionality for setting the number of times that the same paths are used, and then Global Link Manager is uninstalled, the values set for each LU remain valid but they cannot be displayed or changed.

   Therefore, do either of the following procedures to enable the functionality for setting the number of times that the same paths are used for each system:

   - If Global Link Manager is not uninstalled yet:

     See *Multipath LU configuration* in the manual *Global Link Manager User Guide*, and set **Following setting in the host** to set the number of times that the same paths are used for each system.

   - If Global Link Manager is already uninstalled:

     Use the `set` operation of the HDLM commands to set the number of times that the same paths are used for each system.

     For details about how to execute the HDLM commands, see the HDLM manuals.

To remove Global Link Manager:

1. Choose **Start**, **Control Panel**, **Add/Remove Programs**, select Hitachi Global Link Manager from the **Currently installed programs** list in the Add/Remove Programs window, and then click the **Change/Remove** button.

   The **Removal of Hitachi Global Link Manager** dialog box appears.

2. Click the **Next** button.

   If any services of Hitachi Command Suite Common Component or of another Hitachi Command Suite product are running, either of the following dialog boxes will appear:

   - The **Stopping the Services of Hitachi Command Suite Products** dialog box appears. Click the **Next** button to stop those services.

3. Click the **Next** button.

   If any service of another Hitachi Command Suite product has already been installed, a dialog box appears, asking you whether you want to

start the services of Hitachi Command Suite products after removal. Select whether to start the services after removal (optional). If the dialog box does not appear, go to step 4.

When you click the **Yes** or **No** button, the **Confirmation Before Removal** dialog box appears.

4. Confirm that the displayed removal settings are correct, and then click the **Remove** button.

   The registered software information is removed, the Global Link Manager database is deleted, and removal starts. When you are using the SNMP trap receiving function and the port that receives SNMP traps is added to the Windows Firewall exceptions list, the **Cancellation of an HGLM Setting is Complete** dialog box appears. Confirm that the settings in the dialog box are correct.

5. Click the **Next** button.

   When the removal has been completed normally, the **Removal Complete** dialog box appears.

6. Click the **Finish** button to finish the removal.

Note

- If you uninstall Hitachi Global Link Manager in an environment where the following products are installed, uninstall these products and then reinstall them. For details on how to migrate data for each product, see the user guide manual for each product.
  - Hitachi Command Suite v7 or earlier
  - Hitachi File Services Manager
  - Hitachi Storage Navigator Modular 2

Setting up license information during initial login

To log into Global Link Manager and start operation, set up Global Link Manager, and then specify initial settings from the Global Link Manager GUI.

To specify initial license information for Global Link Manager:

1. On the Web browser's address bar, enter the login URL as follows:

   ```
   http://IP-address-or-host-name-of-the-Global-Link-Manager-server:port-number-for-HBase-Storage-Mgmt-Web-Service-of-the-Global-Link-Manager-server/GlobalLinkAvailabilityManager/

   Example:
   http://127.0.0.1:22015/GlobalLinkAvailabilityManager/
   ```

   When specifying an IPv6 address, enclose the IP address in square brackets (`[ ]`).

   To check the login URL, execute the following command:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64chgurl /list
   ```

The Back To Login window, and then the User Login window appears.

2. Click the **License** button.
   The License dialog box appears.
3. Register the license information.

The following three types of license keys are available.

Table 2-6 License types

License type	Explanation
Permanent license key	A license key that allows for permanent use of the product.
Temporary license key	A license key that is valid for a limited time, such as the user evaluation period for a product. The license period is 120 days.
Emergency license key	A temporary license key for use while waiting for a permanent license key to be issued. The license period is 30 days.

3

Setting up Global Link Manager

This chapter describes how to set up Global Link Manager, including how to start and stop Global Link Manager, and how to back up and restore the Global Link Manager database.

Some Windows Server 2012 terms refer to items that are assigned different names in other Windows server OSs, but which have similar functions. This chapter uses the names that appear in OSs that are not Windows Server 2012 unless otherwise indicated. If you are using Windows Server 2012, replace the term *resource group* with *role* as you read through the procedures.

- Security settings for user accounts
- Setting a warning banner
- Generating audit logs
- Setting up alert transfer
- Settings required to authenticate users by using an external authentication server

Notes when executing commands

This section describes notes when executing commands that are required for specifying Global Link Manager settings.

Login users

To execute the commands described in this manual, you must log in as a member of the Administrators group.

Elevating to administrator privileges

If the UAC feature is enabled in a Windows OS, when you execute a command, you might be asked to elevate your current privileges to Administrator privileges. Some of the commands necessary to operate a management server require that the command be executed with such elevated privileges. When you execute a command described in this manual on an OS where UAC is enabled, execute the command with elevated privileges unless specifically noted otherwise.

To elevate your privileges to Administrator privileges to execute a command:

1. Right-click the command prompt icon.
2. From the list of right-click menu commands, choose **Run as administrator**.

   The elevated command prompt window opens.

Starting and stopping Global Link Manager

Global Link Manager is started or stopped by starting or stopping Hitachi Command Suite Common Component.

Usually, Global Link Manager is automatically started. However, Global Link Manager needs to be started and stopped manually when, for example, the property file is updated.

Starting Global Link Manager

To start Global Link Manager, start Hitachi Command Suite Common Component by using either of the following methods:

From the Windows **Start** menu:

For OSs other than Windows Server 2012:

In the Windows **Start** menu, choose **All Programs**, **Hitachi Command Suite**, **Global Link Manager**, and then **Start - HGLM**.

For Windows Server 2012:

In the Start window, choose **All apps**, **Hitachi Command Suite**, **Global Link Manager**, and then **Start - HGLM**.

By executing a command:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64srv /start
```

If other Hitachi Command Suite products have been installed on the same machine, the services of these Hitachi Command Suite products are started along with Global Link Manager. Note, however, that the services are not started in the following cases:

- When Hitachi Command Suite Common Component has already been started

In these cases, see the manual for each product to start the services.

Stopping Global Link Manager

To stop Global Link Manager, stop Hitachi Command Suite Common Component by using either of the following methods.

From the Windows **Start** menu:

For OSs other than Windows Server 2012:

In the Windows **Start** menu, choose **All Programs**, **Hitachi Command Suite**, **Global Link Manager**, and then **Stop - HGLM**.

For Windows Server 2012:

In the Start window, choose **All apps**, **Hitachi Command Suite**, **Global Link Manager**, and then **Stop - HGLM**.

By executing a command:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64srv /stop
```

If other Hitachi Command Suite products have been installed on the same machine, the services of these Hitachi Command Suite products are stopped along with Global Link Manager.

Note

Do not execute stopping of Hitachi Command Suite Common Component right after starting. Wait some seconds to execute stopping right after starting.

Checking Global Link Manager status

To check the Global Link Manager status, check the Hitachi Command Suite Common Component status by executing the following command:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64srv /status
```

When the following messages are displayed, Hitachi Command Suite Common Component is running properly.

```
KAPM06440-I The HiRDB service has already started.
KAPM05007-I Already started service. service-name=HBase 64 Storage
Mgmt Web Service
```

```
KAPM05007-I Already started service. service-name=HBase 64 Storage
Mgmt Web SSO Service
KAPM05007-I Already started service. service-name=HBase 64 Storage
Mgmt SSO Service
KAPM05007-I Already started service. service-name=Global Link
Manager Web Service
```

Resident processes of Hitachi Command Suite Common Component

The following table shows the resident processes of Hitachi Command Suite Common Component.

Table 3-1 Resident processes of Hitachi Command Suite Common Component

Process name	Service name	Function
hcmdssvctl.exe cjstartsv.exe	Global Link Manager Web Service	Global Link Manager J2EE service
hcmdssvctl.exe cjstartsv.exe	HBase 64 Storage Mgmt SSO Service	Hitachi Command Suite J2EE service for single sign-on
httpsd.exe rotatelogs.exe	HBase 64 Storage Mgmt Web Service	Hitachi Command Suite common web service. Multiple instances of this process might be running.
httpsd.exe rotatelogs.exe	HBase 64 Storage Mgmt Web SSO Service	Hitachi Command Suite common web service for single sign-on.
hntr2mon.exe	Hitachi Network Objectplaza Trace Monitor 2 Hitachi Network Objectplaza Trace Monitor 2 (x64)	Hitachi Command Suite common trace log collection
hntr2srv.exe		Hitachi Command Suite common trace service (This service processes events from the Services window.)
pdservice.exe#	HiRDB/ EmbeddedEdition _HD1	HiRDB process server control

#:

This process must always be running. Do not stop it manually or register it as a cluster resource.

Changing the time of the machine on which Global Link Manager is installed

Before installing Global Link Manager, you need to set the current time for the machine. This section describes how to change the time when you install Global Link Manager in an environment where other Hitachi Command Suite

products are already installed. This section also describes how to change the time, if necessary, after installing Global Link Manager.

Note

If the machine time is changed while Hitachi Command Suite Common Component is running, Hitachi Command Suite products including Global Link Manager might not operate correctly. We recommend that you change the machine time before installing Global Link Manager.

Settings required when using the time adjustment function

If you use a function that automatically adjusts the time, such as NTP, make sure that the function gradually adjusts the machine time (in a machine that is running faster than the actual time), rather than adjusting the time all at once. Some functions gradually adjust the time for time differences that are within a predefined time, but some other functions adjust the time all at once for time differences that exceed the predefined time. Set the frequency at which the function adjusts the time to ensure that time differences stay within the predefined time required by the function to adjust the time gradually.

For example, the Windows Time service adjusts the machine time gradually rather than adjusting it all at once, when the machine time is running faster than the actual time by no more than the predefined time. After you check the range of time differences that the Windows Time service adjusts gradually, you can set the frequency of the Windows Time service's time adjustments so that differences between machine time and actual time are never outside this range.

When the time adjustment function is unavailable or when you need to change the time immediately

To change the machine time when you cannot use a function that automatically adjusts the time or when you need to change the time immediately:

1. Execute the following command to stop Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /stop
   ```

   If other Hitachi Command Suite products have been installed on the same machine, the services of these Hitachi Command Suite products are also stopped.
2. Change the machine time.
3. Restart the machine.

Setting for changing the Java program used by Global Link Manager

Use the following procedure to change the Java program used by Global Link Manager.

1. Stop the Global Link Manager.

   The stop of Global Link Manager, see Starting and stopping Global Link Manager on page 3-3.

   To change the Java program to be used, do not start services provided by other Hitachi Command Suite products.

2. Execute the following command to select the Java program to be used on the displayed screen..

   Hitachi-Command-Suite-Common-Component-installation-folder`\bin\hcmds64chgjdk`

3. After executing the command, Start Global Link Manager.

   The start of Global Link Manager, see Starting and stopping Global Link Manager on page 3-3.

Notes

- To change the Java program, Global Link Manager must be installed in any of the following OS.

  Windows Server 2012 (x64)

  Windows Server 2012 R2
- If you re-install or update the Java program, the `hcmds64chgjdk` command must be re-executed because the installation destination of the Java program is changed.
- If you remove the Java program that was changed, Global Link Manager cannot be removed. Remove Global Link Manager after changing back the Java program.
- If the user authentication was conducted with the LDAP server, the certification must be imported again. For details, see Security settings for communication between a server and an LDAP directory server on page 5-13.

Maintaining the Global Link Manager database

This section describes the following operations for the Global Link Manager database:

- Backing up and restoring the database
- Migrating (exporting and importing) the database
- Changing the storage location of the database

To perform database operations, you need to execute a backup and restore of the Global Link Manager property files and the path availability information

(path status log). The property files to be backed up and restored are as follows:

- `server.properties`
- `logger.properties`
- `database.properties`

The following table shows the functional differences between backing up and restoring on the one hand and exporting and importing on the other.

Table 3-2 Backing up and restoring versus exporting and importing

Item	Backing up and restoring	Exporting and importing
Conditions of the Hitachi Command Suite Common Component version	No limitation	Hitachi Command Suite Common Component version 5.5 or later must be installed on the machine used for the export source or the import destination.
Main purpose of use	To recover the current operating environment when a failure occurs in the server machine.	To migrate the server machine from the current environment to a different environment (such as a machine with a different OS).
Target data	• Databases for Hitachi Command Suite products • The Hitachi Command Suite Common Component database	• Databases for Hitachi Command Suite products • User information included in the Hitachi Command Suite Common Component database
Conditions for the machine used for the restore destination or the import destination	The following must be the same in the backup source machine and the restore destination machine: • Types, versions, and revisions of the installed Hitachi Command Suite products • Installation locations for each Hitachi Command Suite product, Hitachi Command Suite Common Component, each Hitachi Command Suite product database, and Hitachi Command Suite Common Component database • The IP address and host name of the machine	• The Hitachi Command Suite products whose databases to be imported must be installed. • The versions of the installed Hitachi Command Suite products must be the same as or higher than the ones on the export source machine.

Backing up the Global Link Manager database

Hitachi recommends that you back up the database of Global Link Manager and the databases of Hitachi Command Suite products regularly. In addition, you should always back up these databases before performing the following operations:

- Reinstallation or version upgrade installation of Global Link Manager
- Installing or removing another Hitachi Command Suite product on a server on which Global Link Manager has been installed
- Installing or removing Global Link Manager on a server on which another Hitachi Command Suite product has been installed

The following procedure describes how to back up the Global Link Manager database and other Hitachi Command Suite product databases. In this procedure, you also acquire a backup of the Global Link Manager property files and the path availability information (path status log), in addition to the databases.

If other Hitachi Command Suite products have already been installed on the same machine, the services of these products are also started or stopped at the same time when you start or stop Hitachi Command Suite Common Component.

In a non-cluster configuration

1. Execute the following command to stop Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /stop
   ```

2. Execute the following command to start HiRDB:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64dbsrv /start
   ```

3. Execute the following command to back up the database:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64backups /dir backup-destination-folder-name
   ```

   For *backup-destination-folder-name*, specify the absolute path of a folder on the local disk. When you specify an existing folder, it should be an empty folder.

   When you execute the above command, a backup file (`backup.hdb`) will be created for the databases of the Hitachi Command Suite products installed on the server on which the above command is executed. At the same time, the setting files for Hitachi Command Suite Common Component and other Hitachi Command Suite products are also backed up.

4. Execute the following command to back up the property files and the path availability information (path status log):

   ```
   Global-Link-Manager-installation-folder\bin\hglambackup /dir
   backup-destination-folder-name
   ```

   Use an absolute path to specify *backup-destination-folder-name*. When you specify an existing folder, it should be an empty folder.

   The following characters can be used for *backup-destination-folder-name*:

A to Z, a to z, 0 to 9, period (.), and underscore (_). You can also use a backslash (\), colon (:), and forward slash (/) as the path delimiter. If you specify a path including a space, enclose it in double quotation marks (").

The following shows an example of executing the command:

```
"C:\Program Files\HiCommand\HGLAM\bin\hglambackup" /dir "C:
\hglam backup"
```

Do not change the file structure under the folder specified for *backup-destination-folder-name*.

5. If required, execute the following command to start the Hitachi Command Suite Common Component service:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64srv /start
```

In a cluster configuration

To stop services and disable failovers:

1. Use the cluster software to take the following resources offline:
   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - Other Hitachi Command Suite product resources
2. Execute the following command to stop the Hitachi Command Suite product services:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64srv /stop
```

3. Use the cluster software to take the following service offline:
   - HiRDBClusterService_HD1
4. Use the cluster software to suppress failover of the resource group.

   If you use Microsoft Failover Cluster:

   Right-click the resource name and choose **Properties**. In the **Policies** tab, select **If resource fails, do not restart**.
5. Execute the following command to start HiRDB:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbsrv /start
```

6. Execute the following command to back up the database:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64backups /dir backup-destination-folder-name
```

For *backup-destination-folder-name*, specify the absolute path of a folder on the local disk. When you specify an existing folder, it should be an empty folder.

When you execute the above command, a backup file (backup.hdb) will be created for the databases of the Hitachi Command Suite products

installed on the server on which the above command is executed. At the same time, the setting files for Hitachi Command Suite Common Component and other Hitachi Command Suite products are also backed up.

7. Execute the following command to back up the property files and the path availability information (path status log):

   ```
   Global-Link-Manager-installation-folder\bin\hglambackup /dir
   backup-destination-folder-name
   ```

   Use an absolute path to specify *backup-destination-folder-name*. When you specify an existing folder, it should be an empty folder.

   The following characters can be used for *backup-destination-folder-name*: `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), and underscore (`_`). You can also use a backslash (`\`), colon (`:`), and forward slash (`/`) as the path delimiter. If you specify a path including a space, enclose it in double quotation marks (`"`).

   The following shows an example of executing the command:

   ```
   "C:\Program Files\HiCommand\HGLAM\bin\hglambackup" /dir "C:
   \hglam backup"
   ```

   Do not change the file structure under the folder specified for *backup-destination-folder-name*.

8. If required, execute the following command to start the Hitachi Command Suite Common Component service:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /start
   ```

To start services and enable failovers:

1. Execute the following command to stop the Hitachi Command Suite product services:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /stop
   ```

2. Use the cluster software to enable failover of the following resources:

   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - Other Hitachi Command Suite product resources

   If you use Microsoft Failover Cluster (for OSs other than Windows Server 2012):

   Right-click the resource name and choose **Properties**. In the **Policies** tab, select **If resource fails, attempt restart on current node** and **If restart is unsuccessful, fail over all resources in this service or application**.

   If you use Microsoft Failover Cluster (for Windows Server 2012):

Right-click the resource name and choose **Properties**. In the **Policies** tab, select **If resource fails, attempt restart on current node** and **If restart is unsuccessful, fail over all resources in this Role**.

3. Use the cluster software to put the resource group online.

Restoring the Global Link Manager database

This section describes how to restore the Global Link Manager database and the databases of all installed Hitachi Command Suite products. In this procedure, you also restore the Global Link Manager property files and the path availability information (path status log), in addition to the databases.

If other Hitachi Command Suite products have already been installed on the same machine, the services of these products are also started or stopped at the same time when you start or stop Hitachi Command Suite Common Component.

In a non-cluster configuration

1. Execute the following command to stop Hitachi Command Suite Common Component:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /stop

2. Execute the following command to restore the Global Link Manager database:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64db /restore *backup-file-name* /type HGLAM

   For *backup-file-name*, specify the backup data (backup.hdb) to be restored by using an absolute path.

   To restore the Global Link Manager database, specify /type HGLAM or /type GlobalLinkAvailabilityManager.

   To restore the databases of all installed Hitachi Command Suite products, including Global Link Manager, execute the command by specifying /type ALL.

   To restore the databases after removing and then reinstalling all the Hitachi Command Suite products, specify /type ALL.

   Note

   If you restore the databases by specifying /type ALL, the states of other Hitachi Command Suite products return to the states that existed when backup data was acquired. When you execute the command, make sure there will be no problems in having those states return to the ones that existed when backup data was acquired.

3. Execute the following command to restore the property files and the path availability information (path status log):

   Global-Link-Manager-installation-folder\bin\hglamrestore /dir *name-of-the-folder-for-storing-the-backup-data*

For *name-of-the-folder-for-storing-the-backup-data*, specify an absolute path for the folder in which the data backed up using the `hglambackup` command is to be stored.

4. Execute the following command to start Hitachi Command Suite Common Component:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /start

In a cluster configuration

To stop services and disable failovers:

1. Use the cluster software to take the following resources offline:
   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - Other Hitachi Command Suite product resources
2. Execute the following command to stop the Hitachi Command Suite product services:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /stop
3. Use the cluster software to take the following service offline:
   - HiRDBClusterService_HD1
4. Use the cluster software to suppress failover of the resource group.

   If you use Microsoft Failover Cluster:

   Right-click the resource name and choose **Properties**. In the **Policies** tab, select **If resource fails, do not restart**.
5. Execute the following command to restore the Global Link Manager database:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64db /restore *backup-file-name* /type HGLAM

   For *backup-file-name*, specify the backup data (`backup.hdb`) to be restored by using an absolute path.

   To restore the Global Link Manager database, specify `/type HGLAM` or `/type GlobalLinkAvailabilityManager`.

   To restore the databases of all installed Hitachi Command Suite products, including Global Link Manager, execute the command by specifying `/type ALL`.

   To restore the databases after removing and then reinstalling all the Hitachi Command Suite products, specify `/type ALL`.

   Note

   If you restore the databases by specifying `/type ALL`, the states of other Hitachi Command Suite products return to the states that existed when backup data was acquired. When you execute the

command, make sure there will be no problems in having those states return to the ones that existed when backup data was acquired.

6. Execute the following command to restore the property files and the path availability information (path status log):

   ```
   Global-Link-Manager-installation-folder\bin\hglamrestore /dir
   name-of-the-folder-for-storing-the-backup-data
   ```

   For *name-of-the-folder-for-storing-the-backup-data*, specify an absolute path for the folder in which the data backed up using the `hglambackup` command is to be stored.

7. Execute the following command to start Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /start
   ```

To start services and enable failovers:

1. Execute the following command to stop the Hitachi Command Suite product services:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /stop
   ```

2. Use the cluster software to enable failover of the following resources:

   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - Other Hitachi Command Suite product resources

   If you use Microsoft Failover Cluster (for OSs other than Windows Server 2012):

   Right-click the resource name and choose **Properties**. In the **Policies** tab, select **If resource fails, attempt restart on current node** and **If restart is unsuccessful, fail over all resources in this service or application**.

   If you use Microsoft Failover Cluster (for Windows Server 2012):

   Right-click the resource name and choose **Properties**. In the **Policies** tab, select **If resource fails, attempt restart on current node** and **If restart is unsuccessful, fail over all resources in this Role**.

3. Use the cluster software to put the resource group online.

Migrating the Global Link Manager database

If Hitachi Command Suite products are used for an extended period of time, you might need a higher performance machine to accommodate product version upgrades and the increased number of objects to be managed. In this case, database migration will be an important step in this machine replacement process. In Hitachi Command Suite products, you can migrate the database by using the `hcmds64dbtrans` command. The `hcmds64dbtrans`

command migrates all information stored in the database of each Hitachi Command Suite product as well as user information managed by Hitachi Command Suite Common Component.

In the following two cases, you can use the `hcmds64dbtrans` command to migrate the Global Link Manager database to a machine that has a different environment from the one on the currently operating server machine:

- Migration to a machine on which the installation locations for Hitachi Command Suite products are different from the ones on the migration source
- Migration to a machine on which the versions of Hitachi Command Suite products are newer than the ones on the migration source

Notes when migrating the database

The following are notes for the types, versions, and user information of the Hitachi Command Suite products on the migration source and migration destination servers.

Notes for types and versions of the Hitachi Command Suite products on the migration source and migration destination servers:

- The database of a Hitachi Command Suite product that is not installed on the migration destination server cannot be migrated. Install all necessary Hitachi Command Suite products on the migration destination server.
- If any of the versions of the Hitachi Command Suite products installed on the migration destination server is older than the ones on the migration source server, the database cannot be migrated. On the migration destination server, install the Hitachi Command Suite products whose versions are the same as or higher than the ones on the migration source server.
- If you migrate the database of Replication Monitor version 4.2 or earlier, upgrade Replication Monitor on the source and destination servers to version 5.0 or later in advance.
- If you migrate the Replication Monitor database to the Replication Manager database, first upgrade Replication Monitor on the source server to Replication Manager, and then migrate the database.
- The following limitations apply when you migrate the Tuning Manager database:
    - If the version of Tuning Manager is earlier than 6.0, first upgrade the Tuning Manager to version 6.0 or later on both the migration source and migration destination servers.
    - Set the same capacity for the Tuning Manager database on both the migration source and migration destination servers. For details on how to change the capacity of the database, see the *Hitachi Command Suite Tuning Manager Server Administration Guide*.
    - The database can be migrated when the database configuration (Small or Medium) is the same on both the migration source and the destination server, or when the database configuration on the

migration destination server becomes much larger than that on the source server.

- In the database configuration on the migration source server, if the number of the management target resources exceeds 70% of the management limit, the database cannot be migrated to a database that has the same configuration.

Notes for user information:

- If there is user information on the migration destination server, this user information will be replaced with the user information from the migration source server. Therefore, do not perform a migration to the machine on which user information for the Hitachi Command Suite products already exists.
- If the databases of several Hitachi Command Suite products installed on a management server are migrated in multiple operations, the user information is replaced with new information at each operation, and eventually only the user information for the products migrated during the last operation will remain. When you perform migration for multiple products, be sure to migrate the databases in one operation so that user information for each product can be migrated.
- You cannot perform migration to integrate the Hitachi Command Suite products that were running on multiple management servers on to one management server, because user information will be overwritten with each successive migration.

General procedure for migrating databases

To migrate databases:

1. Install, on the migration destination server, the Hitachi Command Suite products whose databases will be migrated.
2. Export the databases at the migration source server.
3. Transfer the archive file from the migration source server to the migration destination server.
4. Import the database at the migration destination server.

Installing the Hitachi Command Suite products on the migration destination server

Install, on the migration destination server, the Hitachi Command Suite products whose databases will be migrated. The version of each Hitachi Command Suite product installed on the migration destination server must be the same as or higher than the one on the migration source server.

Exporting the database at the migration source server

To export the database of Global Link Manager, a folder for temporarily storing the information of the database, and a folder for storing the archive

file are required. Each of these folders requires as much capacity as the total size of the following two folders:

- The folder storing the Global Link Manager database
- The folder storing the Hitachi Command Suite Common Component database (excluding the `SYS` folder and the folders beneath it)

The folder storing the Global Link Manager database is *Global-Link-Manager-database-storing-folder*`\GlobalLinkAvailabilityManager`, which is specified during the installation.

The folder storing the Hitachi Command Suite Common Component database is *Hitachi-Command-Suite-Component-installation-folder*`\database`.

This capacity is a guideline value applied when only the Global Link Manager database is installed. If Hitachi Command Suite products other than Global Link Manager are also installed, take the capacities of those databases into account as well.

Caution

Databases are exported as archive files. If the capacity of a disk where archive files are created is insufficient, creation of the archive file fails when the database data is exported. In this case, instead of using the archive file, manually transfer the exported database data to the migration destination.

The following procedure describes how to export the database at the migration source server. In this procedure, you also export the Global Link Manager property files and the path availability information (path status log), in addition to the database.

If other Hitachi Command Suite products have already been installed on the same machine, the services of these products are also started or stopped at the same time when you start or stop Hitachi Command Suite Common Component.

In a non-cluster configuration

1. Execute the following command to stop Hitachi Command Suite Common Component:

   Hitachi-Command-Suite-Common-Component-installation-folder`\bin\hcmds64srv /stop`

2. Start HiRDB.

   Execute the following command:

   Hitachi-Command-Suite-Common-Component-installation-folder`\bin\hcmds64dbsrv /start`

3. Execute the following command to export the database:

   Hitachi-Command-Suite-Common-Component-installation-folder`\bin\hcmds64dbtrans /export /workpath` *work-folder* `/file` *archive-file*

For *work-folder*, specify an absolute path for the folder that temporarily stores the database information. Specify an empty folder on the local disk. If you do not specify an empty folder, export processing will be interrupted, in which case you will need to specify an empty folder and then re-execute the `hcmds64dbtrans` command.

For *archive-file*, specify an absolute path for the archive file of the database to be exported.

The following shows an example of executing the command:

```
"C:\Program Files\HiCommand\Base64\bin\hcmds64dbtrans" /export /
workpath D:\trans_work /file D:\trans_file\db_arc
```

4. Execute the following command to export the property files and the path availability information (path status log):

   Global-Link-Manager-installation-folder\bin\hglamexport /dir *export-destination-folder-name*

   Use an absolute path to specify *export-destination-folder-name*. When you specify an existing folder, make sure that the folder is empty.

   The following characters can be used for *export-destination-folder-name*: `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), and underscore (`_`). You can also use a backslash (`\`), colon (`:`), and forward slash (`/`) as the path delimiter. If you specify a path including a space, enclose the path in double quotation marks (`"`).

   The following shows an example of executing the command:

   ```
   "C:\Program Files\HiCommand\HGLAM\bin\hglamexport" /dir "C:
   \hglam export"
   ```

5. Transfer the archive file to the migration destination server.
6. Transfer the export destination folder specified in step 4 to the migration destination server.

   Do not change the file structure under the folder specified for *export-destination-folder-name*.

In a cluster configuration

To stop services and disable failovers:

1. Use the cluster software to take the following resources offline:
   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - Other Hitachi Command Suite product resources
2. Execute the following command to stop the Hitachi Command Suite product services:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /stop
3. Use the cluster software to take the following service offline:
   - HiRDBClusterService_HD1

4. Use the cluster software to suppress failover of the resource group.

   If you use Microsoft Failover Cluster:

   Right-click the resource name and choose **Properties**. In the **Policies** tab, select **If resource fails, do not restart**.

5. Execute the following command to start the Hitachi Command Suite product services:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /start
   ```

6. Execute the following command to export the database:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64dbtrans /export /workpath work-folder /file archive-file
   ```

   For *work-folder*, specify an absolute path for the folder that temporarily stores the database information. Specify an empty folder on the local disk. If you do not specify an empty folder, export processing will be interrupted, in which case you will need to specify an empty folder and then re-execute the `hcmds64dbtrans` command.

   For *archive-file*, specify an absolute path for the archive file of the database to be exported.

   The following shows an example of executing the command:

   ```
   "C:\Program Files\HiCommand\Base64\bin\hcmds64dbtrans" /export /
   workpath D:\trans_work /file D:\trans_file\db_arc
   ```

7. Execute the following command to export the property files and the path availability information (path status log):

   ```
   Global-Link-Manager-installation-folder\bin\hglamexport /dir
   export-destination-folder-name
   ```

   Use an absolute path to specify *export-destination-folder-name*. When you specify an existing folder, make sure that the folder is empty.

   The following characters can be used for *export-destination-folder-name*:

   `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), and underscore (`_`). You can also use a backslash (`\`), colon (`:`), and forward slash (`/`) as the path delimiter. If you specify a path including a space, enclose the path in double quotation marks (`"`).

   The following shows an example of executing the command:

   ```
   "C:\Program Files\HiCommand\HGLAM\bin\hglamexport" /dir "C:
   \hglam export"
   ```

8. Transfer the archive file to the migration destination server.

9. Transfer the export destination folder specified in step 7 to the migration destination server.

   Do not change the file structure under the folder specified for *export-destination-folder-name*.

To start services and enable failovers:

1. Execute the following command to stop the Hitachi Command Suite product services:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64srv /stop
```

2. Use the cluster software to enable failover of the following resources:
   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - Other Hitachi Command Suite product resources

   If you use Microsoft Failover Cluster (for OSs other than Windows Server 2012):

   Right-click the resource name and choose **Properties**. In the **Policies** tab, select **If resource fails, attempt restart on current node** and **If restart is unsuccessful, fail over all resources in this service or application**.

   If you use Microsoft Failover Cluster (for Windows Server 2012):

   Right-click the resource name and choose **Properties**. In the **Policies** tab, select **If resource fails, attempt restart on current node** and **If restart is unsuccessful, fail over all resources in this Role**.
3. Use the cluster software to put the resource group online.
4. Transfer the archive file to the migration destination server.
5. Transfer the export destination folder described above in step 7 *To stop services and disable failovers:* to the migration destination server.

   Do not change the file structure under the folder specified for *export-destination-folder-name*.

When an archive file could not be created:

Transfer all the files in the folder specified for *work-folder* to the migration destination server. When you do so, do not change the structure of files under the folder specified for *work-folder*.

Importing the database at the migration destination server

The following procedure describes how to import the database at the migration destination server. In this procedure, you also restore the path availability information (path status log), in addition to the database.

If other Hitachi Command Suite products have already been installed on the same machine, the services of these products are also started or stopped at the same time when you start or stop Hitachi Command Suite Common Component.

In a non-cluster configuration

1. Execute the following command to stop Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /stop
   ```

2. Start HiRDB.

Execute the following command:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbsrv /start
```

3. Execute the following command to import the database:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbtrans /import /workpath work-folder /file archive-
file /type HGLAM
```

For *work-folder*, specify an absolute path for the folder in which the archive file will be expanded. Specify an empty folder on the local disk. If you do not specify an empty folder, import processing will be interrupted, in which case you will need to specify an empty folder and then re-execute the `hcmds64dbtrans` command. For *archive-file*, specify an absolute path for the archive file of the database information that was transferred from the migration source server.

Note the following if you do not use the archive file:

- For *work-folder*, specify the folder that stores the database information transferred from the migration source. Do not change the structure of files under the transferred folder.
- Do not specify the `/file` option.

To import the Global Link Manager database, specify `/type HGLAM` or `/type GlobalLinkAvailabilityManager`.

To import the databases of all installed Hitachi Command Suite products, including Global Link Manager, execute the command by specifying either `/type ALL` or the names of the Hitachi Command Suite products to be imported, which are separated by using a comma as the delimiter. For the names of other Hitachi Command Suite products that can be specified in the `/type` option, see the manuals for each product.

If you specify `ALL` in the `/type` option, databases of the Hitachi Command Suite products installed on the migration destination are automatically selected and migrated. If you want to specify multiple products, the databases of all the specified products must exist in the folder specified by the archive file or the `/workpath` option, and all the specified products must be installed on the migration destination server. If any of the products do not meet the conditions above, migration will not be performed.

Caution

- The import procedure depends on the Hitachi Command Suite products. To migrate databases of Hitachi Command Suite products other than Global Link Manager, see the documentation for those products.
- If Replication Monitor version 4.2 or earlier is installed on the migration source machine, you cannot migrate the database. Therefore, upgrade Replication Monitor on the migration source and migration destination machines to version 5.0 or later, and then perform migration. If Replication Monitor cannot be upgraded

to version 5.0 or later, or the Replication Monitor database does not have to be migrated, use the `/type` option and specify all products other than Replication Monitor when you execute the command.

4. Execute the following command to import the path availability information (path status log) and update the database:

   ```
   Global-Link-Manager-installation-folder\bin\hglamimport /dir
   name-of-the-folder-for-storing-the-exported-data
   ```

   For *name-of-the-folder-for-storing-the-exported-data*, specify an absolute path for the folder in which the data exported by using the `hglamexport` command is to be stored.

   After the import processing is complete, the Global Link Manager database is updated.

   Caution

   The property files will not be imported because the environment on the migration source and destination server might be different. If you want to change the property files, check the folder that stores the data exported using the `hglamexport` command and the property files on the migration source server, and then edit the property files on the migration destination server.

5. Execute the following command to start Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /start
   ```

In a cluster configuration

To stop services and disable failovers:

1. Use the cluster software to take the following resources offline:
   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - Other Hitachi Command Suite product resources
2. Execute the following command to stop the Hitachi Command Suite product services:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /stop
   ```

3. Use the cluster software to take the following service offline:
   - HiRDBClusterService_HD1
4. Use the cluster software to suppress failover of the resource group.

   If you use Microsoft Failover Cluster:

   Right-click the resource name and choose **Properties**. In the **Policies** tab, select **If resource fails, do not restart**.

5. Execute the following command to start HiRDB:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64dbsrv /start

6. Execute the following command to import the database:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64dbtrans /import /workpath *work-folder* /file *archive-file* /type HGLAM

   For *work-folder*, specify an absolute path for the folder in which the archive file will be expanded. Specify an empty folder on the local disk. If you do not specify an empty folder, import processing will be interrupted, in which case you will need to specify an empty folder and then re-execute the `hcmds64dbtrans` command. For *archive-file*, specify an absolute path for the archive file of the database information that was transferred from the migration source server.

   Note the following if you do not use the archive file:

   - For *work-folder*, specify the folder that stores the database information transferred from the migration source. Do not change the structure of files under the transferred folder.
   - Do not specify the `/file` option.

   To import the Global Link Manager database, specify `/type HGLAM` or `/type GlobalLinkAvailabilityManager`.

   To import the databases of all installed Hitachi Command Suite products, including Global Link Manager, execute the command by specifying either `/type ALL` or the names of the Hitachi Command Suite products to be imported, which are separated by using a comma as the delimiter. For the names of other Hitachi Command Suite products that can be specified in the `/type` option, see the manuals for each product.

   If you specify `ALL` in the `/type` option, databases of the Hitachi Command Suite products installed on the migration destination are automatically selected and migrated. If you want to specify multiple products, the databases of all the specified products must exist in the folder specified by the archive file or the `/workpath` option, and all the specified products must be installed on the migration destination server. If any of the products do not meet the conditions above, migration will not be performed.

   Caution

   - The import procedure depends on the Hitachi Command Suite products. To migrate databases of Hitachi Command Suite products other than Global Link Manager, see the documentation for those products.
   - If Replication Monitor version 4.2 or earlier is installed on the migration source machine, you cannot migrate the database. Therefore, upgrade Replication Monitor on the migration source and migration destination machines to version 5.0 or later, and then perform migration. If Replication Monitor cannot be upgraded to version 5.0 or later, or the Replication Monitor database does

not have to be migrated, use the `/type` option and specify all products other than Replication Monitor when you execute the command.

7. Execute the following command to import the path availability information (path status log) and update the database:

   Global-Link-Manager-installation-folder\bin\hglamimport /dir *name-of-folder-for-storing-exported-data*

   For *name-of-folder-for-storing-exported-data*, specify an absolute path for the folder that stores the data exported by the `hglamexport` command.

   After the import processing is complete, the Global Link Manager database is updated.

   Caution

   The property files will not be imported because the environments on the migration-source and migration-destination servers might be different. If you want to change the property files, check the folder that stores the data exported by the `hglamexport` command and the property files on the migration-source server, and then edit the property files on the migration-destination server (primary and secondary nodes).

To start services and enable failovers:

1. Execute the following command to stop the Hitachi Command Suite product services:

   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /stop

2. Use the cluster software to enable failover of the following resources:

   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - Other Hitachi Command Suite product resources

   If you use Microsoft Failover Cluster (for OSs other than Windows Server 2012):

   Right-click the resource name and choose **Properties**. In the **Policies** tab, select **If resource fails, attempt restart on current node** and **If restart is unsuccessful, fail over all resources in this service or application**.

   If you use Microsoft Failover Cluster (for Windows Server 2012):

   Right-click the resource name and choose **Properties**. In the **Policies** tab, select **If resource fails, attempt restart on current node** and **If restart is unsuccessful, fail over all resources in this Role**.

3. Use the cluster software to put the resource group online.

Changing the storage location of the Global Link Manager database (non-cluster)

If the amount of free space in the disk where the database files are to be stored is insufficient during a version upgrade installation, change the storage location of the database files. This section describes how to change the storage location of the database files.

If other Hitachi Command Suite products have already been installed on the same machine, the services of these products are also started or stopped at the same time when you start or stop Hitachi Command Suite Common Component.

Notes

- If other Hitachi Command Suite products have already been installed on the same machine, the storage location of the database files for the Hitachi Command Suite products will be changed when you perform this procedure. In this case, the amount of free disk space required must be enough for the total size of the database files for Global Link Manager and other Hitachi Command Suite products. Make sure to consider the total size of the database files for all of the Hitachi Command Suite products installed on the same machine, and then reserve sufficient free disk space. For details on the size of database files for other Hitachi Command Suite products, see the manual for each product.
- If you execute the `hcmds64dbinit` command in the following procedure, the default (22032) is set to the port number that HiRDB uses. Therefore, if you are using a port number other than the default to perform operations, you need to reset the port number later. Write down the port number you are using so that you can set the port number again.
- When you execute the `hcmds64dbinit` command used in this procedure, the authentication information of the built-in account (user ID: System), including the password, will be initialized.
- After performing this procedure, check the URLs for the Hitachi Command Suite products, and if there are changes, set the URLs again.

  To check the URLs for the Hitachi Command Suite products, execute the following command:

  ```
  Hitachi-Command-Suite-Common-Component-installation-folder\bin
  \hcmds64chgurl /list
  ```

1. Execute the following command to stop Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /stop
   ```

2. Execute the following command to start HiRDB:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbsrv /start
```

3. Execute the following command to back up the database:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbtrans /export /workpath work-folder /file archive-file
```

Notes

- For *work-folder*, specify an absolute path for the folder that temporarily stores the database information. Specify an empty folder on the local disk. If you do not specify an empty folder, export processing will be interrupted, in which case you will need to specify an empty folder and then re-execute the `hcmds64dbtrans` command.
- For *archive-file*, specify an absolute path for the archive file of the database to be exported.
- If the capacity of a disk where archive files are created is insufficient, creation of the archive file fails when the database data is exported.

4. Re-create the database system in the local disk.

Execute the following command:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbinit /databasepath target-folder-for-re-creating-the-
database
```

Before executing the command, delete or empty *target-folder-for-re-creating-the-database*.

Specify an absolute path (maximum of 63 bytes) for *target-folder-for-re-creating-the-database*, and deploy this folder on the local disk.

You can use the following characters for this folder:

`A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), and underscore (`_`). You can also use a backslash (`\`), colon (`:`), and forward slash (`/`) as the path delimiter.

5. Import the database that was exported in step 3.

Execute the following command:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbtrans /import /workpath work-folder /file archive-
file /type ALL
```

Notes

- For *work-folder*, specify the absolute path of the archive file to be deployed. Specify an empty folder on the local disk. If you do not specify an empty folder, import processing will be interrupted. Specify an absolute path for temporarily storing the database information.
- For *archive-file*, specify the absolute path for the archive file of the database specified in step 3.

- If you are not using the archive file, specify the folder that stores the database information specified for *work-folder* in step 3. In this procedure, do not change the file structure under the specified folder. Also, do not specify the `/file` option.

6. If the port number that HiRDB uses has already been changed and is being used, reset the port number.

   When the `hcmds64dbinit` command is executed, the default (22032) is set to the port number that HiRDB uses. Therefore, reset the port number.

Changing the storage location of the Global Link Manager database (for a cluster environment)

This subsection describes how to migrate data in a Windows cluster environment when Windows Server Failover Clustering is used.

If other Hitachi Command Suite products have already been installed on the same machine, the services of these products are also started or stopped at the same time when you start or stop Hitachi Command Suite Common Component.

Notes

- If other Hitachi Command Suite products have already been installed on the same machine, the storage location of the database files for the Hitachi Command Suite products will be changed when you perform this procedure. In this case, the amount of free disk space required must be enough for the total size of the database files for Global Link Manager and other Hitachi Command Suite products. Make sure to consider the total size of the database files for all of the Hitachi Command Suite products installed on the same machine, and then reserve sufficient free disk space. For details on the size of database files for other Hitachi Command Suite products, see the manual for each product.
- If you execute the `hcmds64dbclustersetup` command in the following procedure, the default (22032) is set to the port number that HiRDB uses. Therefore, if you are using a port number other than the default to perform operations, you need to reset the port number later. Write down the port number you are using so that you can set the port number again.

Procedure on the executing node

1. On the executing node, make sure that the Hitachi Command Suite Common Component service is online, and that the executing node currently owns the service and shared disk.
2. Execute either of the commands below to place the Global Link Manager service offline.

   If other Hitachi Command Suite products have been installed, this procedure places their services offline.

If Hitachi Command Suite products of versions v8.1.2 or later are installed:

```
Hitachi-Command-Suite-Common-Component-installation-folder
\ClusterSetup\hcmds64clustersrvstate /soff /r resource-group-
name
```

If Hitachi Command Suite products of versions v8.1.2 or later are not installed:

```
drive-in-which-the-installation-DVD-ROM-is-set:\HGLM\Hbase
\ClusterSetup\hcmds64clustersrvstate /soff /r resource-group-
name
```

The options for the `hcmds64clustersrvstate` command are as follows:

- `/soff`

  Places the Hitachi Command Suite product services that have been configured in cluster management applications offline and suppresses a failover.

- `/r`

  Specifies a resource group name. If a resource group name includes any of the following characters, use double quotation marks to enclose the resource group name.

  `, ; =` spaces

  In addition, you cannot use the following characters:

  `! " & ) * ^ | < >`

3. Execute the following command to back up the database to the folder for backup data storage on the local disk, and then re-create the database in the specified folder on the shared disk.

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64dbclustersetup /createcluster /databasepath folder-on-
shared-disk-for-database-re-creation /exportpath folder-on-local-
disk-for-backup-data-storage /auto
```

folder-on-shared-disk-for-database-re-creation

Specifies the folder for database re-creation on the shared disk to be used in a cluster environment.

folder-on-local-disk-for-backup-data-storage

Specifies the destination folder in which to store the database before migration to be backed up.

Caution:

- Before executing the command `hcmds64dbclustersetup`, delete or empty the folders *folder-on-shared-disk-for-database-re-creation* and *folder-on-local-disk-for-backup-data-storage*.
- Executing the command `hcmds64dbclustersetup` returns the port number used by HiRDB back to its default value (22032).
- For the folder *folder-on-shared-disk-for-database-re-creation* on the shared disk, free space equal to the sum of the database capacities shown below is required.

If execution of the command `hcmds64dbclustersetup` fails due to insufficient free space, increase the amount of free space in the folder, and then re-execute the command `hcmds64dbclustersetup`.

  - Database capacity of Hitachi Command Suite Common Component
  - Database capacity of all Hitachi Command Suite products (including Global Link Manager) that are installed on the same host as Global Link Manager

- Do not detach the shared disk from the active node before execution of the command `hcmds64dbclustersetup` ends normally. If the host is restarted while the command `hcmds64dbclustersetup` is in an abnormal end status, the connection destination of the shared disk might switch to the standby node.
- If you use the `auto` option, after command execution, Hitachi Command Suite Common Component and HiRDB will be in the stopped status.
- For the *folder-on-shared-disk-for-database-re-creation* folder, specify a path on the shared disk. For the *folder-on-local-disk-for-backup-data-storage* folder, specify a path on the local disk.
- For the *folder-on-shared-disk-for-database-re-creation* and the *folder-on-local-disk-for-backup-data-storage* folders, specify an absolute path in a string of characters that is no more than 63 bytes.
- The following characters can be used for the *folder-on-shared-disk-for-database-re-creation* and the *folder-on-local-disk-for-backup-data-storage* folders:

  `A` to `Z`, `a` to `z`, `0` to `9`, `.`, `_`

  As a path delimiter character, you can also use `\`, `:`, and `/`.

4. If you have been using the function that outputs path availability information in a report, move the output path availability information (path status log) to a shared disk on which the database is stored. If you have not used the function, steps 4 to 6 are not necessary. Go to step 7.

   To export the path availability information (path status log):

   Execute the following command:

   ```
   Global-Link-Manager-installation-folder\bin\hglamexport /dir
   export-destination-folder-name
   ```

   Use an absolute path to specify *export-destination-folder-name*. When you specify an existing folder, make sure that the folder is empty.

   The following characters can be used for *export-destination-folder-name*:

   `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), and underscore (`_`). You can also use a backslash (`\`), colon (`:`), and forward slash (`/`) as the path delimiter. If you specify a path that includes a space character, enclose the path in double quotation marks (`"`).

   The following shows an example of executing the command:

   ```
   "C:\Program Files\HiCommand\HGLAM\bin\hglamexport" /dir "C:
   \hglamexport"
   ```

5. Edit the property file (`server.properties`).

   The `server.properties` file is stored in the following location:

   Global-Link-Manager-installation-folder\conf

   Change the folder for storing reports to a folder on the shared disk on which the database is stored.

   For `server.pathreport.log_location`, specify an absolute path (maximum of 150 bytes) for the folder that stores reports. Deploy this folder on the shared disk on which the database is stored. To use a backslash (\) as the path delimiter, you must use two consecutive backslashes.

   The following shows a coding example:

   ```
   server.pathreport.log_location=E:\\HGLAM\\pathreport
   ```

6. Import the path availability information (path status log).

   Execute the following command:

   Global-Link-Manager-installation-folder\bin\hglamimport /report *export-destination-folder-name*

   For *export-destination-folder-name*, use an absolute path to specify the folder for which backup data storage on the local disk exported by using the `hglamexport` command is stored.

   Caution

   Before executing the command, you must either delete the folder that you specified in step 5 or make sure that the folder is empty.

   If the folder is not empty, subfolders and files in the folder will be deleted.

7. Switch the group to which the services used by Global Link Manager have been registered to the standby system.

   Global Link Manager uses the following five services:

   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
   - Global Link Manager Web Service
   - HiRDB/ClusterService _HD1

   If Microsoft Failover Cluster is used (on OSs other than Windows Server 2012):

   In Failover Cluster Management, right-click the resource group to which the services used by Global Link Manager have been registered, and then choose **Move this service or application to another node**.

   If Microsoft Failover Cluster is used (on Windows Server 2012):

   In Failover Cluster Manager, right-click the role to which the services used by Global Link Manager have been registered, choose **Move** and then **Select Node**.

Procedure on the standby node

1. On the standby node, make sure that the standby node currently owns the Hitachi Command Suite Common Component service and the shared disk.
2. Execute the following command to confirm that the Hitachi Command Suite Common Component service has stopped:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /status
   ```

   If the service has not stopped, execute the command below to take the Global Link Manager services offline.

   If other Hitachi Command Suite products have been installed, this procedure places their services offline.

   If Hitachi Command Suite products of versions v8.1.2 or later are installed:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder
   \ClusterSetup\hcmds64clustersrvstate /soff /r resource-group-
   name
   ```

   If Hitachi Command Suite products of versions v8.1.2 or later are not installed:

   ```
   drive-in-which-the-installation-DVD-ROM-is-set:\HGLM\Hbase
   \ClusterSetup\hcmds64clustersrvstate /soff /r resource-group-
   name
   ```

   The options for the `hcmds64clustersrvstate` command are as follows:

   - `/soff`

     Places the Hitachi Command Suite product services that have been configured in cluster management applications offline and suppresses a failover.
   - `/r`

     Specifies a resource group name. If a resource group name includes any of the following characters, use double quotation marks to enclose the resource group name.

     `, ; =` spaces

     In addition, you cannot use the following characters:

     `! " & ) * ^ | < >`
3. Execute the following command to back up the database to the folder for backup data storage on the local disk, and then change the settings so that the specified folder for database re-creation on the shared disk is used.

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64dbclustersetup /createcluster /databasepath folder-on-
   shared-disk-for-database-re-creation /exportpath folder-on-local-
   disk-for-backup-data-storage /auto
   ```

   For the *folder-on-shared-disk-for-database-re-creation* folder, specify the same folder that you specified when migrating the database to the shared disk on the active node.

   folder-on-shared-disk-for-database-re-creation

Specifies the folder for database re-creation on the shared disk to be used in a cluster environment specified on the primary node.

folder-on-local-disk-for-backup-data-storage

Specifies the destination folder in which to store the database before migration to be backed up.

Caution:

- Before executing the command `hcmds64dbclustersetup`, delete or empty the folders *folder-on-shared-disk-for-database-re-creation* and *folder-on-local-disk-for-backup-data-storage*.
- If you use the `auto` option, after command execution, Hitachi Command Suite Common Component and HiRDB will be in the stopped status.
- For the folder *folder-on-local-disk-for-backup-data-storage*, specify a folder on the local disk.
- For the folder *folder-on-local-disk-for-backup-data-storage*, specify an absolute path whose length is 63 bytes or less.
- You can specify the following characters for the folder *folder-on-local-disk-for-backup-data-storage*:

  `A` to `Z`, `a` to `z`, `0` to `9`, `.`, `_`

  As path delimiter characters, you can also use `\`, `:`, and `/`.

---

4. When you want to use a function that outputs path availability information in a report, edit the property file (`server.properties`).

   The `server.properties` file is stored in the following location:

   `Global-Link-Manager-installation-folder``\conf`

   Change the folder for saving reports to a folder on the shared disk.

   For `server.pathreport.log_location`, specify the folder for saving reports. Specify the same folder as the one specified on the primary node.

5. Switch the group to which the services used by Global Link Manager have been registered to the executing system.

   Global Link Manager uses the following five services:

   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
   - Global Link Manager Web Service
   - HiRDB/ClusterService _HD1

   If Microsoft Failover Cluster is used (on OSs other than Windows Server 2012):

   In Failover Cluster Management, right-click the resource group to which a Hitachi Command Suite product service has been registered, and then select **Move this service or application to another node**.

   If Microsoft Failover Cluster is used (on Windows Server 2012):

In Failover Cluster Manager, right-click the role to which the services used by Global Link Manager have been registered, choose **Move**, and then **Select Node**.

6. Execute the following command to place the resource group and Global Link Manager product services online:

   If Hitachi Command Suite products of versions v8.1.2 or later are installed:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder
   \ClusterSetup\hcmds64clustersrvstate /son /r resource-group-
   name
   ```

   If Hitachi Command Suite products of versions v8.1.2 or later are not installed:

   ```
   drive-in-which-the-installation-DVD-ROM-is-set:\HGLM\Hbase
   \ClusterSetup\hcmds64clustersrvstate /son /r resource-group-
   name
   ```

   The options for the `hcmds64clustersrvstate` command are as follows:

   - `/son`

     Places the Hitachi Command Suite product services that have been configured in cluster management applications offline and suppresses a failover.

   - `/r`

     Specifies a resource group name. If a resource group name includes any of the following characters, use double quotation marks to enclose the resource group name.

     `, ; =` spaces

     In addition, you cannot use the following characters:

     `! " & ) * ^ | < >`

Caution

In the case you use Microsoft Failover Cluster, if HBase 64 Storage Mgmt Web Service is not started, start HBase 64 Storage Mgmt Web Service by in the **Services** panel, and place the service online by Failover Cluster Management.

Changing Global Link Manager environment settings

To change the Global Link Manager environment settings, edit the appropriate property files.

Location of files:

Global-Link-Manager-installation-folder\conf

Files:

- `server.properties` (Global Link Manager server settings file)
- `logger.properties` (Global Link Manager log file settings file)

- `database.properties` (Global Link Manager database settings file)

File format:

```
property-name=value
#comment
```

- Separate the property name and the value by using an equal sign (=).
- When inserting a comment line, begin the line by using a hash mark (#).

To edit the property file:

1. Use an application such as a text editor to open the property file, and then edit the file.

   For details on the values to be specified for each property, see the following sections:

   - Changing Global Link Manager server settings on page 3-34
   - Changing Global Link Manager log file settings on page 3-52
   - Changing Global Link Manager database settings on page 3-52

2. Restart Global Link Manager.

   To restart Global Link Manager, stop the services, and then start them again. For details on how to start and stop the services, see Starting and stopping Global Link Manager on page 3-3.

   Note

   If the format or value of the properties in the `server.properties` or `database.properties` file is incorrect, even if Hitachi Command Suite Common Component starts, Global Link Manager will not start. You should therefore check if the `KAIF10002-E` message has been output to the Global Link Manager message log file (`HGLAM_Message`*n*`.log`). If the `KAIF10002-E` exists, take appropriate action for the error by referencing the `KAIF10002-E` message and the preceding `KAIF24101-E` message, and then restart Global Link Manager. If no values are set for the properties or the format or value of the properties in the `logger.properties` file is incorrect, the default values are applied and Global Link Manager will start.

   The Global Link Manager message log file is stored in the following location:

   Global-Link-Manager-installation-folder`\logs`

Changing Global Link Manager server settings

To change the Global Link Manager server settings, edit the values for individual properties in the `server.properties` file. Rules for entering property values are as follows:

- Specify ASCII code characters.

- For a value for which `true` or `false` is to be specified, if you specify another value, `false` is assumed.
- To specify a folder, enter two consecutive path delimiters (`\`).

  Coding example:

  ```
  server.pathreport.log_location=C:\\Program Files\\HiCommand\
  \HGLAM\\pathreport
  ```

The following table describes the properties that are used to change the Global Link Manager server settings.

Table 3-3 Global Link Manager server properties (server.properties)

No.	Property name	Description
1	`server.thread.max_size`	Specifies the maximum number of threads that can be executed concurrently. Note Specify a value larger than the sum of the values specified for the following properties: ○ `server.auto_refresh.thread_num` ○ `server.network_scan.thread_num` Specifiable value: 1 to 50 Default: 15
2	`server.task.max_queue_size`	Specifies the maximum number of task queues. This value is regarded as the maximum number of hosts that you can operate at one time from the Global Link Manager GUI. Note Generally, do not change this value. If you want to use more than 100 hosts, divide them into separate groups. Specifiable value: 100 to 10000 Default: 100
3	`server.dbms.sweep_init`	Specifies the time from server startup until free-page collection starts. Specifiable value: 1 to 60 (minutes) Default: 5
4	`server.dbms.sweep_interval`	Specifies the interval between free-page collections. Specifiable value: 60 to 100000 (minutes) Default: 10080
5	`server.agent.max_retry_count`	Specifies the maximum number of retries for checking whether Hitachi

No.	Property name	Description
		Command Suite Common Agent Component has finished processing. Specifiable value: 1 to 350 Default: 110
6	`server.agent.timeout`	Specifies the period of time to detect a timeout when there is no response from HDLM. Specifiable value: 60 to 3600 (seconds) Default: 1200
7	`server.snmp.trap`	Specifies whether to enable the SNMP trap receiving function. Specify `true` to enable the function. Specify `false` to disable it.#7 Specifiable value: `true` or `false` Default: `true`#1
8	`server.snmp.trap_port_num`	Specifies the port number for receiving SNMP traps.#7 Note If Windows Firewall is used and you have changed this value, you must change the port number registered in the Windows Firewall exceptions list. Specifiable value: 1 to 65535 Default: 22620#1
9	`server.snmp.trap_thread_num`	Specifies the number of threads for processing SNMP traps. Specifiable value: 1 to 10 Default: 3
10	`server.snmp.trap_max`	Specifies the maximum number of SNMP traps (alerts) to be retained. Specifiable value: 1000 to 30000 Default: 10000
11	`server.snmp.auto_set`	Specifies whether to automatically configure alert notification for a host when the host is added or host information is updated. Specify `true` to automatically configure alert notification. Specify `false` not to automatically configure alert notification. Note To configure alert notification for each host, specify `false`. Specifiable value: `true` or `false`

No.	Property name	Description
		Default: `true`#10
12	`server.snmp.trap_community`	Specifies the SNMP Community value.#7 Specifiable value: Alphanumeric string of 15 characters or less (a-z, A-Z, and 0-9)#8 Default: `public`
13	`server.snmp.trap_ip_address`	Specifies the IP address of the SNMP trap destination. An IPv4 address can be specified. The SNMP trap destination is the server on which Global Link Manager is installed. If you change the IP address for the server on which Global Link Manager is installed, make sure to change the value of this property.#7 Note If you do not change the value of this property when the IP address for the server on which Global Link Manager is installed is changed, reception of SNMP traps becomes unavailable. Specifiable value: String of 15 characters or less Default: `--`#1
14	`server.snmp.trap_ipv6_address`	Specifies the IP address of the SNMP trap destination. An IPv6 address can be specified. The SNMP trap destination is the server on which Global Link Manager is installed. If you change the IP address for the server on which Global Link Manager is installed, make sure to change the value of this property.#7 Note If you do not change the value of this property when the IP address for the server on which Global Link Manager is installed is changed, reception of SNMP traps becomes unavailable. Specifiable value: String of 39 characters or less Default: `--`#1
15	`gui.indicator.auto_refresh_interval`	Specifies the automatic refresh interval for the **Dashboard** menu in the Global Link Manager GUI. Specifiable value: 1 to 10000 (minutes)

No.	Property name	Description
		Default: 1
16	`server.snmp_transfer.enable`	Specifies whether to enable alert transfer. Specify `true` to enable alert transfer. Specify `false` to disable it. Note If alert transfer is enabled: You can specify the SNMP version. For details, see the section that describes the **Configure Alert Transfer** dialog box in the Global Link Manager User Guide. If alert transfer is disabled: The settings specified in the **Configure Alert Transfer** dialog box are deleted. Specifiable value: `true` or `false` Default: `false`
17	`server.snmp_transfer.ip_address`	Specifies the IP address of the alert transfer destination server. Either an IPv4 address or IPv6 address can be specified. If a firewall is set up between the Global Link Manager server and the destination server, be sure to set the IP address and port number of the destination server for the firewall. Note Do not specify the following values: ○ The IP address specified for `server.snmp.trap_ip_address` ○ The IP address of the Global Link Manager server (when the machine has multiple IP addresses, the specified IP address must be different from any of these IP addresses.) ○ `127.0.0.1` and `0.0.0.0` (for IPv4) ○ `0:0:0:0:0:0:0:1` and `0:0:0:0:0:0:0:0` (for IPv6) ○ A multicast address (for IPv6) This can only be used when the same multicast address is set for all hosts on the network, and the multicast

No.	Property name	Description
		address is operating in the same manner as IPv4 broadcasts. ○ A broadcast address (for IPv4) Specifiable value: Character string Default: None
18	`server.snmp_transfer.port_num`	Specifies the port number of the alert transfer destination server. If a firewall is set up between the Global Link Manager server and the destination server, be sure to set the IP address and port number of the destination server for the firewall. Specifiable value: Number from 1 to 65535 Default: 162
19	`server.snmp_transfer.critical_enable`	Specifies whether to transfer `Critical` level alerts during alert transfer. Specify `true` to transfer Critical level alerts. Specify `false` not to transfer them. Specifiable value: `true` or `false` Default: `true`#2
20	`server.snmp_transfer.error_enable`	Specifies whether to transfer `Error` level alerts during alert transfer. Specify `true` to transfer Critical level alerts. Specify `false` not to transfer them. Specifiable value: `true` or `false` Default: `true`#2
21	`server.snmp_transfer.warning_enable`	Specifies whether to transfer `Warning` level alerts during alert transfer. Specify `true` to transfer Critical level alerts. Specify `false` not to transfer them. Specifiable value: `true` or `false` Default: `true`#2
22	`server.snmp_transfer.information_enable`	Specifies whether to transfer `Information` level alerts during alert transfer. Specify `true` to transfer Critical level alerts. Specify `false` not to transfer them. Specifiable value: `true` or `false` Default: `true`#2

No.	Property name	Description
23	server.snmp_transfer.path_enable	Specifies whether to transfer alerts whose category is Path during alert transfer. Specify true to transfer alerts of the Path category. Specify false not to transfer them. Specifiable value: true or false Default: true#2
24	server.snmp_transfer.host_enable	Specifies whether to transfer alerts whose category is Host during alert transfer. Specify true to transfer alerts of the Host category. Specify false not to transfer them. Specifiable value: true or false Default: true#2
25	server.snmp_transfer.hdlm_enable	Specifies whether to transfer alerts whose category is HDLM during alert transfer. Specify true to transfer alerts of the HDLM category. Specify false to not transfer them. Specifiable value: true or false Default: true#2
26	server.snmp.alert_refresh_enable	Specifies whether to enable automatic update of the host when an alert is received.#9 Specify true to enable it. Specify false to disable it. Specifiable value: true or false Default: true
27	server.auto_refresh.enable	Specifies whether to enable automatic update of the host. Specify true to enable it. Specify false to disable it. Specifiable value: true or false Default: true
28	server.auto_refresh.interval	Specifies the automatic update interval for the host. Specifiable value: 180 to 2880 (minutes) Default: 180
29	server.auto_refresh.thread_num	Specifies the maximum number of automatic update operations that can be performed concurrently on the hosts. Note When you change this value, specify a value so that the sum of this value and the value of server.network_scan.thread_n

No.	Property name	Description
		um is less than the value of server.thread.max_size. Specifiable value: 1 to 50 Default: 5
30	server.pathreport.enable	Specifies whether to allow Global Link Manager to acquire the path availability information (path status log) from HDLM for output in a report. Specify true to allow Global Link Manager to acquire the information. Specify false if you do not want to allow Global Link Manager to acquire the information.#3 Notes ○ If you have changed this value, you must update the host information. ○ If you have specified true for this value, check the following information: • true is specified for server.auto_refresh.enable. • The disk has sufficient free space for acquiring the path availability information (path status log). For details on the required log file size per host, see the explanation for server.pathreport.log_total_size_per_host. ○ If the path availability information is not required and you specify false for this property, return the value set for server.pathreport.log_location to the default. If you do not do this, the folder specified for that value will be created. Specifiable value: true or false Default: false
31	server.pathreport.log_location	Specifies the folder for storing the path availability information (path status log). Under this folder, the subfolder \PathStatusLog*IP-address-of-the-host* is created, and a CSV file is output to that subfolder in the following format:

No.	Property name	Description
		`PathStatusLog_`*host-IP-address_date*`.csv` For the IPv6 format, (`:`) is changed to (`-`) in *host-IP-address*. When the path availability information (path status log) has already been output and you want to change the folder in which the information is stored, you need to move the output path availability information (path status log) to a new folder. For details on how to move the output information, see When changing a folder in which path availability information (path status log) is stored on page 3-50. If you use the default value for the folder, that folder is automatically deleted when Global Link Manager is removed. If you specify a folder other than the default, you need to delete the folder manually because it is not deleted automatically. Notes ○ You cannot specify a path on the network. Specify the local disk. ○ If you specify a value other than the default, a folder will be created regardless of the setting for `server.pathreport.enable`. If the folder cannot be created, an error will occur when Global Link Manager starts. ○ Do not edit the file stored in this folder because it is used for the report output in the Global Link Manager GUI. If you edit the file, the report might not be output correctly. Specifiable value: Valid absolute path of 150 bytes or less#4 Default: *Global-Link-Manager-installation-folder*`\pathreport`
32	`server.pathreport.log_total_size_per_host`	Specifies the size of the path availability information (path status log) for a host. When the specified value is exceeded, files will be deleted starting from a file whose file name has the oldest

No.	Property name	Description
		date. Therefore, if needed, back up those files. For a large-scale configuration, the default value is the approximate size of the information for about 90 days. Specifiable value: 10 to 1024 (MB) Default: 100
33	`server.network_scan.thread_num`	Specifies the maximum number of hosts that can be added concurrently for network scanning. Note When you change this value, specify a value so that the sum of this value and the value of `server.auto_refresh.thread_num` is less than the value of `server.thread.max_size`. Specifiable value: 1 to 20 Default: 3
34	`server.trouble_detection.enable`	Specifies whether to enable the path error detection function. Specify `true` to enable it. Specify `false` to disable it. Specifiable value: `true` or `false` Default: `true`
35	`server.alert_gathering.interval`	Specifies the interval for gathering alert information for the email notification function. Specifiable value: `0` to `1440` (minutes) Default: `10`
36	`server.alert_email.from.address`	Specifies the address when changing the source address of emails that are sent from the Global Link Manager server by using the email notification function of alerts. Notes ○ This property is case-sensitive. ○ Use two backslashes (`\\`) to specify a single backslash (`\`) as a character. Specifiable value: Character string that complies with the email address format (RFC 822) Default: None (An anonymous address is used.)
37	`gui.export.version`	Specifies the Global Link Manager version of the format of a CSV file to

No.	Property name	Description
		which management information is output. If the value is not specified or is invalid, the format of the latest version is used. Specifiable value: `5.0`, `5.6`, `5.7`, `6.0`, `6.1`, `6.2`, `6.3`, `7.2`, `7.3`, `7.6`, or `8.0` Default: None (output in the format of the latest version)
38	`gui.report.version`	Specifies the Global Link Manager version to use for formatting reports that are output. If no value is specified or the value is invalid, reports are output using the format of the latest version. Specifiable value: `7.2`, `7.6`, or `8.0` Default: None (Reports are output using the format of the latest version.)
39	`gui.ham.view`	If gui.export.version is version 7.6 or earlier, specifies whether to export the following information to a CSV file when paths obtained from managed hosts are in the HAM configuration: • Original LDEV ID of the secondary volume • Original storage system name of the secondary volume Specifiable value: `true` or `false` Default: `true`
40	`gui.id_take_over.view`	If gui.export.version or gui.report.version is version 7.6 or earlier, specifies whether to export the following information to a CSV file. Specify `true` to export the information. Specify `false` to not export the information. • Physical LDEV ID • Physical Storage System • Physical CHA Specifiable value: `true` or `false` Default: `false`
41	`gui.physical.view`	Specifies whether to display the physical information in the path list in the Hitachi Global Link Manager management window when paths obtained from managed hosts include the following information. Specify `true` to display the information.

No.	Property name	Description
		Specify `false` to not display the information. • HAM • ID take over • H-UVM configuration Note If gui.export.version or gui.report.version is v8.0 or later and you output physical information of HUVM to a CSV file, specify `true`. Note that if gui.id_take_over.view is `true`, the physical information of the migration destination for ID take over is also output. Also, if gui.ham.view is `true`, the physical information of the S-VOL for HAM is also output. Specify `false` to not output the physical information. Specifiable value: `true` or `false` Default: `true`
42	`getlogs.pathreport.get_mode`	Specifies the method of acquiring the path availability information (path status log), as the Global Link Manager diagnostic information#5. Specifiable value: 0 to 3 0: Does not acquire the path availability information (path status log). 1: Acquires, for all hosts, logs from the 90 days preceding the current date. 2: Specifies, for a specific host, the starting date and ending date of log acquisition. (If you specify this value, also specify the values for `getlogs.pathreport.host`, `getlogs.pathreport.startDate`, and `getlogs.pathreport.endDate`.) 3: Acquires all of the folders specified for `server.pathreport.log_location`. Default: 0
43	`getlogs.pathreport.host`	Specifies the IP address of the target host or hosts when acquiring the path availability information (path status log), as the Global Link Manager diagnostic information#5. Either an

No.	Property name	Description
		IPv4 address or IPv6 address can be specified. To specify multiple hosts, separate them by commas (,). This value takes effect only when the value set for `getlogs.pathreport.get_mode` is 2. Specifiable value: Character string Default: None (The information is acquired from all hosts)
44	`getlogs.pathreport.startDate`	Specifies the start date for acquisition of the path availability information (path status log), as the Global Link Manager diagnostic information#5. Specify a date in the *yyyymmdd* format. This value takes effect only when the value of `getlogs.pathreport.get_mode` is 2. Specifiable value: Character string Default: None (The information is acquired in the order of the date in the file name from oldest to newest.)
45	`getlogs.pathreport.endDate`	Specifies the end date for acquisition of the path availability information (path status log), as the Global Link Manager diagnostic information#5. Specify a date in the *yyyymmdd* format. This value takes effect only when the value set for `getlogs.pathreport.get_mode` is 2. Specifiable value: Character string Default: None (The information is acquired up to the file that has the most recent date in the file name.)
46	`server.hdvm.polling.time`	Specifies the time for acquisition of LDEV label information. Specify a date in the *hh*:*mm*:*ss* format. This value takes effect only if the value set for `server.hdvm.ldevlabel.acquisition.enable` is `true`. Specifiable value: 00:00:00 to 23:59:59 (hours, minutes, seconds) Default: None
47	`server.hdvm.http.ipaddr`	Specifies the IP address of the Device Manager server from which LDEV label information is acquired, as well as the HTTP port number#6 used by the Device Manager server (`2001` by

No.	Property name	Description
		default). This property applies to Device Manager servers where SSL communication has not been set up. Either an IPv4 address or IPv6 address can be specified. When specifying an IPv6 address, enclose the IP address in square brackets (`[ ]`). Specify the port number after the IP address by separating them by a colon. You can specify up to 10 Device Manager servers, including those specified by using `server.hdvm.https.ipaddr`. Device Manager servers specified by using `server.hdvm.https.ipaddr` take priority over those specified by this property. To specify multiple Device Manager servers, separate them by commas. For example, specify an IPv4 address Device Manager server and an IPv6 address Device Manager server as two hosts as follows: `10.208.999.01:2001,[::128]:2001` This value takes effect only if the value set for `server.hdvm.ldevlabel.acquisition.enable` is `true`. Specifiable value: Character string Default: None
48	`server.hdvm.https.ipaddr`	Specifies the IP address of the Device Manager server from which LDEV label information is acquired, as well as the HTTP port number#6 used by the Device Manager server (`2443` by default). This property applies to Device Manager servers where SSL communication has been set up. Either an IPv4 address or IPv6 address can be specified. When specifying an IPv6 address, enclose the IP address in square brackets (`[ ]`). Specify the port number after the IP address by separating them by a colon. You can specify up to 10 Device Manager servers, including those specified by using `server.hdvm.http.ipaddr`. Device Manager servers specified by this

No.	Property name	Description
		property take priority over those specified by using `server.hdvm.http.ipaddr`. To specify multiple Device Manager servers, separate them by commas. For example, specify an IPv4 address Device Manager server and an IPv6 address Device Manager server as two hosts as follows: `10.208.999.01:2443,[::128]:2443` This value takes effect only if the value set for `server.hdvm.ldevlabel.acquisition.enable` and each `server.https.enable` is `true`. Specifiable value: Character string Default: None
49	`server.hdvm.ldevlabel.acquisition.enable`	Specifies whether to enable acquisition of LDEV label information. Specify `true` to enable it. Specify `false` to disable it. Specifiable value: `true` or `false` Default: `false`
50	`server.https.enable`	Specifies whether to enable SSL communication. Specify `true` to enable it. Specify `false` to disable it. Specifiable value: `true` or `false` Default: `false`
51	`server.https.truststore`	Specifies the truststore file set by using the `hglamkeytool` utility. Specify an absolute path within 255 bytes. Note If you specify a path that includes a symbolic link, for example *installation-folder-specified-in-the-installer*`\\Base64\\uCPSB\\jdk\\jre\\lib\\security\\jssecacerts`, the destination of the link might change. Use the `hcmds64chgjdk` command or a similar method to change the Java program. If the destination of the symbolic link has changed, you will have to re-import the certificate to the truststore file. Specifiable value: Character string Default: None

No.	Property name	Description
52	gui.hdlm_installer.downloadfromdvd.enable	Specifies whether to enable the downloading of the HDLM installer from DVD-ROM data on a server. Specify true to enable this function. Specify false to disable it. Specifiable values: true or false Default: true
53	gui.hdlm_installer.fromdvd.location	Specifies a folder as a mount point for the DVD-ROM. This value takes effect only if the value specified for gui.hdlm_installer.downloadfromdvd.enable is true. Specifiable value: Character string Default: *DVD-drive-used-when-installing-Global-Link-Manager*\\HGLM

#1

These values are replaced with the values that are specified during the installation.

#2

When alert transfer is used on a host on which HDLM has been installed, all alert information is output by default, causing a huge amount of alert information to be transferred. If you do not want to have so much alert information transferred, we recommend that you set up the Global Link Manager server so that only alerts whose category is Host are transferred. You can also specify true for server.snmp.alert_refresh_enable so that the host is automatically updated when a machine that receives SNMP traps receives an alert from the host. This specification enables immediate alert transfer.

To transfer only the alerts whose category is Host, specify true for the following properties and specify false for other properties superscripted with #2.

- server.snmp_transfer.host_enable
- server.snmp_transfer.critical_enable (when transferring Critical level alerts)
- server.snmp_transfer.error_enable (when transferring Error level alerts)

#3

Regardless of the setting, information that has already been acquired can be output as a report. However, an empty report is output when path availability information (path status log) for the specified period of time does not exist.

#4

The Windows local system account (`SYSTEM`) must have full control permissions for the specified folder including subfolders and files, and the output CSV files (path availability information files). For the specified folder including subfolders and files, do not set the access permission for accounts other than the Windows local system account (`SYSTEM`) and Global Link Manager administrator.

#5

For details on how to acquire Global Link Manager diagnostic information, see Diagnostic batch collection about the Global Link Manager server on page 7-6.

#6

For details about the port numbers used by Device Manager servers, see the *Hitachi Command Suite Administrator Guide*.

#7

If this value is changed, you need to refresh the hosts monitored by SNMP traps so that the new value is applied to those hosts as well. Note, however, that the `server.snmp.auto_set` property must be set to `true` so that the new value is applied when the host is refreshed.

#8

In addition to alphanumeric characters, you can also use the following symbols if the hosts registered in HGLM are hosts running HDLM 06-40-00 or later: ` ~ ! # $ % ( ) * + , - . / : ; ? @ [\ ] ^ _ { | }

Note that you must use two backslashes (`\\`) to specify a single backslash (`\`).

#9

The alert of the path error includes the following message IDs.

- KAIF60100-E
- KAIF60145-E
- KAIF60155-E
- KAPL08022-E

#10

Depending on the settings configured during installation, the value of this property is replaced with the value of `server.snmp.trap`.

When changing a folder in which path availability information (path status log) is stored

When you change the folder in which path availability information (path status log) is stored, you need to move the output path availability information (path status log) to a new folder.

If other Hitachi Command Suite products have already been installed on the same machine, the services of these products are also started or stopped at

the same time when you start or stop Hitachi Command Suite Common Component.

To move the output path availability information (path status log) to a new folder:

1. Execute the following command to stop Hitachi Command Suite Common Component:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder\bin
   \hcmds64srv /stop
   ```

2. Export the path availability information (path status log).

   Execute the following command:

   ```
   Global-Link-Manager-installation-folder\bin\hglamexport /dir
   export-destination-folder-name
   ```

   Use an absolute path to specify *export-destination-folder-name*. When you specify an existing folder, make sure that the folder is empty.

   The following characters can be used for *export-destination-folder-name*:

   `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), and underscore (`_`). You can also use a backslash (`\`), colon (`:`), and forward slash (`/`) as the path delimiter. If you specify a path that includes a space character, enclose the path in double quotation marks (`"`).

   The following shows an example of executing the command:

   ```
   "C:\Program Files\HiCommand\HGLAM\bin\hglamexport" /dir "C:
   \hglam export"
   ```

3. For `server.pathreport.log_location` in the property file, specify the name of the folder in which you want to store the path availability information (path status log).

   For details on how to set the property file, see Changing Global Link Manager environment settings on page 3-33.

4. Import the path availability information (path status log).

   Execute the following command:

   ```
   Global-Link-Manager-installation-folder\bin\hglamimport /report
   export-destination-folder-name
   ```

   For *export-destination-folder-name*, use an absolute path to specify the folder in which the data exported by using the `hglamexport` command is stored.

   Caution

   Before executing the command, you must either delete the folder that you specified in step 3 or make sure that the folder is empty.

   If the folder is not empty, subfolders and files in the folder will be deleted.

5. Execute the following command to start Hitachi Command Suite Common Component:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64srv /start
```

Changing Global Link Manager log file settings

To change the settings for Global Link Manager log files (`HGLAM_Message`*n*`.log`), edit the `logger.properties` file. The following table describes the properties that are used to change the Global Link Manager log file settings.

Table 3-4 Global Link Manager log file properties (logger.properties)

No.	Property name	Description
1	`logger.max_backup_index`	Specifies the maximum number of log file backups. Specifiable value: 1 to 16 Default: 10
2	`logger.max_file_size`	Specifies the maximum log file size. Specifiable value: 4096 to 2147483647 bytes (4 KB to approximately 2 GB) Default: 16777216 bytes (approximately 16 MB)
3	`logger.syslog_level`	Specifies the logging level (threshold) for output to the OS event log or syslog. Specifiable value: 0, 10, 20, or 30 (in order of importance from left to right)# Default: 0
4	`logger.log_level`	Specifies the logging level (threshold) for output to the log file. Specifiable value: 0, 10, 20, or 30 (in order of importance from left to right)# Default: 20

#

The output levels of log files and the contents of the output messages are as follows:

0: Critical error, high-priority information

10: Non-critical error, medium-priority information

20: Warning

30: All debug information

Changing Global Link Manager database settings

To change the Global Link Manager database settings, edit the `database.properties` file. The following table describes the properties that are used to change the Global Link Manager database settings.

Table 3-5 Global Link Manager database properties (database.properties)

No.	Property name	Description
1	`database.poolsize`	Specifies the number of connections for a connection pool Specifiable value: 4 to 20 Default: 20
2	`database.connection_check_interval`	Specifies the connection check interval. Specifiable value: 600 to 7200 (seconds) Default: 3600
3	`database.connection_retry_times`	Specifies the maximum number of connection retries. Specifiable value: 18 to 180 Default: 30
4	`database.connection_retry_interval`	Specifies the connection retry interval. Specifiable value: 10 to 100 (seconds) Default: 30
5	`database.connectionpool_retry_times`	Specifies the maximum number of retries for acquiring a connection from the connection pool. Specifiable value: 0 to 5 Default: 3
6	`database.connectionpool_retry_interval`	Specifies the retry interval for acquiring a connection from the connection pool. Specifiable value: 1 to 180 (seconds) Default: 15
7	`database.transaction_retry_times`	Specifies the maximum number of transaction retries. Specifiable value: 0 to 10 Default: 5
8	`database.transaction_retry_interval`	Specifies the transaction retry interval. Specifiable value: 0 to 5 (seconds) Default: 1

Changing the Global Link Manager database password

You can change the authentication password that Global Link Manager uses to access the database.

Use the `hcmds64dbuser` command to change the database password.

The format of the `hcmds64dbuser` command is as follows:

Command format

```
hcmds64dbuser /type {GlobalLinkAvailabilityManager | HGLAM} {/
newpass password | /default}
```

This command is stored in the following location:

Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64dbuser

Option description

Table 3-6 hcmds64dbuser command options

Option	Description
/newpass *password*	Specify the password to be used for authentication when Global Link Manager accesses the database. The value specified for this option becomes the new authentication password. If this option is omitted, you will be prompted to enter a password. Specifiable values: A string of the following characters that is no more than 28 bytes Characters can be used for the first character: A to Z, a to z, \ (backslashes), @ (at marks), and # (number signs) Characters can be used for all other characters: A to Z, a to z, 0 to 9, \ (backslashes), @ (at marks), and # (number signs)
/default	Resets the authentication information to the default (for both HiRDB and Hitachi Command Suite Common Component resources). If you specify this option while the system is being changed to a cluster configuration or a database backup is being restored, because the authentication information is reset to the default, you do not need to set the authentication information again, thus simplifying operation.

Note

The hcmds64dbuser command can be executed even while a Hitachi Command Suite Common Component is being executed.

Changing the IP address or host name of the Global Link Manager server

If you change the IP address or host name of the management server on which Global Link Manager is installed, you also need to change the settings file for Hitachi Command Suite Common Component.

Changing the IP address of the Global Link Manager server

This section describes how to change the IP address of the management server on which Global Link Manager is installed.

Notes

- If you have changed the IP address of the management server before changing the settings files of Hitachi Command Suite products, write down the new IP address.
- Do not change the settings in the cluster configuration file (the `cluster.conf` file).

If other Hitachi Command Suite products have already been installed on the same machine, the services of these products are also started or stopped at the same time when you start or stop Hitachi Command Suite Common Component.

To change the IP address of the management server:

1. Execute the following command to stop Hitachi Command Suite Common Component:
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /stop
2. Edit the `user_httpsd.conf` file.
   If the old IP address is specified in the `user_httpsd.conf` file, change the IP address to the host name or the new IP address. We recommend that you specify the host name in the `user_httpsd.conf` file.
   The `user_httpsd.conf` file is stored in the following locations:
   Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\httpsd\conf\user_httpsd.conf
3. Change the IP address of the management server, and then restart the computer.
   If the IP address of the management server has already been changed before you change the Hitachi Command Suite Common Component settings files, just restart the computer.
4. Execute the following command to make sure that Hitachi Command Suite Common Component is running:
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /status
5. If the IP address is used in the URLs for accessing Global Link Manager, change the setting.
   For details on how to change the URLs, see Changing the Global Link Manager login URL on page 3-64.

Note that, if you change the IP address of the management server, you need to check and, if necessary, revise the settings for each Hitachi Command Suite product. For details about the settings that need to be changed, see Settings required after changing the IP address or host name of the Global Link Manager server on page 3-57.

Changing the Global Link Manager server host name

This section describes how to change the host name of the management server on which Global Link Manager is installed.

Note

The host name must be no more than 32 bytes. You can use the following characters:

A to Z a to z 0 to 9 –

Note that the host name cannot start or end with a hyphen (-).

If other Hitachi Command Suite products have already been installed on the same machine, the services of these products are also started or stopped at the same time when you start or stop Hitachi Command Suite Common Component.

To change the host name of the management server:

1. Before changing the host name, write down the host name.

   Execute the `hostname` command to check the host name (the `ipconfig /ALL` command can also be used). The host name to be specified in the settings file is case sensitive.

2. Execute the following command to stop Hitachi Command Suite Common Component:

   Hitachi-Command-Suite-Common-Component-installation-folder`\bin\hcmds64srv /stop`

3. If SSL is used for communication between the management client and management server, configure them again.

   Use the new host name to reconfigure the SSL settings. For details on how to configure SSL settings, see Security settings for communication between a server and clients on page 5-2.

4. Edit the `user_httpsd.conf` file.

   Change the value for the `ServerName` directive to the new host name.

   The following shows the storage destination for the `user_httpsd.conf` file:

   Hitachi-Command-Suite-Common-Component-installation-folder`\uCPSB\httpsd\conf\user_httpsd.conf`

   If SSL is used for communication between the management client and management server, change the following settings as well:

   - If a host name has been specified for the `<VirtualHost>` tag, change the host name to an asterisk (`*`).
   - Change the value for the `ServerName` directive in the `<VirtualHost>` tag to the new host name.

   Note

   Do not edit the `httpsd.conf` and `hsso_httpsd.conf` files.

5. In the cluster configuration, edit the `cluster.conf` file.

From among the virtual host name, host name for the primary node, and host name for the secondary node, change the corresponding host name to the new host name.

The following shows the storage destination for the `cluster.conf` file:

- *Hitachi-Command-Suite-Common-Component-installation-folder*`\conf\cluster.conf`

6. Change the host name for the management server, and then restart the computer.

   If you have changed the host name for the management server before changing the settings file for Hitachi Command Suite Common Component, restart the computer.

7. Execute the following command to make sure that Hitachi Command Suite Common Component is running:

   Hitachi-Command-Suite-Common-Component-installation-folder`\bin\hcmds64srv /status`

8. If a host name is used for the URL for logging into Global Link Manager, change the settings.

   For details on how to use the `hcmds64chgurl` command, see Changing the Global Link Manager login URL on page 3-64.

Note that, if you change the host name of the management server, you need to check and, if necessary, revise the settings for each Hitachi Command Suite product. For details about the settings that need to be changed, see Settings required after changing the IP address or host name of the Global Link Manager server on page 3-57.

Settings required after changing the IP address or host name of the Global Link Manager server

This section describes the settings required in Global Link Manager after you change the IP address or host name of the management server on which the Global Link Manager server is installed. For details about the settings for other Hitachi Command Suite products installed on the same server, see the manual for each product.

In Global Link Manager, check and revise the following settings:

List of hosts

Use the Global Link Manager GUI to re-register hosts in the list of hosts. If you do not re-register the hosts, you will not receive alerts. To re-register hosts, you have to delete all of the hosts from the list of hosts, and then add the hosts again. For details about the list of hosts in the Global Link Manager GUI, see the manual *Global Link Manager User Guide*.

Also, depending on the operating environment, you might need to check and revise the following settings:

If a RADIUS server is used to authenticate accounts

Check the settings in the `exauth.properties` file. For details on how to specify settings in the `exauth.properties` file, see Setting the exauth.properties file (when the authentication method is RADIUS) on page 3-107.

Changing Hitachi Command Suite Common Component port numbers

The following table lists and describes the port numbers used by Hitachi Command Suite Common Component:

Table 3-7 Ports used by Hitachi Command Suite Common Component

Network port	Description
22015/tcp#	This port is used to access non-SSL HBase 64 Storage Mgmt Web Service. If you want to change this port number, see Changing port numbers for accessing the HBase 64 Storage Mgmt Web Service on page 3-60.
22016/tcp	This port is used by Web browsers to access SSL HBase 64 Storage Mgmt Web Service. If you want to change this port number, see Changing port numbers for accessing the HBase 64 Storage Mgmt Web Service on page 3-60.
22031/tcp	This port is used for the internal communication (single sign-on) of Hitachi Command Suite Common Component. If you want to change this port number, see Changing the port number used for the internal communication (single sign-on) of Hitachi Command Suite Common Component on page 3-60.
22032/tcp	This port is used for the internal communication (HiRDB) of Hitachi Command Suite Common Component. If you want to change this port number, see Changing port numbers used for the internal communication (HiRDB) of Hitachi Command Suite Common Component on page 3-61.
22035/tcp 22037/tcp 22038/tcp 22125/tcp 22127/tcp 22128/tcp	This port is used for the internal communication (communication with the Web server) of Hitachi Command Suite Common Component. If you want to change this port number, see Changing the port number used by the internal communication (communication with the Web server) of Hitachi Command Suite Common Component on page 3-61.
22036/tcp 22126/tcp	This port is used for the internal communication (naming service) of Hitachi Command Suite Common Component. If you want to change this port number, see Changing the port number used by the internal communication (naming service) of Hitachi Command Suite Common Component on page 3-63.
22019/tcp to 22030/tcp, 22033/tcp, and 22034/tcp	These port numbers are reserved.

#

This port is also used when SSL is enabled. To interrupt non-SSL communication from outside the network to the management server, you need to edit the `user_httpsd.conf` file.

If other Hitachi Command Suite products have already been installed on the same machine, the services of these products are also started or stopped at the same time when you start or stop Hitachi Command Suite Common Component.

To change the Hitachi Command Suite Common Component port numbers after installing the Global Link Manager server:

1. Execute the following command to stop Hitachi Command Suite Common Component:
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /stop

2. Change the port numbers.
   The method used depends on which port number you want to change. For details on the correct method to use, see the appropriate section in the following:
   - Changing port numbers for accessing the HBase 64 Storage Mgmt Web Service on page 3-60
   - Changing the port number used for the internal communication (single sign-on) of Hitachi Command Suite Common Component on page 3-60
   - Changing port numbers used for the internal communication (HiRDB) of Hitachi Command Suite Common Component on page 3-61
   - Changing the port number used by the internal communication (communication with the Web server) of Hitachi Command Suite Common Component on page 3-61
   - Changing the port number used by the internal communication (naming service) of Hitachi Command Suite Common Component on page 3-63

3. Execute the following command to start Hitachi Command Suite Common Component:
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /start

4. If you change the following port numbers, you need to change the URLs used for accessing Hitachi Command Suite products:
   - 22015/tcp (used for accessing HBase 64 Storage Mgmt Web Service)
     You need to change the URLs if you use non-SSL for communication between the management server and management clients.
   - 22016/tcp (used for accessing SSL HBase 64 Storage Mgmt Web Service)

You need to change the URLs if you use SSL for communication between the management server and management clients.

For details about how to change the URLs, see Changing the Global Link Manager login URL on page 3-64.

Note that you might not need to change the URLs depending on the network environment between the management server and management clients, such as an environment that has a firewall configured.

Changing port numbers for accessing the HBase 64 Storage Mgmt Web Service

To change the port used to access the HBase 64 Storage Mgmt Web Service, change the port number specified in the `user_httpsd.conf` file.

1. Open the `user_httpsd.conf` file at the following location:

   Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\httpsd\conf\user_httpsd.conf

2. If you want to change the port number for HTTP communication, change the port number in the `Listen` directive where 22015 is specified by default. To change the port number for HTTPS communication (using SSL), change the port number for the `Listen` #directive where 22016 is specified by default, and the value for `VirtualHost`.

   ```
   Listen 22015
   SSLDisable

   Listen 22016
   <VirtualHost www.example.com:22016>
   ```

   #

   Even when SSL is enabled for accessing HBase 64 Storage Mgmt Web Service, do not delete or comment out the `Listen 22015` lines.

   To interrupt non-SSL communication from outside the network to the management server, you need to edit the `user_httpsd.conf` file.

   To use SSL, perform SSL setup in addition to changing the port number. For details about SSL setup, see Chapter 5, Security settings for communication on page 5-1.

Changing the port number used for the internal communication (single sign-on) of Hitachi Command Suite Common Component

To change the port used for the internal communication (single sign-on) of Hitachi Command Suite Common Component, change the port in the following file:

1. Open the `user_hsso_httpsd.conf` file at the following location:

   Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\httpsd\conf\user_hsso_httpsd.conf

2. Specify the port number to `Listen` in the following format:
   `Listen 127.0.0.1:`*`port-number`*

Changing port numbers used for the internal communication (HiRDB) of Hitachi Command Suite Common Component

To change the port numbers used for the internal communication (HiRDB) of Hitachi Command Suite Common Component, change the port number specified in the `HiRDB.ini`, `pdsys`, and `def_pdsys` files.

Editing the HiRDB.ini file

1. Open the `HiRDB.ini` file at the following location:
   `Hitachi-Command-Suite-Common-Component-installation-folder``\HDB\CONF\emb\HiRDB.ini`

2. Change the port number in the entry `PDNAMEPORT=22032`.

Editing the pdsys file

1. Open the `pdsys` file at the following location:
   `Hitachi-Command-Suite-Common-Component-installation-folder``\HDB\CONF\pdsys`

2. Change the port number in the entry `pd_name_port=22032`.

Editing the def_pdsys file

1. Open the `def_pdsys` file at the following location:
   `Hitachi-Command-Suite-Common-Component-installation-folder``\database\work\def_pdsys`

2. Change the port number in the entry `pd_name_port=22032`.

Changing the port number used by the internal communication (communication with the Web server) of Hitachi Command Suite Common Component

To change the port number used by the internal communication (communication with the Web server) of Hitachi Command Suite Common Component, change the port number in the `workers.properties` and `usrconf.properties` files.

Editing the workers.properties file

When changing 22035/tcp

1. Open the `workers.properties` file at the following location:

Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\CC\web\redirector\workers.properties

2. Change the port number in the entry worker.HBase64StgMgmtSSOService.port=22035.

When changing 22125/tcp

1. Open the workers.properties file at the following location:
   Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\CC\web\redirector\workers.properties
2. Change the port number in the entry worker.GlobalLinkManagerWebService.port=22125.

Editing the usrconf.properties file

When changing 22035/tcp

1. Open the usrconf.properties file at the following location:
   Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties
2. Change the port number in the entry webserver.connector.ajp13.port=22035.

When changing 22037/tcp

1. Open the usrconf.properties file at the following location:
   Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties
2. Change the port number in the entry ejbserver.http.port=22037.

When changing 22038/tcp

1. Open the usrconf.properties file at the following location:
   Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties
2. Change the port number in the entry ejbserver.rmi.remote.listener.port=22038.

When changing 22125/tcp

1. Open the usrconf.properties file at the following location:
   Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\CC\server\usrconf\ejb\\GlobalLinkManagerWebService\usrconf.properties

2. Change the port number in the entry
`webserver.connector.ajp13.port=22125`.

When changing 22127/tcp

1. Open the `usrconf.properties` file at the following location:
Hitachi-Command-Suite-Common-Component-installation-folder`\uCPSB\CC\server\usrconf\ejb\\GlobalLinkManagerWebService\usrconf.properties`
2. Change the port number in the entry `ejbserver.http.port=22127`.

When changing 22128/tcp

1. Open the `usrconf.properties` file at the following location:
Hitachi-Command-Suite-Common-Component-installation-folder`\uCPSB\CC\server\usrconf\ejb\\GlobalLinkManagerWebService\usrconf.properties`
2. Change the port number in the entry
`ejbserver.rmi.remote.listener.port=22128`.

Changing the port number used by the internal communication (naming service) of Hitachi Command Suite Common Component

To change the port number used by the internal communication (naming service) of Hitachi Command Suite Common Component, you need to specify the port number in the `usrconf.properties` file.

When changing 22036/tcp

1. Open the `usrconf.properties` file at the following location:
Hitachi-Command-Suite-Common-Component-installation-folder`\uCPSB\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties`

2. Change the port number in the entry
`ejbserver.rmi.naming.port=22036`.

When changing 22126/tcp

1. Open the `usrconf.properties` file at the following location:
Hitachi-Command-Suite-Common-Component-installation-folder`\uCPSB\CC\server\usrconf\ejb\\GlobalLinkManagerWebService\usrconf.properties`

2. Change the port number in the entry
`ejbserver.rmi.naming.port=22126`.

Setting up the Global Link Manager server to use the Global Link Manager GUI

This section describes the settings for changing the URL used for starting the Global Link Manager GUI, and the settings for adding the Go menu and the Links menu item to the Global Link Manager GUI.

Changing the Global Link Manager login URL

If you have changed the following Global Link Manager settings, you must change the URL that is used for starting the Global Link Manager GUI.

- The IP address or host name of the server on which Global Link Manager is installed
- The port number used by HBase 64 Storage Mgmt Web Service
- The settings for using SSL, or for stopping the use of SSL
- Changing from a non-cluster configuration to a cluster configuration

To change the URL used for starting the Global Link Manager GUI, execute the following command:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64chgurl /change old-URL new-URL
```

Specify the URL in the following format:

```
http://IP-address-or-host-name-of-server:HBase-Storage-Mgmt-Web-
Service-port-number
```

Note

The specified URL needs to be complete, including the protocol and port. IPv6 addresses cannot be used. Specify a host name for an IPv6 environment. The following gives an example:

```
http://127.0.0.1:22015
http://hostname:22015
```

To change the URL only for Global Link Manager on a machine that has multiple Hitachi Command Suite products installed, execute the following command:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64chgurl /change new-URL /type GlobalLinkAvailabilityManager
```

To check *old-URL*, execute the following command:

```
Hitachi-Command-Suite-Common-Component-installation-folder\bin
\hcmds64chgurl /list
```

Adding the Go and Links menus

By using the Global Link Manager GUI, you can register links to any Web application or Web page. After you register links, the **Go** menu and its **Links** menu item are added to the Global task bar area in the Global Link Manager GUI.

To register links, execute the following command:

```
hcmds64link {/add | /delete } /file user-setup-application-file[/
nolog] /user user-ID /pass password
```

Option

Table 3-8 hcmds64link command option

Option	Description
`/add`	Specify this option when you add links.
`/delete`	Specify this option when you delete links.
`/file` *user-setup-application-file*	Specify the file used for registering the link information (user setup application file).
`/nolog`	If you specify this option, messages are output only to the command line. Note that the messages for option errors are displayed even if this option is specified.
`/user` *user-ID* `/pass` *password*	This option specifies the user ID and password for logging in to Global Link Manager. Specify the ID for the user who has the Admin (Global Link Manager management) permission.

How to create the user setup application file

In the file specified as the user setup application file, add the link information in the following format:

Table 3-9 Format of the user setup application file

```
@TOOL-LINK
@NAME registration-key-name
@URL startup-URL
@DISPLAYNAME display-in-links-dialog-box
@DISPLAYORDER display-order-in-links-dialog-box
@ICONURL icon-URL
@TOOL-END
```

Table 3-10 Items specified in the user setup application file

Item	Description
`@TOOL-LINK`	Starting key of the user setup application file. This item is mandatory.
`@NAME` *registration-key-name*	This information is used as the key used for registration. For *registration-key-name*, specify the name so that the link information becomes unique, using alphanumeric characters (maximum 256 bytes). This item is mandatory.
`@URL` *startup-URL*	Specify the URL to be started from the Global Link Manager GUI (maximum 256 bytes). IPv6 addresses cannot be used. Specify a host name for an IPv6 environment.

Item	Description
`@DISPLAYNAME` *display-in-links-dialog-box*	Specify the link name to be displayed in the Links dialog box (maximum 80 bytes). You can specify a Unicode code point in the range from U+10000 to U +10FFFF. If you do not specify this item, the value specified in the `@NAME` line will be the link name.
`@DISPLAYORDER` *display-order-in-links-dialog-box*	Specify the order of values to be displayed in the Links dialog box (from -2147483648 to 2147483647). Values specified here are displayed in ascending order in the Links dialog box.
`@ICONURL` *icon-URL*	Specify the location of the icon displayed on the side of the link (maximum 256 bytes). IPv6 addresses cannot be used. Specify a host name for an IPv6 environment.
`@TOOL-END`	Ending key of the user setup application file. This item is mandatory.

The user setup application file is coded by ASCII code. Available character control codes are CR and LF.

Table 3-11 Example of the user setup application file

```
@TOOL-LINK
@NAME SampleApp
@URL http://SampleApp/index.html
@DISPLAYNAME SampleApplication
@DISPLAYORDER 1
@ICONURL http://SampleApp/graphic/icon.gif
@TOOL-END
```

Setup when a firewall is used

When a firewall is already configured, if you enable Windows Firewall after installing Global Link Manager, you need to perform the following setup.

Setup required for a network that has a firewall configured

If a firewall is already configured between a management server and management client, or between a management server and management host, set up the firewall so that each port can be used for communication, according to the tables below.

Table 3-12 Port numbers required for communications between a management server and management client

Port number	Source of communication	Destination of communication	Remarks
22015/tcp#	Management client	Management server	This setting is required for non-SSL communications.

Port number	Source of communication	Destination of communication	Remarks
22016/tcp#	Management client	Management server	This setting is required for SSL communications.

#: The port number is changeable. For details on port numbers used for communications between a Management Server and Management Client, see Changing port numbers for accessing the HBase 64 Storage Mgmt Web Service on page 3-60.

Table 3-13 Port numbers required for communications between a management server and management host

Port number	Source of communication	Destination of communication	Remarks
24041/tcp#	Management server	Management host	This setting is required.
24042/tcp#	Management server	Management host	This setting is required for non-SSL communications.
24045/tcp#	Management server	Management host	This setting is required for SSL communications.
22620/udp#	Management host	Management server	This setting is required if the management host receives SNMP traps.

The port number is changeable. For details on the port number required for communications between a management server and management host, see Changing the settings of Hitachi Command Suite Common Agent Component on page A-3. For details on the port number required for receiving SNMP traps, see the part that describes the `server.snmp.trap_port_num` property in Changing Global Link Manager server settings on page 3-34.

Settings for Windows firewalls

If you enable Windows Firewall after installing Global Link Manager, you must register Hitachi Command Suite Common Component and a port number that receives SNMP traps as an exception in the Windows Firewall exceptions list.

To register Hitachi Command Suite Common Component and a port number as an exception:

1. Execute the following command to register Hitachi Command Suite Common Component as an exception:
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64fwcancel.bat

2. In the Windows Firewall dialog box, register the port number that receives SNMP traps as an exception.
   The items that you need to register are as follows:

Name: Specify the name that indicates the port number that receives SNMP traps (example: HGLAM_SNMP).

Port number: Specify the port number that receives SNMP traps. Select **UDP** for the protocol.

Security settings for user accounts

To prevent users' passwords from being guessed by a third party, Global Link Manager allows password conditions (the minimum number of characters and the combination of characters that can be used) to be specified. You can also have user accounts locked automatically if the wrong password is repeatedly entered for a specific user ID. A locked user account cannot be used for login until it has been unlocked. If a user with a locked account attempts to log in, the user is notified only of an authentication error. The user is not notified that the account is locked.

You can also use the Global Link Manager GUI to specify security settings. However, when the system is operating in a cluster environment, the settings from the Global Link Manager GUI are applied only to the primary node. To apply the settings to the secondary node, switch the nodes, and then specify the same settings. For details on how to use the Global Link Manager GUI, see the manual *Global Link Manager User Guide*.

When authenticating users by linking to an external authentication server, on the external authentication server you need to specify settings to manage passwords and control user accounts. However, when a new user is registered in a Hitachi Command Suite product, the password conditions that have been specified for the Hitachi Command Suite products are applied.

Caution

When you install Hitachi Command Suite Common Component version 5.1 or later, the user account log function and password complexity check function will be enabled. These functions are enabled for users of all Hitachi Command Suite products, so the following problems might occur in operations of Hitachi Command Suite products that are version 5.0 or earlier:

- A user is unable to log in even with a correct user ID and password.

  The user account might be locked. Take appropriate action such as unlocking the relevant account or registering a new user account.
- A password cannot be changed, or a user account cannot be added.

  The specified password might not follow the password-entry rules. Specify an appropriate password, by following the action given in the output message.

Using a user-defined file to specify security settings

This subsection describes how to use a user-defined file to specify security settings for user accounts.

Security settings using the security.conf file

The password conditions and settings related to account locking are implemented from the `security.conf` file.

The `security.conf` file is stored in the following folder:

installation-folder-for-Hitachi-Command-Suite-Common-Component\conf\sec

If you change the settings in the `security.conf` file, the new settings take effect immediately. The password conditions that you set in the `security.conf` file are applied when a user account is created or when a password is changed, and are not applied to passwords of existing user accounts. As a result, even if an existing password does not satisfy the password conditions, a user can use the password to log in to the system.

The following table lists and describes the items specified in the `security.conf` file.

Table 3-14 Items specified in the security.conf file

No.	Property name	Description
1	password.min.length	Specifies the minimum number of characters that can be set as a password. Specifiable value: 1 to 256 (characters) Default: 4
2	password.min.uppercase	Specifies the minimum number of uppercase letters the password must contain. If you specify 0, no restriction applies. Specifiable value: 0 to 256 (characters) Default: 0 (no restriction)
3	password.min.lowercase	Specifies the minimum number of lowercase letters the password must contain. If you specify 0, no restriction applies. Specifiable value: 0 to 256 (characters) Default: 0 (no restriction)
4	password.min.numeric	Specifies the minimum number of numeric characters the password must contain. If you specify 0, no restriction applies. Specifiable value: 0 to 256 (characters) Default: 0 (no restriction)
5	password.min.symbol	Specifies the minimum number of symbols the password must contain. If you specify 0, no restriction applies. Specifiable value: 0 to 256 (characters) Default: 0 (no restriction)
6	password.check.userID	Specifies whether the password can be the same as the user ID. When true is specified,

No.	Property name	Description
		passwords cannot be the same as the corresponding user ID. When `false` is specified, passwords can be the same as the corresponding user ID. Specifiable value: `true` or `false` Default: `false`
7	`account.lock.num`#1	Specifies the number of unsuccessful login attempts to allow before a user account is automatically locked. If a user makes the specified number of unsuccessful login attempts, his or her user account will be locked. If you specify `0`, any number of unsuccessful login attempts is allowed.#2 Specifiable value: 0 to 10 Default: 0

#1

This property is not available for users who are authenticated by an external authentication server.

#2

When the single sign-on feature is used

Unsuccessful login attempts by a user for other Hitachi Command Suite products are also included in the number of unsuccessful login attempts for that user. The number of unsuccessful login attempts is cleared when the user logs in successfully or when the account is locked.

How users are affected when the number of unsuccessful login attempts is changed

If you change the value for the number of unsuccessful login attempts, the new value does not apply to users who have already failed to log in more times than the new value for the number of unsuccessful login attempts or to users with a locked user account.

Security settings using the user.conf file

The built-in account (user ID: `System`) is not automatically or manually locked by default. To enable automatic or manual lock settings for the built-in account, specify the `account.lock.system` parameter in the `user.conf` file. The `user.conf` file is stored in the following location:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\conf
\user.conf
```

If there is no `user.conf` file, create it.

Specify the `account.lock.system` property as follows:

```
account.lock.system = value
```

You can specify either `true` or `false`. To enable locking of the built-in account, specify `true`; to disable locking of the built-in account, specify `false`. The default is `false`.

When `true` is specified and the login failure count for the built-in account reaches the value of the `account.lock.num` property specified in the `security.conf` file, the built-in account is locked automatically.

The following example enables locking of the built-in account:

```
account.lock.system = true
```

Perform the following procedures after you change the settings in the `user.conf` file:

- Restart Global Link Manager. Before restarting, stop the services that are running. For details about starting and stopping the service, see Starting and stopping Global Link Manager on page 3-3.
- If you are operating the management server in a cluster environment, settings specified in the `user.conf` files on both executing and standby nodes must be the same. If you change the settings in the `user.conf` file on the executing node, you must specify the same settings in the `user.conf` file on the standby node.

Unlocking accounts

You use Global Link Manager GUI to unlock user accounts. For details about how to unlock user accounts, see the manual *Global Link Manager User Guide*.

If all user accounts are locked or all user accounts with `Admin` permissions for User Management are locked, Global Link Manager GUI cannot unlock the accounts. Follow the procedure below to unlock a user account with `Admin` permissions for User Management.

To unlock a user account:

1. Make sure that Hitachi Command Suite Common Component is running. Execute the following command:

   ```
   installation-folder-for-Hitachi-Command-Suite-Common-Component
   \bin\hcmds64srv /status
   ```

   If Hitachi Command Suite Common Component is not running, start it as described in Starting Global Link Manager on page 3-3.
2. Unlock the user account with `Admin` permissions for User Management. Execute the following command:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component
\bin\hcmds64unlockaccount  /user user-ID /pass password
```

If you want to specify a backslash (\) at the end of the argument, add a backslash to each backslash specified.

The following shows an example of executing the command with a\b\c\ specified for *password*:

```
hcmds64unlockaccount /user system /pass a\b\c\\
```

The following shows an example of executing the command with a\b\c\\\ specified for *password*:

```
hcmds64unlockaccount /user system /pass a\b\c\\\\\\
```

If the argument includes ampersands (&), vertical bars (|), or carets (^), enclose each of these characters by double quotation marks ("), or insert a caret (^) just before each of these characters. The following shows an example of executing the command with &a&b&c& specified for *password*:

```
hcmds64unlockaccount /user system /pass ^&a^&b^&c^&
```

Specify the *user-ID* and *password* for the user with Admin permissions for User Management.

Note that, if no password is set for the target user, you cannot unlock the account by using the hcmds64unlockaccount command.

After you unlock the user account with Admin permissions for User Management, use this account to log into Global Link Manager GUI, then unlock the other user accounts.

Setting a warning banner

In version 5.1 or later of Hitachi Command Suite products, an optional message (warning banner) can be displayed as a security risk measure at login. Issuing a warning beforehand to third parties that might attempt invalid access can help reduce the risk of problems such as data loss or information leakage.

A message that is no more than 1,000 characters can be displayed on the Login panel. If a message with the same content is registered in a different language for each locale, the message can be automatically switched to match the locale of the Web browser.

To specify a message, you must log in as a user who has Administrator permission for the operating system.

You can also use the Global Link Manager GUI to set up a warning banner. However, when the system is operating in a cluster environment, the settings from the Global Link Manager GUI are applied only to the primary node. To

apply the settings to the secondary node, switch the nodes, and then specify the same settings. For details on how to use the Global Link Manager GUI, see the manual *Global Link Manager User Guide*.

Editing message

You edit the message in HTML format. No more than 1,000 characters can be used. In addition to the usual characters, you can use HTML tags to change font attributes or place line breaks in desired locations. (The tag characters are also counted in the number of characters.) Usable characters are from the Unicode UTF-8 encoding.

There are no restrictions on the characters you can use in the message, other than that the character encoding must be Unicode (UTF-8). To display a character used in the HTML syntax (e.g., `<`, `>`, `"`, `'`, `&`), use the HTML escape sequence. For example, to display an ampersand (&) in the Login window, write `&` in the HTML file. To insert a line break at a desired location in the message, use the HTML tag `<br>`. If there are any linefeed characters in the message, they will be ignored when the message is registered.

The following shows an example of message editing.

Example of Editing a Message:

```
<center><b>Warning Notice!</b></center>
This is a {Company Name Here} computer system, which may be accessed and used
only for authorized {Company Name Here} business by authorized personnel.
Unauthorized access or use of this computer system may subject violators to
criminal, civil, and/or administrative action. <br>
All information on this computer system may be intercepted, recorded, read,
copied, and disclosed by and to authorized personnel for official purposes,
including criminal investigations. Such information includes sensitive data
encrypted to comply with confidentiality and privacy requirements. Access or
use of this computer system by any person, whether authorized or unauthorized,
constitutes consent to these terms. There is no right of privacy in this
system.
```

Caution

When the message is registered, the HTML syntax is neither checked nor corrected. Edit the message correctly in accordance with HTML syntax rules because the edited message will be registered as is. If there is an error in the HTML syntax in the message, the message might not be displayed correctly in the Login panel.

Note

Sample messages in English (`bannermsg.txt`) and Japanese (`bannermsg_ja.txt`) are provided in the following locations:

installation-folder-for-Hitachi-Command-Suite-Common-Component`\sample\resource`

These sample files are overwritten at installation so, if you wish to use a sample file, copy it and then edit it.

Registering message

To register an edited message, execute the following command:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64banner /add /file file-name [/locale locale-name]
```

The following shows an example of executing the command:

```
"C:\Program Files\HiCommand\Base64\bin\hcmds64banner" /add /file C:
\W_Banner\wbfile1 /locale en
```

If you execute the command without specifying `/locale` *locale-name*, you can also use the Global Link Manager GUI to edit the registered contents. However, if you use the Global Link Manager GUI to edit the contents, the HTML tags that can be used are limited.

If you operate the Global Link Manager client under multiple locales, you can also specify, for *locale-name*, the locale of the language used for the messages (e.g., `en` for English, or `ja` for Japanese).

The locale for a warning banner displayed in the Global Link Manager GUI is set according to the priority of the language set for the Web browser on the Global Link Manager client.

Caution

If a message for the specified locale is already registered, it will be updated by being overwritten.

Deleting message

To delete an edited message, execute the following command:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64banner /delete [/locale locale-name]
```

The following shows an example of executing the command:

```
"C:\Program Files\HiCommand\Base64\bin\hcmds64banner" /delete /
locale en
```

For *locale-name*, specify the locale for the message you want to delete (e.g., `en` for English, or `ja` for Japanese). If you do not specify a locale, the default locale will be assumed.

Generating audit logs

You can generate audit logs for Global Link Manager and other Hitachi storage-related products to prove to auditors and evaluators the compliance with regulations, security evaluation standards, and other business standards. The following table lists and describes the audit logs that you can generate from Hitachi storage-related products.

Table 3-15 Types of audit logs

Log type	Description
`StartStop`	Events indicating starting or stopping of hardware or software: • Starting or stopping an OS

Log type	Description
	• Starting or stopping a hardware component (including a microprogram) • Starting or stopping software on a storage system or SVP, and Hitachi Command Suite products
`Failure`	Events indicating a hardware or software error: • Hardware error • Software error (such as a memory error)
`LinkStatus`	Events indicating the status of a link between devices: • Whether a link is up or down
`ExternalService`	Events indicating the results of communication between a Hitachi storage-related product and an external service: • Communication with a RADIUS server, LDAP server, NTP server, or DNS server • Communication with a management server (SNMP)
`Authentication`	Events indicating that a device, administrator, or end user attempted connection or authentication and whether the attempt was successful: • FC login • Device authentication (FC-SP authentication, iSCSI login authentication, or SSL server/client authentication) • Administrator or end user authentication
`AccessControl`	Events indicating that a device, administrator, or end user attempted to access resources and whether the attempt was successful: • Access control for devices • Access control for the administrator or end users
`ContentAccess`	Events indicating that an attempt was made to access important data and whether the access was successful: • Access to an important file on NAS or to content when HTTP is supported • Access to an audit log file
`ConfigurationAccess`	Events indicating that an administrator performed a permitted operation and whether the operation terminated normally or failed: • Referencing or updating configuration information • Updating account settings, including addition and deletion of accounts • Setting security • Referencing or updating the audit log settings
`Maintenance`	Events indicating that a maintenance operation was performed and whether the operation terminated normally or failed: • Adding or removing a hardware component • Adding or removing a software component

Log type	Description
AnomalyEvent	Events indicating that an error, such as an exceeded threshold, occurred: • The network traffic threshold was exceeded. • The CPU load threshold was exceeded. • Notification that the amount of temporarily saved audit log data is approaching the maximum or a wraparound
	Events indicating a communication error: • A SYN flooding attack against ports in normal use or a protocol violation • Attempted access of unused ports (such as port scans)

The audit logs that can be generated depend on the products. The following section describes the types of audit logs and the audit events that can be generated from Global Link Manager. For details on the audit logs of other products, see the documentation for those products.

Categories of information output to audit logs in Global Link Manager, and audit events

This section describes the categories of information output to audit logs in Global Link Manager and the audit events included in these categories. These categories include the following:

- StartStop
- Authentication
- ConfigurationAccess

A severity level is set for each audit event.

The following table lists the audit events for each category.

Table 3-16 StartStop audit events

Description	Audit event	Severity	Message ID
Starting and stopping software	The SSO server was started successfully.	6	KAPM00090-I
	The SSO server could not be started.	3	KAPM00091-E
	The SSO server stopped.	6	KAPM00092-I

Table 3-17 Authentication audit events

Description	Audit event	Severity	Message ID
Administrator or end user authentication	Login succeeded.	6	KAPM01124-I
	Successful login (to the external authentication server).	6	KAPM02450-I
	Login failed (the specified user ID or password is invalid).	4	KAPM02291-W
	Login failed (login was attempted by a locked user).	4	KAPM02291-W
	Login failed (login was attempted by a nonexistent user).	4	KAPM02291-W
	Login failed (no permissions).	4	KAPM01095-E
	Login failed (authentication failed).	4	KAPM01125-E
	Failed login (to the external authentication server).	4	KAPM02451-W
	Logout succeeded.	6	KAPM08009-I
	Logout failed.	4	KAPM01126-W
Automatic locking of an account	Account was locked automatically (successive authentication attempts failed, or the account has expired).	4	KAPM02292-W

Table 3-18 Configuration Access audit events

Description	Audit event	Severity	Message ID
User registration (GUI)	User registration succeeded.	6	KAPM07230-I
	User registration failed.	3	KAPM07240-E
User registration (GUI and CLI)	User registration succeeded.	6	KAPM07241-I
	User registration failed.	3	KAPM07242-E
User deletion (GUI)	User deletion succeeded.	6	KAPM07231-I
	User deletion failed.	3	KAPM07240-E
User deletion (GUI and CLI)	User deletion succeeded.	6	KAPM07245-I
	User deletion failed.	3	KAPM07246-E
User information update (GUI and CLI)	Successful user information update.	6	KAPM07243-I
	Failed user information update.	3	KAPM07244-E
Changing the password (from the administrator window)	The administrator changed the password successfully.	6	KAPM07232-I
	The administrator could not change the password.	3	KAPM07240-E

Description	Audit event	Severity	Message ID
Changing the password (from a local user window)	Authentication to determine whether the old password is correct failed.	3	KAPM07239-E
	The password of the login user was changed successfully from the local user window.	6	KAPM07232-I
	The password of the login user could not be changed from the local user window.	3	KAPM07240-E
Changing a profile	The profile was changed successfully.	6	KAPM07233-I
	The profile could not be changed.	3	KAPM07240-E
Changing permissions	Permissions were changed successfully.	6	KAPM02280-I
	Permissions could not be changed.	3	KAPM07240-E
Locking an account	The account was locked successfully.#1	6	KAPM07235-I
	The account could not be locked.	3	KAPM07240-E
Unlocking an account	The account was unlocked successfully.#2	6	KAPM07236-I
	The account could not be unlocked.	3	KAPM07240-E
Authentication method change	Successful authentication method change.	6	KAPM02452-I
	Failed authentication method change.	3	KAPM02453-E
Backing up or restoring the database.	Backup by the hcmds64backups command succeeded.	6	KAPM05561-I
	Backup by the hcmds64backups command failed.	3	KAPM05562-E
	Full restoration by the hcmds64db command succeeded.	6	KAPM05563-I
	Full restoration by the hcmds64db command failed.	3	KAPM05564-E
	Partial restoration by the hcmds64db command succeeded.	6	KAPM05565-I
	Partial restoration by the hcmds64db command failed.	3	KAPM05566-E
Input and output of data on the database	Data output by the hcmdsdbmove command succeeded.	6	KAPM06543-I
	Data output by the hcmdsdbmove command failed.	3	KAPM06544-E

Description	Audit event	Severity	Message ID
	Data input by the hcmdsdbmove command succeeded.	6	KAPM06545-I
	Data input by the hcmdsdbmove command failed.	3	KAPM06546-E
Input and output of authentication data	Data output by the hcmds64authmove command succeeded.	6	KAPM05832-I
	Data output by the hcmds64authmove command failed.	3	KAPM05833-E
	Data input by the hcmds64authmove command succeeded.	6	KAPM05834-I
	Data input by the hcmds64authmove command failed.	3	KAPM05835-E
Placing paths online or offline	A request to place paths online or offline was received successfully.	6	KAIF50200-I
	A request to place paths online or offline could not be received.	3	KAIF50201-E
	All paths were successfully placed online or offline.	6	KAIF50202-I
	Some paths could not be placed online or offline.	4	KAIF50203-W
	No paths could be placed online or offline.	3	KAIF50204-E
Setting up a multipath LU	The multipath LU setting was received successfully.	6	KAIF50200-I
	The multipath LU setting could not be received.	3	KAIF50201-E
	The multipath LU was set up successfully.	6	KAIF50202-I
	Part of the multipath LU was not set up successfully.	4	KAIF50203-W
	The multipath LU could not be set up.	3	KAIF50204-E
Setting up HDLM	The HDLM setting was received successfully.	6	KAIF50200-I
	The HDLM setting could not be received.	3	KAIF50201-E
	HDLM was set up successfully.	6	KAIF50202-I
	HDLM setup partially failed.	4	KAIF50203-W
	HDLM could not be set up.	3	KAIF50204-E

Description	Audit event	Severity	Message ID
Setting up alerts	Alert settings were received successfully.	6	KAIF50200-I
	Alert settings could not be received.	3	KAIF50201-E
	The alerts were set up successfully.	6	KAIF50202-I
	Some alerts could not be set up.	4	KAIF50203-W
	The alerts could not be set up.	3	KAIF50204-E
Resetting the number of path I/O counts and the number of I/O errors	A request to reset the number of path I/O counts and the number of I/O errors was received successfully.	6	KAIF50200-I
	A request to reset the number of path I/O counts and the number of I/O errors could not be received.	3	KAIF50201-E
	The number of path I/O counts and the number of I/O errors were reset successfully.	6	KAIF50202-I
	Resetting of the number of path I/O counts and the number of I/O errors was only partially successful.	4	KAIF50203-W
	The number of path I/O counts and the number of I/O errors could not be reset.	3	KAIF50204-E

#1

If an account is locked because the authentication method was changed for a user whose password is not set, this information is not recorded in the audit log.

#2

If an account is unlocked because a password was set for a user, this information is not recorded in the audit log.

Editing the environment settings file for audit logs

To generate Global Link Manager audit logs, you must edit the environment settings file (`auditlog.conf`). Once the categories of the audit events for which a log is to be generated are specified for `Log.Event.Category` in the environment settings file, audit logs can be generated. Audit logs are output to the Windows event log file. For details on the event log format, see Output format of the event log files on page 7-11.

Note

Collecting an audit log causes a huge amount of event data to be output. Make sure that you change the size of the event log file, and save and archive the generated log files.

The location of the `auditlog.conf` file is as follows:

Hitachi-Command-Suite-Common-Component-installation-folder\conf\sec

The following table lists and describes the items specified in the `auditlog.conf` file.

Table 3-19 Items specified in the auditlog.conf file

Item	Description
`Log.Facility`	This item is not used, and is ignored if specified.
`Log.Event.Category`	Specifies the category of the audit events for which a log is to be generated. To specify multiple categories, use a comma (,) to separate each category. Do not enter a space between a comma and the category. By default, the category is not specified, so if you fail to specify it, the audit log is not output. For details on the types you can specify, see Categories of information output to audit logs in Global Link Manager, and audit events on page 3-76.
`Log.Level`	Specifies the severity of the audit events for which a log is to be generated. Information whose severity is the specified value or lower will be output. For details on the audit events output in Global Link Manager, see Categories of information output to audit logs in Global Link Manager, and audit events on page 3-76. For details on the correspondence between the severity levels of audit events and the types of event log data, see Table 3-20 Correspondence between the severity levels of audit events and the types of event log data on page 3-81 . The following shows how the event log types correspond to the audit event severity. For example, if you want to output error and warning information, specify `4`. • Error: `3` • Warning: `4` • Information: `6` Specifiable value: `0` to `7` (Severity) Default: `6`

The table below shows the correspondence between the severity levels of audit events and the types of event log data.

Table 3-20 Correspondence between the severity levels of audit events and the types of event log data

Severity of audit events	Type of event log data
0	Error
1	
2	
3	
4	Warning

Severity of audit events	Type of event log data
5	Information
6	
7	

The following shows an example of the `auditlog.conf` file:

```
# Specify an integer for Facility. (specifiable range: 1-23)
Log.Facility 1

# Specify the event category.
# You can specify any of the following:
# StartStop, Failure, LinkStatus, ExternalService,
# Authentication, AccessControl, ContentAccess,
# ConfigurationAccess, Maintenance, or AnomalyEvent.
Log.Event.Category Authentication,ConfigurationAccess

# Specify an integer for Severity. (specifiable range: 0-7)
Log.Level 6
```

In this example, audit logs for the audit events in the `Authentication` or `ConfigurationAccess` category whose type is error, warning, or information will be output.

Output format of the audit log files

Audit logs are output to the Windows event log file. This section shows the format of entries and describes the elements in an entry.

Event output format:

date time type user computer source category event-ID explanation

Table 3-21 Information output to the windows event log (audit log)

Item	Description
date	The date this entry was logged is output here in `yyyy/mm/dd` format.
time	The time this entry was logged is output here in `hh:mm` format.
type	One of the following strings is output here to indicate the type of message: • Information • Warning • Error
user	`N/A` is always output here.
computer	The computer name is output here.
source	`HBase64 Event` is always output here.

Item	Description
category	`None` is always output here.
event-ID	`1` is always output here.
explanation	A message in the audit log beginning with *program-name* [*process-ID*]: `CELFSS` For details on what is displayed, see Output format of "explanation" on page 3-83 below, and Table 3-22 Information output to "explanation" in the audit log on page 3-83 .

Output format of "explanation"

program-name [*process-ID*]: *uniform-identifier*, *unified-specification-revision-number*, *serial-number*, *message-ID*, *date-and-time*, *detected-entity*, *detected-location*, *audit-event-type*, *audit-event-result*, *audit-event-result-subject-identification-information*, *hardware-identification-information*, *location-information*, *location-identification-information*, *FQDN*, *redundancy-identification-information*, *agent-information*, *request-source-host*, *request-source-port-number*, *request-destination-host*, *request-destination-port-number*, *batch-operation-identifier*, *log-type-information*, *application-identification-information*, *reserved-area*, *message-text*

Table 3-22 Information output to "explanation" in the audit log

Item#1	Output information
program-name	The component name or process name is output.
process-ID	The process ID is output.
uniform-identifier	`CELFSS` is output.
unified-specification-revision-number	`1.1` is output.
serial-number	The serial number of the message in the audit log is output.
message-ID#2	The message ID is output.
date-and-time	The date and time that the message was logged is output in the format `yyyy-mm-ddThh:mm:ss.s`*time-zone*.
detected-entity	The component name or process name is output.
detected-location	The host name is output.
audit-event-type	The event type is output.
audit-event-result	The result of the event is output.
audit-event-result-subject-identification-information	Depending on the event, the account ID, process ID, or IP address is output.
hardware-identification-information	The model name and product number of hardware is output.

Item#1	Output information
location-information	The identification information of the hardware component is output.
location-identification-information	The location identification information is output.
FQDN	The fully qualified domain name is output.
redundancy-identification-information	The redundancy identification information is output.
agent-information	The agent information is output.
request-source-host	The host name of the server that sent a processing request is output.
request-source-port-number	The port number of the server that sent a processing request is output.
request-destination-host	The host name of the server that received a processing request is output.
request-destination-port-number	The port number of the server that received a processing request is output.
batch-operation-identifier	The serial number of the operation in the program is output.
log-type-information	`BasicLog` is output.
application-identification-information	The identification information for the program is output.
reserved-area	This is a reserved area. No information is output.
message-text#2	The output information depends on the audit event. The `Command ID` contained in *message-text* is used to identify a single operation performed from the Global Link Manager GUI. If multiple messages contain the same command ID, this means that those messages were output for a single operation.

#1: Some items might not be output, depending on the audit event.

#2: For details on the message IDs corresponding to audit events, see Categories of information output to audit logs in Global Link Manager, and audit events on page 3-76. For details on the message text for each message ID, see the *Global Link Manager Messages*.

Example of an audit event for login

```
CELFSS,1.1,0,KAPM01124-I,2014-07-22T14:08:23.1+09:00,HBase-SSO,management-
host,Authentication,Success,uid=hoge,,,,,,,,,,,,BasicLog,,,"The login was
successful. (session ID =session ID)"
```

Setting up alert transfer

Alert information can be transferred from the Global Link Manager server to the SNMP transfer destination server. You can use any application to manage the alert information.

When transferring alerts, you can convert the alert information received from Global Link Manager into characters by registering Global Link Manager MIB files on the SNMP transfer destination server.

The MIB file to be registered (`hglam.mib`) is stored in the following folder:
Global-Link-Manager-installation-DVD-ROM-drive:\HGLM\mib

Use the property file (`server.properties`) to specify whether to enable alert transfer and to specify the SNMP transfer destination server. For details on how to set up the property file, see Changing Global Link Manager environment settings on page 3-33.

Settings required to authenticate users by using an external authentication server

Hitachi Command Suite products can authenticate users by linking to an external authentication server. If you register the user IDs that are registered on the external authentication server into Hitachi Command Suite products, you can use those user IDs to log in to Hitachi Command Suite products. This saves you from having to managing login passwords and controlling accounts in Hitachi Command Suite products.

In addition, if you use both an external authentication server and an external authorization server, you can control users' access permissions for Hitachi Command Suite products by using the external authorization server. When an external authorization server is also linked to, you do not need to manage accounts and set permissions for individual users because Hitachi Command Suite products manage users by using the `authorization groups` external authorization server.

Settings required to link to an external authentication server or an external authorization server depend on the authentication method used in the external authentication server. Settings required for each authentication method are described in the sections below.

Note

If command line control characters are included in the arguments of commands that will be executed when specifying the settings to link to an external authentication server, escape the characters correctly according to the specifications of the command line. Also, you need to pay attention to backslashes (\) included in the arguments because they are treated specially in the command line.

If the following characters are included in an argument, enclose the argument in double quotation marks (") or use a caret (^) to escape each character:

Spaces & | ^ < > ( )

A backslash might be treated as an escape character depending on the character that follows it. Therefore, if a backslash and any of the above characters are included in an argument, use a caret to escape each character rather than enclose the argument in double quotation marks.

Also, if there is a backslash at the end of an argument, escape it by using another backslash.

For example, if a shared secret to be registered by the `hcmds64radiussecret` command is `secret01\`, escape it as follows:

```
hcmds64radiussecret /set secret01\\ /name ServerName
```

Configurations when multiple external authentication servers are linked

When multiple external authentication servers are linked, user authentication is performed in a redundant configuration or a multi-domain configuration.

A redundant configuration is used when each external authentication server manages the same user information. If a failure occurs on one external authentication server, user authentication can be performed by using another external authentication server.

A multi-domain configuration is used when each external authentication server manages different user information. If a user logs in with a user ID that includes a domain name, the user will be authenticated by an external authentication server in the domain whose name is included in the user ID. When a Kerberos server is used as an external authentication server, you can create a configuration similar to a multi-domain configuration by managing different user information for each realm.

The following table shows external authentication servers for which redundant configurations and multi-domain configurations are supported.

Table 3-23 Support status for redundant configurations and multi-domain configurations

External authentication server	Redundant configuration	Multi-domain configuration
LDAP directory server	Y#1	Y#1
RADIUS server	Y	N
Kerberos server	Y	Y#2

Legend:

Y: Supported

N: Not supported

#1

You can use either a redundant configuration or a multi-domain configuration.

If the global catalog for Active Directory is set, you can use both a redundant configuration and a multi-domain configuration.

#2

By managing different user information for each realm, you can create a configuration that is similar to a multi-domain configuration.

When an LDAP directory server is used for user authentication in a multi-domain configuration, the user authentication process varies depending on whether you log in with a user ID that includes a domain name. If you log in with a user ID that includes a domain name, as in the following figure, user authentication will be performed by using the LDAP directory server of the specified domain.

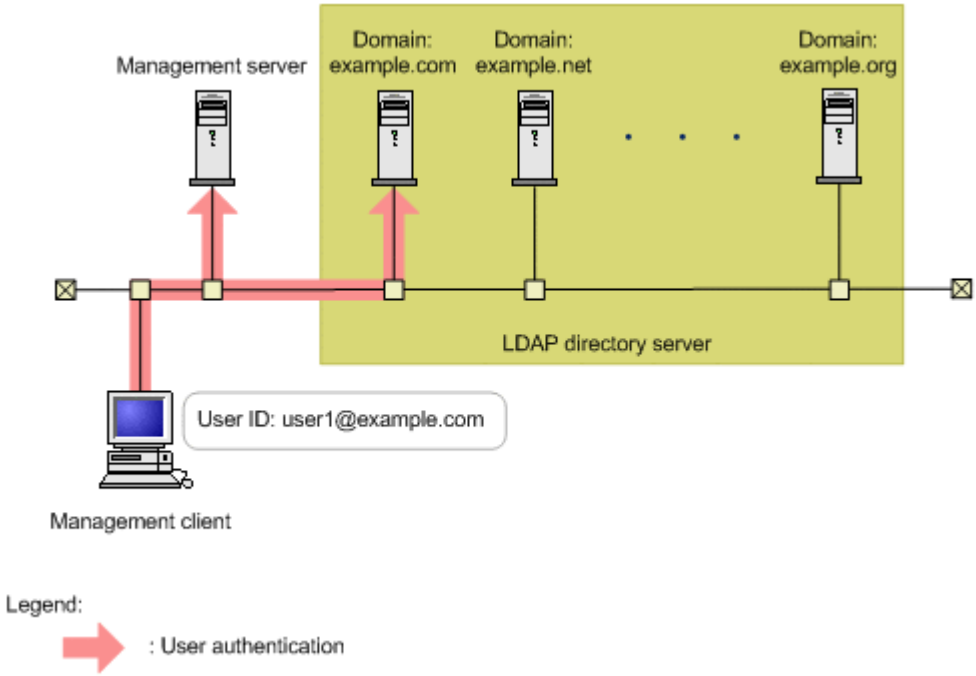

Figure 3-1 User authentication in a multi-domain configuration (when using a user ID that includes a domain name)

If you log in with a user ID that does not include a domain name, user authentication will be performed sequentially on all LDAP directory servers that are linked, as shown in the figure below. If a large number of LDAP directory servers are linked, user authentication will take a long time. For this reason, we recommend that you log in with a user ID that includes a domain name.

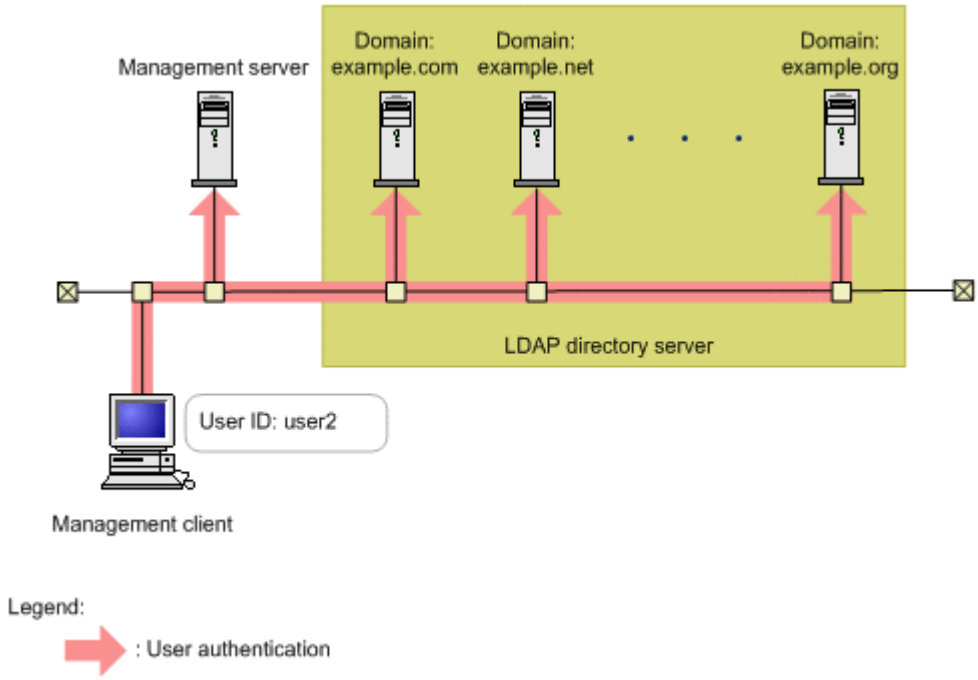

Figure 3-2 User authentication in a multi-domain configuration (when using a user ID that does not include a domain name)

Settings required when using an LDAP directory server for authentication

To authenticate users by using an LDAP directory server, specify the following settings in Hitachi Command Suite products.

1. Check the data structure of the LDAP directory server to determine the method for linking with Hitachi Command Suite products and for authentication.
2. In the `exauth.properties` file on the management server, specify necessary information.

   Necessary settings depend on whether only an external authentication server is linked to or an external authorization server is also linked to.

   You can use either of the following methods to define the LDAP directory server:

   - In the `exauth.properties` file, directly specify information about the LDAP directory server to connect to.

     Specify information such as IP address and port number in the `exauth.properties` file for each LDAP directory server.
   - Use the DNS server to look up the LDAP directory server to connect to.

     Before using this method, you need to set up the DNS server environment on the OS of the LDAP directory server. In addition, you need to register the host name, port number, and domain name of the LDAP directory server in the SRV records of the DNS server.

Note

To use StartTLS for communication between the management server and the LDAP directory server, you need to directly specify information about the LDAP directory server to connect to in the `exauth.properties` file.

If you use the DNS server to look up the LDAP directory server to connect to, it might take longer for users to log in.

If the LDAP directory server to which you want to connect is in a multidomain configuration, you will not be able to look up the LDAP directory server by using the DNS server.

3. In the following cases, on the management server, register a user account used to search for user information on the LDAP directory server.
   - When the data structure is the hierarchical structure model
   - When the data structure is the flat model and an external authorization server is also linked to#

   #:

   When registering an authorization group in Hitachi Command Suite products by using Global Link Manager GUI (For details on the procedure, see step 5), if you want to check whether the distinguished name of the authorization group is registered on the external authorization server by using a user ID such as the `System` account registered in Hitachi Command Suite products, you need to register a user account used to search for LDAP user information on the management server.

4. On the LDAP directory server, register the accounts of users that will use Hitachi Command Suite products.

   User IDs and passwords must consist of characters that can be used in Hitachi Command Suite products. Specify 1 to 256 bytes of the following characters:

   `0 to 9 A to Z a to z ! # $ % & ' ( ) * + - . = @ \ ^ _ |`

   In Hitachi Command Suite products, user IDs are not case-sensitive. The combination of character types for passwords must follow the settings in the external authentication server.

5. Register accounts and set permissions by using Global Link Manager GUI.

   When linking to only an external authentication server

   Register users.

   Change the authentication method of users.#

   Set permissions for users.

   Assign resource groups to users.

   #: This operation is required if you want to change the authentication method of existing users.

   When also linking to an external authorization server

   Register authorization groups.

   Set permissions for authorization groups.

You do not need to assign resource groups to authorization groups. `All Resources` will be automatically assigned to users who belong to authorization groups.

6. Use the `hcmds64checkauth` command to make sure that the external authentication server and the external authorization server can be properly connected to.

The following sections describe operations you need to perform on the management server. For details on how to use Global Link Manager GUI, see the manual *Global Link Manager User Guide*.

Checking the data structure and authentication method

The LDAP directory server has the following two data structure models.

- Hierarchical structure model
- Flat model

You must first determine which data structure model is being used, because the information you need to set in the `exauth.properties` file and the operations you need to perform on the management server depend on the data structure.

In addition, check BaseDN, which is the entry that will be the start point for searching for LDAP user information during authentication. BaseDN must be specified in the `exauth.properties` file. Only the user entries that are in the hierarchy below BaseDN can be authenticated. Make sure that all users you want to authenticate for Hitachi Command Suite products are in this hierarchy.

Hierarchical structure model

A data structure in which the hierarchies below BaseDN branch off and in which user entries are registered in another hierarchy. If the hierarchical structure model is used, the entries in the hierarchy below BaseDN are searched for an entry that has the same login ID and user attribute value.

The following figure shows an example of the hierarchical structure model. The user entries enclosed by the dotted line can be authenticated. In this example, BaseDN is `cn=group,dc=example,dc=com`, because the target user entries extend across two departments (`cn=sales` and `cn=development`).

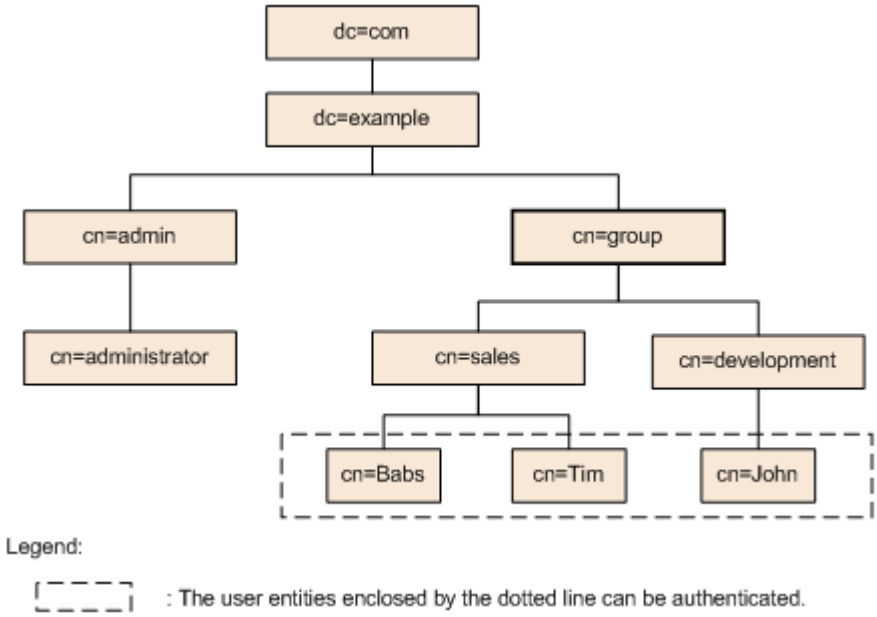

Figure 3-3 Example of the hierarchical structure model

Flat model

A data structure in which there are no branches in the hierarchy below BaseDN and in which user entries are registered in the hierarchy located just below BaseDN. If the flat model is used, the entries in the hierarchy below BaseDN are searched for an entry that has the DN that consists of a combination of the login ID and BaseDN. If such a value is found, the user is authenticated.

The following figure shows an example of the flat model. The user entities enclosed by the dotted line can be authenticated. In this example, BaseDN is `ou=people,dc=example,dc=com`, because all of the user entries are located just below `ou=people`.

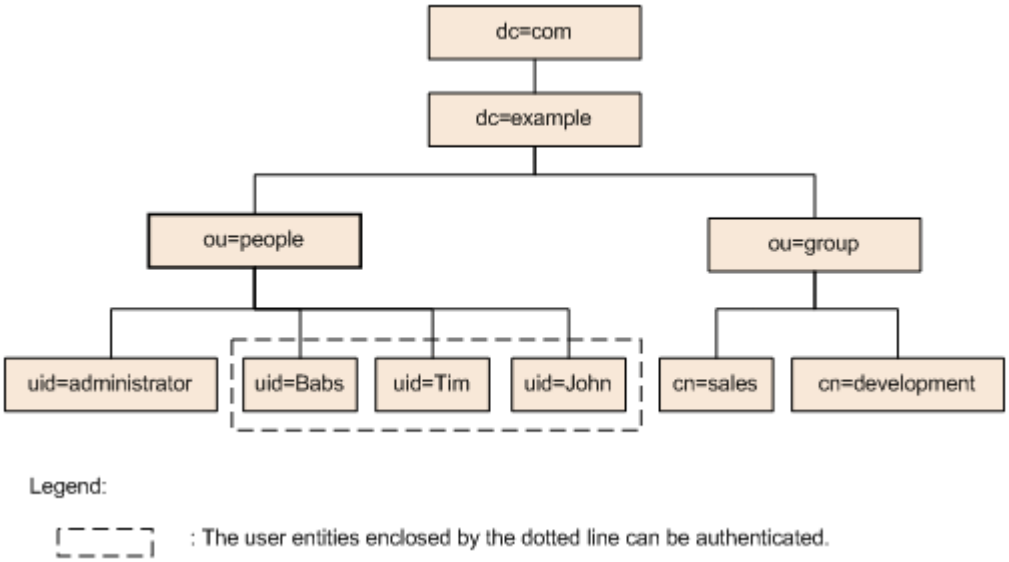

Figure 3-4 Example of the flat model

Note, however, that even if the flat model is being used, if either of the following conditions is satisfied, specify the settings by following the explanation for the hierarchical structure model:

- If a user attribute value other than the RDN attribute value is used as the user ID of a Hitachi Command Suite product:

  If a user attribute value other than the RDN attribute value (for example, the Windows logon ID) of a user entry is used as the user ID of a Hitachi Command Suite product, you must use the authentication method for the hierarchical structure model.
- If the RDN attribute value of a user entry includes an invalid character that cannot be used in a user ID for a Hitachi Command Suite product:

  When using the authentication method for the flat model, the RDN attribute value of a user entry functions as the user ID for Hitachi Command Suite products. Therefore, if the RDN attribute value of a user entry includes an invalid character that cannot be used in a user ID of the Hitachi Command Suite product, you cannot use the authentication method for the flat model.

  - Example of a valid RDN:

    `uid=John123S`

    `cn=John_Smith`
  - Example of an invalid RDN:

    `uid=John:123S` (A colon (`:`) is used.)

    `cn=John Smith` (A space is used between `John` and `Smith`.)

Setting the exauth.properties file (when the authentication method is LDAP)

This section describes the settings required for the `exauth.properties` file in order to use an LDAP directory server to authenticate users.

1. Specify values for the following properties in the `exauth.properties` file:

- Common properties (Table 3-24 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (common items) on page 3-93)
- Properties for an external authentication server and an external authorization server

  Specify these property values for each LDAP directory server.

  The items you need to specify differ depending on whether you directly specify information about the LDAP directory server (Table 3-25 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (when directly specifying information about the external authentication server) on page 3-94) or you use the DNS server to look up the LDAP directory server (Table 3-26 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (when using the DNS server to look up information about the external authentication server) on page 3-97).

The template of the `exauth.properties` file is stored in the following location:

installation-folder-for-Hitachi-Command-Suite-Common-Component
`\sample\conf\exauth.properties`

Note

Do not enter a space at the beginning or end of a setting value. Also, do not enclose a setting value in double quotation marks (`"`). If you do, the value is ignored, and the default value is used instead.

2. Save the `exauth.properties` file in the following location:

   installation-folder-for-Hitachi-Command-Suite-Common-Component
   `\conf\exauth.properties`

   Table 3-24 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (common items) on page 3-93 through Table 3-26 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (when using the DNS server to look up information about the external authentication server) on page 3-97 describe the items to specify in the `exauth.properties` file.

The following table describes the properties for linking to an external authentication server.

Table 3-24 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (common items)

Property names	Details
`auth.server.type`	Specify an external authentication server type. Specify `ldap`. Default value: `internal` (used when not linking to an external authentication server)

Property names	Details
auth.server.name	Specify the server identification names of LDAP directory servers. You can specify any name for this property in order to identify which LDAP directory servers the settings such as the port number and the protocol for connecting to the LDAP directory server (see Table 3-25 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (when directly specifying information about the external authentication server) on page 3-94 or Table 3-26 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (when using the DNS server to look up information about the external authentication server) on page 3-97) are applied to. ServerName has been set as the initial value. You must specify at least one name. To specify multiple server identification names, delimit the server identification names by using commas (,). Do not register the same server identification name more than once. Specifiable values: No more than 64 bytes of the following characters: 0 to 9 A to Z a to z ! # ( ) + - . = @ [ ] ^ _ { } ~ Default value: none
auth.ldap.multi_domain	When specifying multiple server identification names for LDAP directory servers, specify, for each server, the configuration to be used. Specify true to use a multi-domain configuration. Specify false to use a redundant configuration. Default value: false
auth.ldap.default_domain	Specify settings for the Active Directory global catalog. Specify the domain name of the default server configuration to be used for authentication when no domain name is specified in the login ID. If you specify multiple servers in auth.server.name, a multi-domain configuration will be used, and a redundant configuration will not be used. Default value: none
auth.group.mapping	Specify whether to also link to an external authorization server. Specify true to link to an external authorization server. Specify false to not to link to an external authorization server. Default value: false

Table 3-25 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (when directly specifying information about the external authentication server)

Attributes	Details
protocol#1	Specify the protocol for connecting to the LDAP directory server. This attribute is required. When communicating in plain text format, specify ldap. When using StartTLS communication, specify tls.

Attributes	Details
	Before specifying `tls`, make sure that one of the following encryption methods can be used on the LDAP directory server. • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256 Specifiable values: `ldap` or `tls` Default value: none
`host`#2	Specify the host name or IP address of the LDAP directory server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets (`[]`). To use a redundant configuration when the global catalog is enabled (`auth.ldap.default_domain` is specified), specify multiple host names or IP addresses, delimited by commas. This attribute is required. Default value: none
`port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. To use a redundant configuration when the global catalog is enabled (`auth.ldap.default_domain` is specified), specify multiple port numbers, delimited by commas. Make sure that the number of ports is the same as the number of host names or IP addresses specified in `host`. Specifiable values: 1 to 65535 Default value: 389 (when the global catalog is disabled), 3268 (when the global catalog is enabled)
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
`attr`	Specify the attribute name (Attribute Type) which has been defined for the user ID to be used during authentication. • For the hierarchical structure model Specify the name of the attribute containing the unique value to be used for identifying the user. The value stored in this attribute is used as the user ID of the Hitachi Command Suite product.#3 For example, if you are using Active Directory and you want to use a Windows logon ID as a user ID of the Hitachi Command

Attributes	Details
	Suite product, specify the attribute name `sAMAccountName` in which the Windows logon ID has been defined. • For the flat model Specify the RDN attribute name of the user entry. For example, if the user's DN is `uid=John,ou=People,dc=example,dc=com`, specify the `uid` that is the attribute name of the RDN `uid=John`. `sAMAccountName` has been set as the initial value. This attribute is required. Default value: none
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authentication. If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. • For the hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries to be searched. For example, for Figure 3-1, specify `cn=group,dc=example,dc=com`. • For the flat model Specify the DN of the hierarchy just above the user entries to be searched. For example, for Figure 3-2, specify `ou=people,dc=example,dc=com`. This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (`\`) to escape each character. Spaces `# + ; , < = > \` Default value: none
`retry.interval`	Specify the retry interval in seconds for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify `0`, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
`domain.name`	Specify the name of a domain for external authentication servers managed by the LDAP directory server. This item is required when an external authorization server is also linked to. Default value: none

Attributes	Details
domain	Specify the name of a domain for multi-domain configurations managed by the LDAP directory server, or the domain name for the global catalog. If you log in by using a user ID that includes the domain name specified in this attribute, the LDAP directory server that belongs to the specified domain will be used as the authentication server. When specifying a domain name for the server identification name of each LDAP directory server, do not specify the same domain name more than once. This value is not case sensitive. If the global catalog is enabled, be sure to specify the domain name that is specified in auth.ldap.default_domain as the default server configuration to be used for authentication. This item is required when a multi-domain configuration is used. Default value: none
dns_lookup	Specify false. Default value: false

Note

To specify the attributes, use the following syntax:

auth.ldap.*auth.server.name-property-value*.*attribute*=*value*

#1

When using StartTLS communication as the protocol for connecting to the LDAP directory server, you need to specify the security settings of Hitachi Command Suite Common Component. For details about specifying security settings for StartTLS communication, see Security settings for communication between a server and an LDAP directory server on page 5-13.

#2

When using StartTLS as the protocol for connecting to the LDAP directory server, in the host attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.

#3

The specified attribute must not include invalid characters that cannot be used in a user ID of the Hitachi Command Suite product.

Table 3-26 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (when using the DNS server to look up information about the external authentication server)

Attributes	Details
protocol	Specify the protocol for connecting to the LDAP directory server. This attribute is required. Specifiable values: ldap Default value: none

Attributes	Details
port	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
timeout	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
attr	Specify the attribute (Attribute Type) to use as the user ID during authentication. • For the hierarchical structure model Specify the name of the attribute containing the unique value to be used for identifying the user. The value stored in this attribute will be used as the user ID for Hitachi Command Suite products.# For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of a Hitachi Command Suite product, specify the attribute name sAMAccountName in which the Windows logon ID has been defined. • For the flat model Specify the RDN attribute name of the user entry. For example, if the user's DN is uid=John,ou=People,dc=example,dc=com, specify the uid that is the attribute name of the RDN uid=John. sAMAccountName has been set as the initial value. This attribute is required. Default value: none
basedn	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authentication. If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. • For the hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries to be searched. For example, for Figure 3-1, specify cn=group,dc=example,dc=com. • For the flat model Specify the DN of the hierarchy just above the user entries to be searched.

Attributes	Details
	For example, for Figure 3-2, specify `ou=people,dc=example,dc=com`. This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (`\`) to escape each character. Spaces `# + ; , < = > \` Default value: none
`retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
`domain.name`	Specify the domain for external authentication servers name managed by the LDAP directory server. Default value: none
`dns_lookup`	Specify `true`. However, if the following attribute values are already set, the LDAP directory server will be connected to by using the user-specified values instead of by using the DNS server to look up the information. • `auth.ldap.auth.server.`*name-property-value*`.host` • `auth.ldap.auth.server.`*name-property-value*`.port` Default value: `false`

Note

To specify the attributes, use the following syntax:

`auth.ldap.auth.server.`*name-property-value*`.attribute=value`

#:

The specified attribute must not include invalid characters that cannot be used in a user ID of the Hitachi Command Suite product.

The following examples show how to specify the properties:

- When directly specifying information about an LDAP directory server (when linking to only an external authentication server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
```

```
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.dns_lookup=false
```

- When Using the DNS server to look up an LDAP directory server (when linking to only an external authentication server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- When directly specifying about the LDAP directory server (when also linking to an authorization server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=false
```

- When using the DNS server to look up the LDAP directory server (when also linking to an authorization server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- When using a redundant configuration

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=false
auth.group.mapping=false
```

```
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
```

- When using a multi-domain configuration

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=true
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName1.domain=example.com
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
auth.ldap.ServerName2.domain=example.net
```

- When the global catalog is enabled

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.default_domain=example.com
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap.example1.com,ldap.example2.com
auth.ldap.ServerName1.port=3268,3268
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName1.domain=example.com
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap.example1.com,ldap.example2.com
auth.ldap.ServerName2.port=3268,3268
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
auth.ldap.ServerName2.domain=example.net
```

Registering a user account used to search for LDAP user information (when the authentication method is LDAP)

By using the `hcmds64ldapuser` command, you can register, on the management server, a user account used to search for LDAP user information. After registering a user account, you can use this command to delete such an account or check LDAP directory servers for which user accounts used to search for LDAP user information have been registered on the management server.

This step is necessary in the following cases:

- When the data structure is the hierarchical model
- When the data structure is the flat model and an external authorization server is also linked to#

  #:

  When registering an authorization group in Hitachi Command Suite products by using Global Link Manager GUI, if you want to check whether the distinguished name of the authorization group is registered on the external authorization server by using a user ID such as the `System` account registered in Hitachi Command Suite products, you need to register a user account used to search for LDAP user information on the management server.

In cases other than above, this step is not necessary, because LDAP user information is not searched during authentication and authorization. If a user account used to search for LDAP user information has been already registered, delete it.

Registering a user account for information searching

Use the `hcmds64ldapuser` command to register a user account used to search for LDAP user information.

For a user account used to search for LDAP user information, register a user account that satisfies the following conditions:

- The user account is already registered in the LDAP directory server.
- The user account can bind to the DN specified for `auth.ldap.`*auth.server.name-property-value*`.basedn` in the `exauth.properties` file
- The user account can search the attributes for all entries below the DN specified for `auth.ldap.`*auth.server.name-property-value*`.basedn` in the `exauth.properties` file
- The user account can reference the DN specified for `auth.ldap.`*auth.server.name-property-value*`.basedn` in the `exauth.properties` file

The format of the `hcmds64ldapuser` command is as follows:

installation-folder-for-Hitachi-Command-Suite-Common-Component\bin

```
\hcmds64ldapuser /set /dn DN-of-user-account-used-to-search-for-LDAP-
user-info /pass password-of-user-account-used-to-search-for-LDAP-
user-info /name server-identification-name-or-the-domain-name-for-
the-external-authorization-server
```

- *DN-of-user-account-used-to-search-for-LDAP-user-info*

  Specify a DN by following the rules defined in RFC4514. For example, if the following characters are included in a DN, you need to use a backslash (\) to escape each character.

  Spaces # + , ; < = > \

- *password-of-user-account-used-to-search-for-LDAP-user-info*

  This is case-sensitive and must exactly match the password registered in the LDAP directory server.

- *server-identification-name-or-the-domain-name-for-the-external-authorization-server*

  Specify the server identification name specified for the `auth.server.name` property, or the domain name specified for the `auth.ldap.`*value-specified-for-auth.server.name*`.domain.name` property in the `exauth.properties` file.

Note

In the LDAP directory server, you can use double quotation marks (") for the DN and password. In the management server, however, you need to register a user account whose DN and password do not include double quotation marks.

The following describes an example of execution when the data structure is as indicated in Figure 3-1. In Figure 3-1, the DN of the entry that is the start point for searching is specified as `cn=group,dc=example,dc=com`. If the user who searches the attribute values of all users (`Babs`, `Tim`, and `John`) below the DN has the `administrator` privilege, for the `/dn` option specify the `administrator` DN (`cn=administrator,cn=admin,dc=example,dc=com`). The following is an example of executing the command. The password of `administrator` is `administrator_pass`:

```
hcmds64ldapuser /set /dn
"cn=administrator,cn=admin,dc=example,dc=com" /pass
administrator_pass /name ServerName
```

Note

If you are using Active Directory, you can use the `dsquery` command provided by Active Directory to check the DN of the user. The following example shows how to use the `dsquery` command to check the DN of the user `administrator`, and shows the execution results:

```
dsquery user -name administrator
"CN=administrator,CN=admin,DC=example,DC=com"
```

If the DN includes commas such as `cn=administrator,cn=admin,dc=example,com`, specify as follows:

```
hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example
\,com" /pass administrator_pass /name ServerName
```

Deleting a user account for information searching

To delete a user account for information searching, execute the following command:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64ldapuser /delete /name server-identification-name-or-the-
domain-name-for-the-external-authorization-server
```

Checking LDAP directory servers for which a user account used to search for LDAP user information has been registered

To check the names of LDAP directory servers for which a user account used to search for LDAP user information has been registered on the management server, execute the following command.

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64ldapuser /list
```

Checking the connection status of the external authentication server and the external authorization server (when the authentication method is LDAP)

By using the `hcmds64checkauth` command, you can make sure that the external authentication server and the external authorization server can properly be connected to.

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64checkauth /user user-ID /pass password [/summary]
```

If you specify the `/summary` option, the confirmation message is displayed in summary format during command execution.

user-ID and *password* must match those of the user account that has been registered in the LDAP directory server. *user-ID* must be the same value as the one stored in the attribute that has been specified by `auth.ldap.`*auth.server.name-property-value*`.attr` in the `exauth.properties` file. However, for *user-ID* and *password*, you cannot specify a string that begins with `/`.

Note: In a multi-domain configuration, if you execute the `hcmds64checkauth` command, the connection status of all linked external authentication servers will be checked and the check result for each external authentication server will be displayed.
For an authentication server where the user account specified by the `hcmds64checkauth` command is not registered, an error message indicating that the user account is not registered appears in the check result for Phase 3, and the check process for Phase 3 sometimes fails.

In this case, use a user account registered on an external authentication server to check the connection status for each external authentication server.

The `hcmds64checkauth` command performs the checks in the four phases described below. Check results are displayed for each phase.

Phase 1

The command verifies that common properties (Table 3-24 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (common items) on page 3-93) have been correctly specified in the `exauth.properties` file.

Phase 2

The command verifies that the properties for the external authentication server and the external authorization server (Table 3-25 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (when directly specifying information about the external authentication server) on page 3-94 or Table 3-26 Items to specify in the exauth.properties file when using an LDAP directory server for authentication (when using the DNS server to look up information about the external authentication server) on page 3-97) have been correctly specified in the `exauth.properties` file.

Phase 3

The command verifies that the external authentication server can be connected to.

Phase 4

If an external authorization server is also linked to, the command verifies that the external authorization server can be connected to and authorization groups can be searched.

When a phase finishes normally, the following message is displayed:

```
KAPM15004-I The result of the configuration check of Phase X# was
normal.
```

#: *X* is the phase number.

Example of executing the `hcmds64checkauth` command when the hierarchical structure model is used:

The following describes an example of executing the `hcmds64checkauth` command by using the user account `John` shown in Figure 3-1.

This example assumes that `sAMAccountName` has been specified in `auth.ldap.`*auth.server.name-property-value*`.attr` in the `exauth.properties` file. If the `sAMAccountName` attribute value of `John` is `John_Smith`, specify `John_Smith` in *user-ID*. If the password of `John` to be used on the LDAP directory server is `John_pass`, specify `John_pass` in *password*.

```
hcmds64checkauth /user John_Smith /pass John_pass
```

Example of executing the hcmds64checkauth command when the flat model is used:

The following describes an example of executing the `hcmds64checkauth` command by using the user account `John` shown in Figure 3-2.

This example assumes that `uid` has been specified in `auth.ldap.`*auth.server.name-property-value*`.attr` in the `exauth.properties` file. As the RDN of `John` is `uid=John`, specify the RDN attribute value `John` in *user-ID*. If the password of `John` to be used on the LDAP directory server is `John_pass`, specify `John_pass` in *password*.

```
hcmds64checkauth /user John /pass John_pass
```

Settings required when using a RADIUS server for authentication

To authenticate users by using a RADIUS server, specify the following settings in Hitachi Command Suite products.

1. In the `exauth.properties` file on the management server, specify necessary information.

   Necessary settings depend on whether only an external authentication server is linked to or an external authorization server is also linked to.

   You can use either of the following methods to define the LDAP directory server to be used as an external authorization server:

   - In the `exauth.properties` file, directly specify information about the LDAP directory server to connect to.

     Specify information such as IP address and port number in the `exauth.properties` file for each LDAP directory server.
   - Use the DNS server to look up the LDAP directory server to connect to.

     Before using this method, you need to set up the DNS server environment on the OS of the LDAP directory server. In addition, you need to register the host name, port number, and domain name of the LDAP directory server in the SRV records of the DNS server.

   Note

   To use StartTLS for communication between the management server and the LDAP directory server, you need to directly specify information about the LDAP directory server to connect to in the `exauth.properties` file.

   When using the DNS server to look up the LDAP directory server to connect to, it might take longer for users to log in.
2. When also linking to an external authorization server, on the management server, register a user account used to search for user information on the LDAP directory server.
3. On the RADIUS server, register the accounts of user that will use Hitachi Command Suite products.

User IDs and passwords must consist of characters that can be used in Hitachi Command Suite products. Specify 1 to 256 bytes of the following characters:

`0 to 9 A to Z a to z ! # $ % & ' ( ) * + - . = @ \ ^ _ |`

In Hitachi Command Suite products, user IDs are not case-sensitive. The combination of character types for passwords must follow the settings in the external authentication server.

4. Specify a shared secret on the management server for communicating with the RADIUS server.
5. Register accounts and set permissions by using Global Link Manager GUI.

   When linking to only an external authentication server

   Register users.

   Change the authentication method of users.#

   Set permissions for users.

   Assign resource groups to users.

   #: This operation is required if you want to change the authentication method of existing users.

   When also linking to an external authorization server

   Register authorization groups.

   Set permissions for authorization groups.

   You do not need to assign resource groups to authorization groups. `All Resources` will be automatically assigned to users who belong to authorization groups.
6. Use the `hcmds64checkauth` command to make sure that the external authentication server and the external authorization server can be properly connected to.

The following sections describe operations you need to perform on the management server. For details on how to use Global Link Manager GUI, see the manual *Global Link Manager User Guide*.

Setting the exauth.properties file (when the authentication method is RADIUS)

This section describes the settings required for the `exauth.properties` file in order to use a RADIUS server to authenticate users.

1. Specify values for the following properties in the `exauth.properties` file:
   - Common properties (Table 3-27 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common items) on page 3-108)
   - Properties for an external authentication server (Table 3-28 Items to specify in the exauth.properties file when using a RADIUS server for authentication (settings for the external authentication server) on page 3-109)

     Specify these property values for each RADIUS server.
   - Properties for an external authorization server

These properties need to be set when an external authorization server is also linked to. Specify information about the LDAP directory server for each domain.

The items you need to specify differ depending on whether you directly specify information about the LDAP directory server (Table 3-29 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common settings for the external authorization server) on page 3-111 and Table 3-30 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when directly specifying information about the external authentication server) on page 3-111) or you use the DNS server to look up the LDAP directory server (Table 3-29 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common settings for the external authorization server) on page 3-111 and Table 3-31 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when using the DNS server to look up information about the external authentication server) on page 3-113).

The template of the `exauth.properties` file is stored in the following location:

installation-folder-for-Hitachi-Command-Suite-Common-Component
`\sample\conf\exauth.properties`

Note

Do not enter a space at the beginning or end of a setting value. Also, do not enclose a setting value in double quotation marks (`"`). If you do, the value is ignored, and the default value is used instead.

2. Save the `exauth.properties` file in the following location:

installation-folder-for-Hitachi-Command-Suite-Common-Component
`\conf\exauth.properties`

If you change a setting value in the `exauth.properties` file, the changed value immediately takes effect.

Table 3-27 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common items) on page 3-108 through Table 3-31 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when using the DNS server to look up information about the external authentication server) on page 3-113 list and describe the properties to specify in the `exauth.properties` file.

Table 3-27 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common items)

Property names	Details
`auth.server.type`	Specify an external authentication server type. Specify `radius`.

Property names	Details
	Default value: `internal` (used when not linking to an external authentication server)
`auth.server.name`	Specify the server identification names of RADIUS servers. You can specify any name for this property in order to identify which RADIUS servers the settings such as the port number and the protocol for connecting to the RADIUS server (see Table 3-28 Items to specify in the exauth.properties file when using a RADIUS server for authentication (settings for the external authentication server) on page 3-109) are applied to. `ServerName` has been set as the initial value. You must specify at least one name. When configuring a redundant configuration, separate the server identification name of each server with a comma (`,`). Do not register the same server identification name more than once. Specifiable values: No more than 64 bytes of the following characters: `0` to `9` `A` to `Z` `a` to `z` `!` `#` `(` `)` `+` `-` `.` `=` `@` `[` `]` `^` `_` `{` `}` `~` Default value: none
`auth.group.mapping`	Specify whether to also link to an external authorization server. Specify `true` to link to an external authorization server. Specify `false` to not to link to an external authorization server. Default value: `false`

Table 3-28 Items to specify in the exauth.properties file when using a RADIUS server for authentication (settings for the external authentication server)

Attributes	Details
`protocol`	Specify the protocol for RADIUS server authentication. This attribute is required. Specifiable values: `PAP` or `CHAP` Default value: none
`host`#1	Specify the host name or IP address of the RADIUS server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets (`[]`). This attribute is required. Default value: none
`port`	Specify the port number for RADIUS server authentication. Make sure beforehand that the port you specify is set as the listen port number on the RADIUS server. Specifiable values: 1 to 65535 Default value: 1812

Attributes	Details
`timeout`	Specify the amount of time to wait before timing out when connecting to the RADIUS server. Specifiable values: 1 to 65535 (seconds) Default value: 1
`retry.times`	Specify the number of retries to attempt when an attempt to connect to the RADIUS server fails. If you specify `0`, no retries are attempted. Specifiable values: 0 to 50 Default value: 3
`attr.NAS-Identifier`#2	Specify the host name of the Global Link Manager management server. The RADIUS server uses this attribute value to identify the management server. The host name of the management server has been set as the initial value. Specifiable values: Specify no more than 253 bytes of the following characters: `0` to `9` `A` to `Z` `a` to `z` `!` `"` `#` `$` `%` `&` `'` `(` `)` `*` `+` `,` `-` `.` `/` `:` `;` `<` `=` `>` `?` `@` `[` `\` `]` `^` `_` `` ` `` `{` `|` `}` `~` Default value: none
`attr.NAS-IP-Address`#2	Specify the IPv4 address of the Global Link Manager management server. The RADIUS server uses this attribute value to identify the management server. If the format of the address is invalid, this property is disabled. Default value: none
`attr.NAS-IPv6-Address`#2	Specify the IPv6 address of the Global Link Manager management server. The RADIUS server uses this attribute value to identify the management server. Enclose the IPv6 address in square brackets (`[]`). If the format of the address is invalid, this property is disabled. Default value: none

Note

To specify the attributes, use the following syntax:

`auth.radius.`*auth.server.name-property-value*`.`*attribute*`=`*value*

#1

When linking to an external authorization server that is running on the same computer and using StartTLS as the protocol for connecting to the LDAP directory server, in the host attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.

#2

You must specify one of the following: `attr.NAS-Identifier`, `attr.NAS-IP-Address`, or `attr.NAS-IPv6-Address`.

Table 3-29 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common settings for the external authorization server)

Attributes	Details
`domain.name`	Specify the name of a domain managed by the LDAP directory server. This item is required when an external authorization server is also linked to. Default value: none
`dns_lookup`	Specify whether to use the DNS server to look up the information about the LDAP directory server. If you want to directly specify information about the LDAP directory server in the `exauth.properties` file, specify `false`. If you want to use the DNS server to look up the information, specify `true`. However, if the following attribute values are already set, the LDAP directory server will be connected to by using the user-specified values instead of by using the DNS server to look up the information. • `auth.group.domain-name.host` • `auth.group.domain-name.port` Default value: `false`

Note

To specify the attributes, use the following syntax:

`auth.radius.auth.server.`*name-property-value*`.attribute=value`

Table 3-30 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when directly specifying information about the external authentication server)

Attributes	Details
`protocol`#1	Specify the protocol for connecting to the LDAP directory server. When communicating in plain text format, specify `ldap`. When using StartTLS communication, specify `tls`. Before specifying `tls`, make sure that one of the following encryption methods can be used on the LDAP directory server. • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256 Specifiable values: `ldap` or `tls`

Attributes	Details
	Default value: `ldap`
`host`#2	If the external authentication server and the external authorization server are running on different computers, specify the host name or IP address of the LDAP directory server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets (`[]`). If you omit this attribute, the external authentication server and the external authorization server are assumed to be running on the same computer. Default value: none
`port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authorization. Specify the DN of the hierarchy that includes all of the user entries to be searched. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (`\`) to escape each character. Spaces `# + ; , < = > \` If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. If you omit this attribute, the value specified in the `defaultNamingContext` property of Active Directory is assumed as the BaseDN. Default value: none
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
`retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify `0`, no retries are attempted. Specifiable values: 0 to 50 Default value: 20

Note

To specify the attributes, use the following syntax:

`auth.group.`*domain-name*`.attribute=value`

For *domain-name*, specify the value specified for `auth.radius.auth.server.`*name-property-value*`.domain.name`.

#1:

When communicating by using StartTLS as the protocol for connecting to the LDAP directory server, you need to specify the security settings of Common Component. For details about specifying security settings in order to communicate by using StartTLS, see Security settings for communication between a server and an LDAP directory server on page 5-13.

#2:

When the external authentication server and the external authorization server are running on different computers and when using StartTLS as the protocol for connecting to the LDAP directory server, in the `host` attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.

Table 3-31 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when using the DNS server to look up information about the external authentication server)

Attributes	Details
`protocol`	Specify the protocol for connecting to the LDAP directory server. Specifiable values: `ldap` Default value: `ldap`
`port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authorization. Specify the DN of the hierarchy that includes all of the user entries to be searched. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (\) to escape each character. Spaces `# + ; , < = > \` If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. If you omit this attribute, the value specified in the `defaultNamingContext` property of Active Directory is assumed as the BaseDN.

Attributes	Details
	Default value: none
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
`retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify `0`, no retries are attempted. Specifiable values: 0 to 50 Default value: 20

Note

To specify the attributes, use the following syntax:

`auth.group.`*domain-name*`.attribute=value`

For *domain-name*, specify the value specified for `auth.radius.auth.server.`*name-property-value*`.domain.name`.

The following examples show how to specify the properties:

- When linking to only an external authentication server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=false
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
```

- When directly specifying information about an external authentication server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=false
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.host=ldap.example.com
```

```
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using the DNS server to look up an external authorization server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=true
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using a redundant configuration

```
auth.server.type=radius
auth.server.name=ServerName1,ServerName2
auth.group.mapping=false
auth.radius.ServerName1.protocol=PAP
auth.radius.ServerName1.host=radius1.example.com
auth.radius.ServerName1.port=1812
auth.radius.ServerName1.timeout=1
auth.radius.ServerName1.retry.times=3
auth.radius.ServerName1.attr.NAS-IP-Address=127.0.0.1
auth.radius.ServerName2.protocol=PAP
auth.radius.ServerName2.host=radius2.example.com
auth.radius.ServerName2.port=1812
auth.radius.ServerName2.timeout=1
auth.radius.ServerName2.retry.times=3
auth.radius.ServerName2.attr.NAS-IP-Address=127.0.0.1
```

Registering a user account used to search for LDAP user information (when the authentication method is RADIUS)

When using an LDAP directory server as an external authorization server, by using the `hcmds64ldapuser` command, you can register, on the management server, a user account used to search for LDAP user information. After registering a user account, you can use this command to delete such an account or check LDAP directory servers for which user accounts used to search for LDAP user information have been registered on the management server.

Registering a user account used to search for LDAP user information

Use the `hcmds64ldapuser` command to register a user account used to search for LDAP user information.

For a user account used to search for LDAP user information, register a user account that satisfies the following conditions:

- The user account is already registered in the LDAP directory server.
- The user account can bind to the DN specified for `auth.group.`*domain-name*`.basedn` in the `exauth.properties` file.
- The user account can search the attributes for all entries below the DN specified for `auth.group.`*domain-name*`.basedn` in the `exauth.properties` file.
- The user account can reference the DN specified for `auth.group.`*domain-name*`.basedn` in the `exauth.properties` file

The format of the `hcmds64ldapuser` command is as follows:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64ldapuser /set /dn DN-of-user-account-used-to-search-for-LDAP-
user-info /pass password-of-user-account-used-to-search-for-LDAP-
user-info /name domain-name
```

- *DN-of-user-account-used-to-search-for-LDAP-user-info*

  Specify a DN by following the rules defined in RFC4514. For example, if the following characters are included in a DN, you need to use a backslash (\) to escape each character.

  Spaces `# + , ; < = > \`
- *password-of-user-account-used-to-search-for-LDAP-user-info*

  This is case-sensitive and must exactly match the password registered in the LDAP directory server.
- *domain-name*

  Specify the domain name specified for `auth.radius.auth.server.`*name-property-value*`.domain.name` in the `exauth.properties` file.

Caution

In the LDAP directory server, you can use double quotation marks (") for the DN and password. In the management server, however, you need to register a user account whose DN and password do not include double quotation marks.

Note

You can use the `dsquery` command provided by Active Directory to check the DN of a user. The following example shows how to use the `dsquery` command to check the DN of the user administrator, and also shows the execution results:

```
dsquery user -name administrator
"CN=administrator,CN=admin,DC=example,DC=com"
```

If the DN includes commas such as `cn=administrator,cn=admin,dc=example,com`, specify as follows:

```
hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example
\,com" /pass administrator_pass /name ServerName
```

Deleting a user account used to search for LDAP user information

To delete a user account used to search for LDAP user information, execute the following command.

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64ldapuser /delete /name domain-name
```

Checking LDAP directory servers for which a user account used to search for LDAP user information has been registered

To check the names of LDAP directory servers for which a user account used to search for LDAP user information has been registered on the management server, execute the following command:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64ldapuser /list
```

Setting a shared secret

By using the `hcmds64radiussecret` command, you can specify a shared secret on the management server to communicate with the RADIUS server. After specifying a shared secret, you can use this command to delete a shared secret or to list the server identification names of external authentication servers in which a shared secret has been registered.

Specifying a shared secret

To specify a shared secret by using the `hcmds64radiussecret` command, execute the following command:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64radiussecret /set shared-secret /name RADIUS-server-
indication-name
```

RADIUS-server-indication-name must match a server name specified for the `auth.server.name` property in the `exauth.properties` file.

The following example shows how to execute the `hcmds64radiussecret` command when the shared secret is `secret01` and the server identification name of the RADIUS server is `ServerName`.

```
hcmds64radiussecret /set secret01 /name ServerName
```

Deleting a shared secret

To delete a shared secret, execute the following command:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64radiussecret /delete /name RADIUS-server-indication-name
```

Listing the servers to which a shared secret has been registered

To list the server identification names of RADIUS servers in which a shared secret has been registered, execute the following command:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64radiussecret /list
```

Checking the connection status of the external authentication server and the external authorization server (when the authentication method is RADIUS)

By using the `hcmds64checkauth` command, you can make sure that the external authentication server and the external authorization server can be properly connected to.

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64checkauth /user user-ID /pass password [/summary]
```

user-ID and *password* must match those of the user account that has been registered in the RADIUS server. However, for *user-ID* and *password*, you cannot specify a string that begins with `/`.

If you execute the command with the `/summary` option specified, the confirmation message is displayed in summary format.

The `hcmds64checkauth` command performs the checks in the four phases described below. Check results are displayed for each phase.

Phase 1

The command verifies that common properties (Table 3-27 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common items) on page 3-108) have been correctly specified in the `exauth.properties` file.

Phase 2

The command verifies that the properties for the external authentication server (Table 3-28 Items to specify in the exauth.properties file when using a RADIUS server for authentication (settings for the external authentication server) on page 3-109) and properties for the external authorization server (Table 3-29 Items to specify in the exauth.properties file when using a RADIUS server for authentication (common settings for the external authorization server) on page 3-111 through Table 3-31 Items to specify in the exauth.properties file when using a RADIUS server for authentication (when using the DNS server to look up information about the external authentication server) on page 3-113) have been correctly specified in the `exauth.properties` file.

Phase 3

The command verifies that the external authentication server can be connected to.

Phase 4

If an external authorization server is also linked to, the command verifies that the external authorization server can be connected to and authorization groups can be searched.

When a phase finishes normally, the following message is displayed:

```
KAPM15004-I The result of the configuration check of Phase X# was
normal.
```

#: *X* is the phase number.

Settings required when using a Kerberos server for authentication

To authenticate users by using a Kerberos server, specify the following settings in Hitachi Command Suite products.

1. In the `exauth.properties` file on the management server, specify necessary information.

   Necessary settings depend on whether only an external authentication server is linked to or an external authorization server is also linked to.

   You can use either of the following methods to define the Kerberos server to be used as an external authorization server:

   - In the `exauth.properties` file, directly specify information about the Kerberos server to connect to.

     Specify information about the Kerberos server, such as the IP address and port number, in the `exauth.properties` file for each realm.
   - Use the DNS server to look up the Kerberos server to connect to.

     Specify information about the DNS server that manages Kerberos servers in the `exauth.properties` file.

     In addition, before using this method, you need to register the host name, port number, and realm name of the Kerberos server in the SRV records of the DNS server.

   Note

   To use StartTLS for communication between the management server and the LDAP directory server, you need to directly specify information about the Kerberos server to connect to in the `exauth.properties` file.

   When using the DNS server to look up the Kerberos server to connect to, it might take longer for users to log in.
2. When also linking to an external authorization server, on the management server, register a user account used to search for user information on the LDAP directory server.
3. On the Kerberos server, register accounts of users that will use Hitachi Command Suite products.

   User IDs and passwords must consist of characters that can be used in Hitachi Command Suite products. Specify 1 to 256 bytes of the following characters:

   `0 to 9 A to Z a to z ! # $ % & ' ( ) * + - . = @ \ ^ _ |`

In Hitachi Command Suite products, user IDs are not case-sensitive. The combination of character types for passwords must follow the settings in the external authentication server.

4. Register accounts and set permissions by using Global Link Manager GUI.

   When linking to only an external authentication server

   Register users.

   Change the authentication method of users.#

   Set permissions for users.

   Assign resource groups to users.

   #: This operation is required if you want to change the authentication method of existing users.

   When also linking to an external authorization server

   Register authorization groups.

   Set permissions for authorization groups.

   You do not need to assign resource groups to authorization groups. All Resources will be automatically assigned to users who belong to authorization groups.

5. On the management server, use the `hcmds64checkauth` command to make sure that the external authentication server and the external authorization server can be properly connected to.

The following sections describe operations you need to perform on the management server. For details on how to use Global Link Manager GUI, see the manual *Global Link Manager User Guide*.

Setting the exauth.properties file (when the authentication method is Kerberos)

This section describes the settings required for the `exauth.properties` file in order to use a Kerberos server to authenticate users.

1. Specify values for the necessary properties in the `exauth.properties` file:

   - Common properties (Table 3-32 Items to specify in the exauth.properties file when using a Kerberos server for authentication (common items) on page 3-121)
   - Properties for an external authentication server

     Specify these property values for each Kerberos server.

     The items you need to specify differ depending on whether you directly specify information about the Kerberos server (Table 3-33 Items to specify in the exauth.properties file when using a Kerberos server for authentication (when directly specifying information about the external authentication server) on page 3-122) or you use the DNS server to look up the Kerberos server (Table 3-34 Items to specify in the exauth.properties file when using a Kerberos server for authentication (settings for the external authorization server) on page 3-123).

- Properties for an external authorization server (Table 3-35 Items to specify in the exauth.properties file when using a Kerberos server for authentication (settings for the external authorization server) on page 3-124)

  These properties need to be set if you directly specify information about the Kerberos server and an external authorization server is also linked. Specify the properties for each realm.

The template of the `exauth.properties` file is stored in the following location:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component
\sample\conf\exauth.properties
```

Note

Do not enter a space at the beginning or end of a setting value. Also, do not enclose a setting value in double quotation marks (`"`). If you do, the value is ignored, and the default value is used instead.

2. Save the `exauth.properties` file in the following location:

```
installation-folder-for-Hitachi-Command-Suite-Common-Component
\conf\exauth.properties
```

If you change a setting value in the `exauth.properties` file, the changed value immediately takes effect.

Table 3-32 Items to specify in the exauth.properties file when using a Kerberos server for authentication (common items) on page 3-121 through Table 3-35 Items to specify in the exauth.properties file when using a Kerberos server for authentication (settings for the external authorization server) on page 3-124 list and describe the properties to specify in the `exauth.properties` file.

Table 3-32 Items to specify in the exauth.properties file when using a Kerberos server for authentication (common items)

Property names	Details
`auth.server.type`	Specify an external authentication server type. Specify `kerberos`. Default value: `internal` (used when not linking to an external authentication server)
`auth.group.mapping`	Specify whether to also link to an external authorization server. Specify `true` to link to an external authorization server. Specify `false` to not to link to an external authorization server. Default value: `false`

Table 3-33 Items to specify in the exauth.properties file when using a Kerberos server for authentication (when directly specifying information about the external authentication server)

Attributes	Details
`default_realm`	Specify the default realm name. If you specify a user ID but not a realm name in the Global Link Manager GUI login window, the user is authenticated as a user that belongs to the realm specified for this attribute. This attribute is required. Default value: none
`dns_lookup_kdc`	Specify `false`. Default value: `false`
`clockskew`	Specify the acceptable range of difference between the management server time and Kerberos server time. If the difference exceeds this value, an authentication error occurs. Specifiable values: 0 to 300 (seconds) Default value: 300
`timeout`	Specify the amount of time to wait before timing out when connecting to the Kerberos server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 3
`realm_name`	Specify the realm identification names. These names can be freely specified in order to identify the Kerberos server information for each realm. You must specify at least one name. When specifying multiple realm identification names, separate the names with commas (`,`). Do not register the same realm identification name more than once. Default value: none
value-specified-for-realm_name`.realm`	Specify the name of the realm set in the Kerberos server. This attribute is required. Default value: none
value-specified-for-realm_name`.kdc`	Specify the information about the Kerberos server in the following format: *host-name-or-IP-address*`[:`*port-number*`]` This attribute is required. *host-name-or-IP-address* If you specify the host name, make sure beforehand that the name can be resolved to an IP address.

Attributes	Details
	If you specify the IP address, use an IPv4 address. In an IPv6 environment, you must specify the host name (and not the host name). Note that you cannot specify the loopback address (`localhost` or `127.0.0.1`). *port-number* Make sure beforehand that the port you specify is set as the listen port number on the Kerberos server. If you do not specify a port number, or if the specified port number cannot be used for the Kerberos server, 88 is assumed. When configuring the Kerberos server in redundant configuration, separate the servers with commas (`,`) as follows: *host-name-or-IP-address*`[:`*port-number*`]`,*host-name-or-IP-address*`[:`*port-number*`]`,...

Note

To specify the attributes, use the following syntax:

`auth.kerberos.`*attribute*=*value*

The following table describes the property attributes for linking to a Kerberos server when you acquire information about the Kerberos server from the DNS server.

Table 3-34 Items to specify in the exauth.properties file when using a Kerberos server for authentication (settings for the external authorization server)

Attributes	Details
`default_realm`	Specify the default realm name. If you specify a user ID but not a realm name in the Global Link Manager GUI login window, the user is authenticated as a user that belongs to the realm specified for this attribute. This attribute is required. Default value: none
`dns_lookup_kdc`	Specify `true`. This attribute is required. However, if all the following attributes values are already set, the Kerberos server will not be looked up by using the DNS server. • `realm_name` • *value-specified-for-realm_name*`.realm` • *value-specified-for-realm_name*`.kdc`
`clockskew`	Specify the acceptable range of difference between the management server time and Kerberos server time. If the difference exceeds this value, an authentication error occurs.

Attributes	Details
	Specifiable values: 0 to 300 (seconds) Default value: 300
`timeout`	Specify the amount of time to wait before timing out when connecting to the Kerberos server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 3

Note

To specify the attributes, use the following syntax:

`auth.kerberos.`*attribute*`=`*value*

Table 3-35 Items to specify in the exauth.properties file when using a Kerberos server for authentication (settings for the external authorization server)

Attributes	Details
`protocol`#	Specify the protocol for connecting to the LDAP directory server. When communicating in plain text format, specify `ldap`. When using StartTLS communication, specify `tls`. StartTLS communication can be used only when directly specifying information about the Kerberos server. Before specifying `tls`, make sure that one of the following encryption methods can be used on the LDAP directory server. • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256 Specifiable values: `ldap` or `tls` Default value: `ldap`
`port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authorization.

Attributes	Details
	Specify the DN of the hierarchy that includes all of the user entries to be searched. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (\) to escape each character. Spaces # + ; , < = > \ If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. If you omit this attribute, the value specified in the defaultNamingContext property of Active Directory is assumed as the BaseDN. Default value: none
timeout	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
retry.interval	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
retry.times	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20

Note

To specify the attributes, use the following syntax:

`auth.group.`*realm-name*`.attribute=value`

For *realm-name*, specify the value specified for `auth.kerberos.`*realm_name-property-value*`.realm`.

#:

When communicating by using StartTLS as the protocol for connecting to the LDAP directory server, you need to specify the security settings of Common Component. For details about specifying security settings in order to communicate by using StartTLS, see Security settings for communication between a server and an LDAP directory server on page 5-13.

The following examples show how to specify the properties:

- When directly specifying information about a Kerberos server (when not linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
```

- When using the DNS server to look up a Kerberos server (when not linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- When directly specifying information about a Kerberos server (when also linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using the DNS server to look up a Kerberos server (when also linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=true
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- When using a redundant configuration

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos.example.com:88,kerberos.example.net:88
```

- When specifying multiple realm identifiers

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1,S2
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos1.example.com:88,kerberos1.example.net:88
auth.kerberos.S2.realm=EXAMPLE.NET
auth.kerberos.S2.kdc=kerberos2.example.com:88,kerberos2.example.net:88
```

Registering a user account used to search for LDAP user information (when the authentication method is Kerberos)

When using an LDAP directory server as an external authorization server, by using the `hcmds64ldapuser` command, you can register, on the management server, a user account used to search for LDAP user information. After registering a user account, you can use this command to delete such an account or check LDAP directory servers for which user accounts used to search for LDAP user information have been registered on the management server.

Registering a user account used to search for LDAP user information

Use the `hcmds64ldapuser` command to register a user account used to search for LDAP user information.

For a user account used to search for LDAP user information, register a user account that satisfies the following conditions:

- The user account is already registered in the LDAP directory server.
- The user account can bind to the DN specified for auth.group.realm-name.basedn in the `exauth.properties` file
- The user account can search the attributes for all entries below the DN specified for auth.group.realm-name.basedn in the `exauth.properties` file
- The user account can reference the DN specified for auth.group.realm-name.basedn in the `exauth.properties` file

The format of the `hcmds64ldapuser` command is as follows:

```
installation-folder-for-Common-Component\bin\hcmds64ldapuser /
set /dn DN-of-user-account-used-to-search-for-LDAP-user-info /pass
password-of-user-account-used-to-search-for-LDAP-user-info /name
realm-name
```

- *DN-of-user-account-used-to-search-for-LDAP-user-info*

  Specify a DN by following the rules defined in RFC4514. For example, if the following characters are included in a DN, you need to use a backslash (\) to escape each character.

Spaces # + , ; < = > \

- *password-of-user-account-used-to-search-for-LDAP-user-info*

  This is case-sensitive and must exactly match the password registered in the LDAP directory server.

- *realm-name*

  If you directly specify information about a Kerberos server in the `exauth.properties` file, specify the value specified for *auth.kerberos.default_realm* or `auth.kerberos.auth.kerberos.`*realm_name-property-value*`.realm`.

  If you specify the settings in the `exauth.properties` file to use the DNS server to look up information about a Kerberos server, specify the realm name registered in the DNS server.

Caution

In the LDAP directory server, you can use double quotation marks (") for the DN and password. In the management server, however, you need to register a user account whose DN and password do not include double quotation marks.

Note

You can use the `dsquery` command provided by Active Directory to check the DN of a user. The following example shows how to use the `dsquery` command to check the DN of the user administrator, and also shows the execution results:

```
dsquery user -name administrator
"CN=administrator,CN=admin,DC=example,DC=com"
```

If the DN includes commas such as `cn=administrator,cn=admin,dc=example,com`, specify as follows:

```
hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example
\,com" /pass administrator_pass /name ServerName
```

Deleting a user account used to search for LDAP user information

To delete a user account used to search for LDAP user information, execute the following command.

```
installation-folder-for-Common-Component\bin\hcmds64ldapuser /
delete /name realm-name
```

Checking LDAP directory servers for which a user account used to search for LDAP user information has been registered

To check the names of LDAP directory servers for which a user account used to search for LDAP user information has been registered on the management server, execute the following command.

```
installation-folder-for-Common-Component\bin\hcmds64ldapuser /list
```

Checking the connection status of the external authentication server and the external authorization server (when the authentication method is Kerberos)

By using the `hcmds64checkauth` command, you can make sure that the external authentication server and the external authorization server can be properly connected to. If you have specified multiple realm names in the `exauth.properties` file, check the connection status for each realm.

```
installation-folder-for-Hitachi-Command-Suite-Common-Component\bin
\hcmds64checkauth /user user-ID /pass password [/summary]
```

The user account to be specified for user-ID and password depends on whether only an external authentication server is linked or an external authorization server is also linked to.

When linking to only an external authentication server:

Specify a user account that is registered in Hitachi Command Suite products and whose authentication method has been set to Kerberos authentication.

When also linking to an external authorization server:

Specify a user account that is not registered in Hitachi Command Suite products.

If you specify a user who belongs to a realm different from the realm name specified for `default_realm` in the `exauth.properties` file, also check which realm the user belongs to. If you specify multiple realm names in the `exauth.properties` file, check all the specified realm names. For *user-ID* and *password*, you cannot specify a string that begins with `/`.

If you execute the command with the `/summary` option specified, the confirmation message is displayed in summary format.

Note: If more than one realm name is specified in the `exauth.properties` file, specify user IDs according to the following:

- To specify a user belonging to a realm other than the realm set for `default_realm` in the `exauth.properties` file:

  user-ID@*realm-name*

- To specify a user who belongs to the realm set for `default_realm` in the `exauth.properties` file:

  You can omit the realm name.

If you execute the hcmds64checkauth command, the settings in the `exauth.properties` file, and the connection status of the external authentication server and the external authorization server are checked in the four phases described below. Check results are displayed for each phase.

Phase 1

The command verifies that common properties (Table 3-32 Items to specify in the exauth.properties file when using a Kerberos server for

authentication (common items) on page 3-121) have been correctly specified in the `exauth.properties` file.

Phase 2

The command verifies that the properties for the external authentication server (Table 3-33 Items to specify in the exauth.properties file when using a Kerberos server for authentication (when directly specifying information about the external authentication server) on page 3-122 and Table 3-34 Items to specify in the exauth.properties file when using a Kerberos server for authentication (settings for the external authorization server) on page 3-123) and properties for the external authorization server (Table 3-35 Items to specify in the exauth.properties file when using a Kerberos server for authentication (settings for the external authorization server) on page 3-124) have been correctly specified in the `exauth.properties` file.

Phase 3

The command verifies that the external authentication server can be connected to.

Phase 4

If an external authorization server is also linked to, the command verifies that the external authorization server can be connected to and authorization groups can be searched.

When a phase finishes normally, the following message is displayed:

```
KAPM15004-I The result of the configuration check of Phase X# was
normal.
```

#: *X* is the phase number.

Encryption types that can be used for the Kerberos authentication

In Hitachi Command Suite products, the encryption types listed below can be used for Kerberos authentication. Configure the Kerberos server so that one of the following encryption types can be used.

- AES256-CTS-HMAC-SHA1-96
- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC

4

Installing Global Link Manager clusters

This chapter describes how to set up Global Link Manager to run in a cluster environment.

Some Windows Server 2012 terms refer to items that are assigned different names in other Windows server OSs, but which have similar functions. This chapter uses the names that appear in OSs that are not Windows Server 2012 unless otherwise indicated. If you are using Windows Server 2012, replace the term *Failover Cluster Management* with *Failover Cluster Manager*, and the term *resource group* with *role*, as you read through the procedures.

Global Link Manager cluster system configuration

The management server for Hitachi Command Suite products supports active-standby failover in clusters. In a cluster, the server system executing system operations is called the *primary node*. The server system that is on standby to take over operations if a failure occurs in the executing system is called the *secondary node*. If a failure occurs, failover clustering switches servers from the primary node to the secondary node to continue operation. High availability is thus assured because a failure will not interrupt operation.

The following figure illustrates the concept of the management server in a cluster configuration.

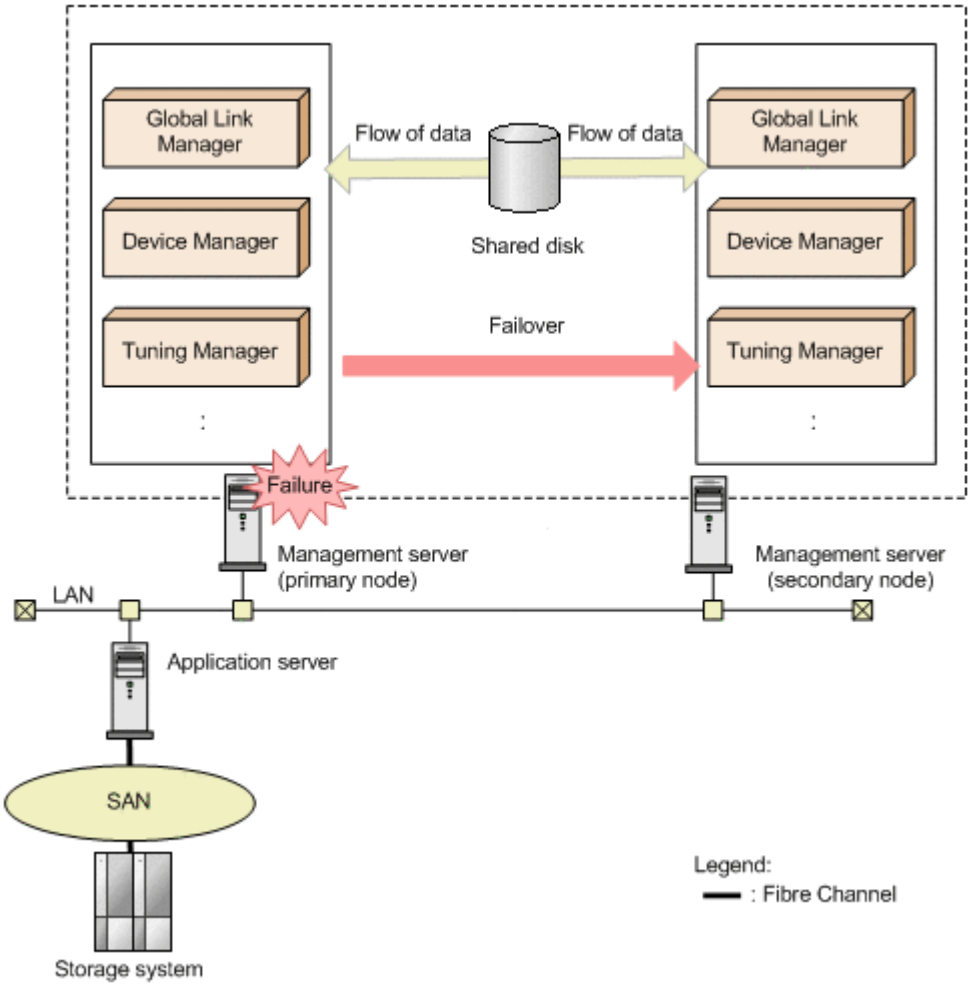

Figure 4-1 Concept of cluster configuration

The software programs controlling the entire cluster system are called *cluster software*. Cluster software monitors the system to make sure that the system is operating properly, and performs a failover to prevent an interruption to operations if the software detects an abnormal condition.

Environment prerequisites for setting up a cluster environment

When you set up a cluster environment, disk capacity for the management server is required to re-create or back up the database on the management server. Confirm that the following disk capacities are available in the management server:

Capacity required to re-create the database

For a new installation:

<database-size-for-Hitachi-Command-Suite-Common-Component> + *<database-size-for-all-Hitachi-Command-Suite-products-including-Global-Link-Manager-installed-on-the-same-host-as-the-Global-Link-Manager-server>*

For an upgrade installation from a version earlier than 8.0.0:

<database-size-for-Hitachi-Command-Suite-Common-Component> + *<database-size-for-all-Hitachi-Command-Suite-products-including-Global-Link-Manager-installed-on-the-same-host-as-the-Global-Link-Manager-server>* + 0.7GB

Capacity required to back up the database

(*<sum-of-the-database-sizes-of-the-Hitachi-Command-Suite-products-to-be-backup-up>* x 2) + 20MB

Note

The database size for Global Link Manager and Hitachi Command Suite Common Component should be the size of the storage folder for the database files. For details about database sizes for different Hitachi Command Suite products, see the manual for that product.

Notes on operating Global Link Manager in a cluster environment

The following notes apply to operating Global Link Manager in a cluster environment:

- On all nodes that make up a cluster, the disk configuration must be the same, and the installation folder for the Hitachi Command Suite products must have the same name (including the drive letter and path name).
- When you change the Hitachi Command Suite product settings after the installation in a cluster environment, specify the same settings on all nodes.
- If you change the port number used by HiRDB from the default (22032/tcp) to another value, you need to set the same port number for both the primary and secondary nodes.

- You need to set different port numbers to be used by HiRDB for versions earlier than 8.0.0 and for version 8.0.0 and later of Hitachi Command Suite products. In addition, you also need to set different port numbers to be used by HiRDB for Hitachi File Services Manager and for version 8.0.0 and later of Hitachi Command Suite products.

  When the database is migrated to a shared disk, the port number used by HiRDB returns to the default. Therefore, if some Hitachi Command Suite products are already running and you changed the port number used by HiRDB to a value other than the default for these products, you need to make a note of the port numbers in advance so that you can set the port numbers in such a way that they do not conflict.

  To reference or set a port number, you need to confirm the port number configuration file in Hitachi Command Suite Common Component. The port number configuration file is stored in the following location:

  For version 8.0.0 or later:

  `<Global-Link-Manager-installation-folder>\Base64`

  For versions earlier than 8.0.0:

  `<Global-Link-Manager-installation-folder>\Base`

- If you are setting up other Hitachi Command Suite products to run in a cluster configuration, complete the work required for the setup, and then start the Global Link Manager installation.
- In this manual, a group of services to be used in a cluster configuration (unit of services for which a failover is performed) is called a resource group.
- Register, as a client access point, the network name (logical host name) and IP address (cluster management IP address) to the resource group for accessing Hitachi Command Suite products, including Global Link Manager. If the IP address is registered to the resource group, re-register as a client access point. In this manual, the network name of a cluster management IP address registered as a client access point is called a "logical host name".
- You cannot use the characters below when specifying a resource group name. If you specified any of the following characters in the resource group name, change the resource group name to one that does not include the following characters:

  `! " & ) * ^ | < >`

- To access a cluster management application, you need to log in as a domain administrator with Administrator permissions.
- If you perform an upgrade installation of Hitachi Global Link Manager from a version earlier than v8 to v8 or later, take note of the following:
  - The name of the Global Link Manager service used in the cluster software will change. For details on service names, see the manual for the applicable version.
  - The URL for activating the Global Link Manager GUI changes to `http://`*logical-host-name*`:22015/GlobalLinkAvailabilityManager/`.

- Before the installation, make sure that the following conditions are satisfied:
  - Resource groups have been created in the cluster software.
  - The primary and secondary nodes have been registered for a resource group.
  - The cluster management IP address and shared disk are placed online.
- Make sure that the structure of the Global Link Manager installation folder is the same for the primary and secondary nodes.
- For the location for storing the Global Link Manager database, specify the shared disk.
- Do not execute the following commands until the installation for the secondary node is complete:
  - The `hcmds64dbclustersetup` command of Hitachi Command Suite Common Component
  - The `setupcluster` command of Hitachi Automation Director

Types of Global Link Manager cluster installations

This section describes the types of Global Link Manager installations in a cluster environment.

There are five types of Global Link Manager installations in a cluster environment:

- Setting up a Global Link Manager cluster for a new installation
- Setting up a Global Link Manager cluster for a reinstallation or version upgrade installation
- Setting up a Global Link Manager cluster for an existing installation
- Setting up a Global Link Manager cluster for a new installation in an environment where other Hitachi Command Suite products are running in a cluster configuration
- Setting up a Global Link Manager cluster for removal

When you perform each installation, see the following subsections.

Table 4-1 Subsections to be referred to when performing a installation

Type of installation and cluster setup	When no other Hitachi Command Suite products have been installed	When other Hitachi Command Suite products are running in a cluster configuration
New installation	Installing Global Link Manager clusters for	Installing Global Link Manager clusters for

Type of installation and cluster setup	When no other Hitachi Command Suite products have been installed	When other Hitachi Command Suite products are running in a cluster configuration
	new installations on page 4-6	new installations on page 4-6
Reinstallation or version upgrade installation	Reinstallation or version upgrade installation of Global Link Manager in a cluster environment on page 4-13	Reinstallation or version upgrade installation of Global Link Manager in a cluster environment on page 4-13#
Removal	Removing a Global Link Manager cluster on page 4-21	Removing a Global Link Manager cluster on page 4-21
Changing from a non-cluster configuration to a cluster configuration	Installing a Global Link Manager cluster for an existing installation on page 4-17	Installing a Global Link Manager cluster for an existing installation on page 4-17#

These setup procedures assume that no other Hitachi Command Suite products have been installed. For details about how to set up the clusters of other Hitachi Command Suite products, see the manual for each product.

Installing Global Link Manager clusters for new installations

For details about items to be configured at new installation, see Installing Global Link Manager for the first time on page 2-6.

You need to enter a logical host name for the "IP address or host name of the server" setting.

Caution

- If you want to also install other Hitachi Command Suite products, install them together.
- When performing a new installation of multiple Hitachi Command Suite products on a standby node, install the products in the order they were installed on the active node.

Performing a new installation of Global Link Manager

1. Start with a new installation on the primary node.

   If other Hitachi Command Suite products have been installed in a cluster configuration, move the resource group owner who registered the Hitachi Command Suite product services from the secondary node to the primary node, and place the IP address and the shared disk online.

2. On the primary node, insert the Global Link Manager installation DVD-ROM.

   In the displayed window, click the **Install** button next to **Hitachi Global Link Manager Software**.

   If the window does not appear, directly execute the installer (`setup.exe`).

   The installer is stored in *drive-where-installation-DVD-ROM-is-set*:`\HGLM`.

   After the installer starts, the **Welcome to the Installation of Hitachi Global Link Manager (New)** dialog box appears.

3. Click the **Next** button.

   The **Select Cluster Configuration** dialog box appears. Select the "Install in a cluster environment" option. If a cluster configuration has already been set up for other Hitachi Command Suite products, the **Select Cluster Configuration** dialog box is not displayed.

4. Click the **Next** button.

   The **Edit Cluster Settings** dialog box appears. Set the following items:

   If a cluster configuration has already been set up for other Hitachi Command Suite products, the **Edit Cluster Settings** dialog box is not displayed.

   - Cluster mode

     Select "Active node". If a cluster configuration has already been set up for other Hitachi Command Suite products, you do not need to select the cluster mode.

   - Resource group name

     Specify a resource group name for which the Global Link Manager services will be registered.

     You do not need to specify this item when the cluster configuration is already set up by another Hitachi Command Suite product. If you changed the resource group name for which the Hitachi Command Suite product services were registered, specify the new resource group name.

   - Logical host name

     Specify the logical host name. If a cluster configuration has already been set up for other Hitachi Command Suite products, you do not need to specify this item.

   - Active node host name

     Specify the host name of the primary node. If a cluster configuration has already been set up for other Hitachi Command Suite products, you do not need to specify this item.

   - Standby node host name

     Specify the host name of the secondary node. If a cluster configuration has already been set up for other Hitachi Command Suite products, you do not need to specify this item.

5. Click the **Next** button.

   The **Dynamic Link Manager Installer File Download** dialog box appears.

Select the check box to enable the function for downloading the HDLM installer. If the download functionality is enabled, the HDLM installer file can be stored on the Global Link Manager server, and then you will be able to download the HDLM installer by using the client Web browser.

6. Click the **Next** button.

   If any other Hitachi Command Suite products have been installed and the services of the Hitachi Command Suite products are placed online, the **Stopping the Services of Hitachi Command Suite Products** dialog box appears. Click the **Next** button to place the services of the Hitachi Command Suite products offline and suppress failovers.

   Note

   If new installation of Global Link Manager is canceled before the installation is started, the services of the Hitachi Command Suite products are placed offline and failovers are suppressed. If you do not perform a new installation of Global Link Manager and continue to operate the Hitachi Command Suite products, see Turning a service online in the cluster management application on page 4-25 to place the services of the Hitachi Command Suite products online and enable failovers.

7. Click the **Next** button.

   The **Setup of the Installation Folder** dialog box appears.

   If you do not want to accept the default installation folder, specify another installation folder. The rules for specifying an installation folder are as follows:

   - Do not specify an installation folder that is directly under a drive letter (such as `C:\` or `D:\`).
   - The maximum length of an absolute path is 64 bytes.
   - Only the following characters can be used:

     `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), underscore (_), and the space character.

     Note that you cannot specify a space character or a period at the beginning or end of a folder name.

     Furthermore, you cannot specify two or more space characters in a row.
   - The path name must not contain any names reserved by the OS (`CON`, `AUX`, `NUL`, `PRN`, `CLOCK$`, `COM1` to `COM9`, and `LPT1` to `LPT9`).

   You cannot install Global Link Manager under any of the following folders:

   - `%ProgramFiles(x86)%\`
   - `%CommonProgramFiles(x86)%\`
   - `%SystemRoot%\SysWOW64\`
   - `%SystemRoot%\system32\`
   - `%ProgramFiles%\WindowsApps\`

   The default installation folder for Global Link Manager is as follows:

   system-drive`:\Program Files\HiCommand`

The default installation folder for Hitachi Command Suite Common Component is as follows:

system-drive:\Program Files\HiCommand\Base64

If you install Global Link Manager on a server on which other Hitachi Command Suite products are not installed, Global Link Manager and Hitachi Command Suite Common Component will be installed in the folder that is specified in the **Setup of the Installation Folder** dialog box. If you install Global Link Manager on a server on which other Hitachi Command Suite products are installed, Global Link Manager will be installed in the folder that is specified in the **Setup of the Installation Folder** dialog box, but Hitachi Command Suite Common Component will be installed in the folder that contains the existing Hitachi Command Suite Common Component, and overwrites it. If you want to check the installation folder for Hitachi Command Suite Common Component, check the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Hitachi\HiCommand Base 64\InstallPath

8. Click the **Next** button.

   The **Setup of the Storage Destination for Database Files of Hitachi Global Link Manager** dialog box appears.

   If you do not want to accept the default folder, specify another folder. The rules for specifying a folder are as follows:

   - Do not specify a storage destination folder for database files that is directly under a drive letter (such as C:\ or D:\).
   - The maximum length of an absolute path is 64 bytes.
   - Only the following characters can be used:

     A to Z, a to z, 0 to 9, period (.), underscore (_), and the space character.

     Note that you cannot specify a space character or a period at the beginning or end of a folder name.

     Furthermore, you cannot specify two or more space characters in a row.
   - The path name must not contain any names reserved by the OS (CON, AUX, NUL, PRN, CLOCK$, COM1 to COM9, and LPT1 to LPT9).

   Note

   The database files of Hitachi Global Link Manager are created under the *specified-storage-destination*\x64 folder.

9. Click the **Next** button.

   If this installation will install the 64-bit version of Hitachi Command Suite Common Component for the first time in an environment where the 32-bit version of Hitachi Command Suite Common Component exists, the **Setup of the data backup storage folder for database files** of Hitachi Command Suite dialog box appears.

   To upgrade the Hitachi Command Suite products from v7 or earlier to v8, specify a storage destination for the database files of Hitachi Command

Suite products. If you want to use a folder different from the default, follow the rules below to specify the folder:

- Absolute paths must be 150 bytes or less.
- Only the following characters can be used:

  `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), underscore (`_`), and the space character.

  Note that you cannot specify a space character or a period at the beginning or end of a folder name.

  Furthermore, you cannot specify two or more space characters in a row.
- The path name must not contain any names reserved by the OS (`CON`, `AUX`, `NUL`, `PRN`, `CLOCK$`, `COM1` to `COM9`, and `LPT1` to `LPT9`).

The following is the default database storage destination for the Hitachi Command Suite products:

specified-installation-folder-for-Hitachi-Global-Link-Manager`\databackup`

10. Click the **Next** button.

    The **Setup of Information about the Server of Hitachi Global Link Manager** dialog box appears.

    Specify the following information (confirm the information before you start installation):

    - Port number for HBase 64 Storage Mgmt Web Service
    - Enabling or disabling reception of an SNMP trap

    In the "IP address or host name of the server" field, the logical host name specified in the **Cluster Settings** dialog box is displayed, but the name is inactive and cannot be edited.

    If another Hitachi Command Suite product has already been installed, the fields for the following information are disabled:

    - Port number for HBase 64 Storage Mgmt Web Service

11. Click the **Next** button.

    If you have enabled the SNMP trap receiving function, the **SNMP Trap Connection Settings for Hitachi Global Link Manager** dialog box appears. If you have disabled this function, go to the next step.

    Specify the following information (check the information before you start installation):

    - IP address for receiving SNMP traps (logical IP address of the cluster)
    - Port number for receiving SNMP traps

    The IP address of the Global Link Manager server is displayed as the IP address for receiving SNMP traps. If nothing is displayed, enter the IP address of the server.

    When specifying an IPv6 address, enclose the IP address in square brackets (`[ ]`).

    Note

When you install Global Link Manager on a server on which Device Manager is installed, specify a port number other than 162 for the port that receives SNMP traps. When the reception of SNMP traps is being used in Device Manager, if you specify 162 for the port that receives SNMP traps during the installation of Global Link Manager, you will no longer be able to start Device Manager.

12. Click the **Next** button.

    If Windows Firewall is installed, the **Windows Firewall** dialog box appears. Check the information on the **Exceptions** tab, and then click the **Next** button. Hitachi Command Suite Common Component and the port that receives SNMP traps will be added to the Windows Firewall exceptions list.

    Note

    If you register Global Link Manager as an exception in the Windows Firewall exceptions list, it might take approximately 15 minutes more to install Global Link Manager. If you enabled Windows Firewall after installing Global Link Manager, you must manually add Global Link Manager to the exceptions list. For details on how to manually add Global Link Manager to the exception list, see Settings for Windows firewalls on page 3-67.

13. Confirm that the displayed installation settings are correct, and then click the **Install** button.

    Installation starts. During the installation, dialog boxes indicating the processing status appear. When the **HGLM Settings Complete** dialog box appears, confirm the settings you specified during installation.

    If a value specified for **URL for the HGLM login window** does not match the information on the server on which Global Link Manager is installed, see the appropriate reference below and change the value:

    - For details on how to change the IP address, see Changing the Global Link Manager login URL on page 3-64.
    - For details on how to change the host name, see Changing the Global Link Manager server host name on page 3-56.
    - For details on how to change the port number of HBase 64 Storage Mgmt Web Service, see Changing port numbers for accessing the HBase 64 Storage Mgmt Web Service on page 3-60.

14. Click the **Next** button.

    When installation has been completed normally, the **Installation Complete** dialog box appears.

15. Click the **Finish** button to finish the installation.

    Note

    If you perform a new installation of Global Link Manager in an environment where no other Hitachi Command Suite products are installed, at this point, the services used by Global Link Manager are not registered to the resource group.

16. When you want to use a function that outputs path availability information in a report, edit the property file (`server.properties`).

The `server.properties` file is stored in the following location:

Global-Link-Manager-installation-folder\conf

Change the folder for storing reports to a folder on the shared disk.

For `server.pathreport.log_location`, specify an absolute path (maximum of 150 bytes) for the folder that stores reports. Deploy this folder on the shared disk. To use a backslash (\) as the path delimiter, you must use two consecutive backslashes.

The following shows a coding example:

```
server.pathreport.log_location=E:\\HGLAM\\pathreport
```

For details about the settings in the property file for path availability information, see Changing Global Link Manager server settings on page 3-34.

17. For the resource group in which the services of Hitachi Command Suite products are registered, move the owner of the resource group from the primary node to the secondary node.

    If Microsoft Failover Cluster is used (on OSs other than Windows Server 2012):

    In Failover Cluster Management, right-click the resource group to which the services used by Global Link Manager have been registered, and then choose **Move this service or application to another node**.

    If Microsoft Failover Cluster is used (on Windows Server 2012):

    In Failover Cluster Manager, right-click the role to which the services used by Global Link Manager have been registered, choose **Move**, and then **Select Node**.

18. Install Global Link Manager on the secondary node.

    In the **Select Cluster Configuration** dialog box, select **Standby node** for **Cluster mode**. For other items, specify the same values as those for the primary node.

19. Start operations for Global Link Manager in the cluster environment.

    For details, see Starting operations for Global Link Manager in a cluster environment on page 4-22.

Setting up Microsoft Failover Cluster

Before specifying the settings for Windows Server Failover Clustering, perform the following operations:

- Prepare a cluster group (resource group) that is the group of services to be used in a cluster configuration (unit of services for which a failover is performed).
- Set up a resource group that includes the cluster management IP address and a shared disk that can be inherited between the primary node and the secondary node.

- Make sure that resource allocation, resource deletion, and operation monitoring can be normally controlled by Windows Server Failover Clustering.
- If a resource group for which other Hitachi Command Suite products are registered already exists, use that resource group.
- Set up a resource group by using only resources that are related to Hitachi Command Suite products.

Reinstallation or version upgrade installation of Global Link Manager in a cluster environment

This section describes how to perform the following installations when the system has been configured in a cluster environment:

- Reinstalling (overwriting) the same version of Global Link Manager
- Upgrading Global Link Manager to a newer version

If the service is not online on the primary node, first place it online, and then perform a reinstallation or version upgrade installation.

Note

For notes on performing a reinstallation or an upgrade installation of Global Link Manager, see Upgrade installation of Global Link Manager on page 2-14.

Performing a reinstallation or upgrade installation of Global Link Manager

1. Display cluster software

   Select **Start**, **Control Panel**, **Administrative Tools**, and then **Failover Cluster Management**.

2. Switch the group to which the services used by Global Link Manager have been registered to the executing system.

   If Microsoft Failover Cluster (on OSs other than Windows Server 2012) is used:

   In Failover Cluster Management, right-click the resource group to which the services used by Global Link Manager have been registered, and then choose **Move this service or application to another node**.

   If Microsoft Failover Cluster is used (on Windows Server 2012):

   In Failover Cluster Manager, right-click the role to which the services used by Global Link Manager have been registered, choose **Move** and then **Select Node**.

3. If the port number that HiRDB uses has already been changed from the default value# and is being used, write down the used port number.

   #

   The default value is as follows:

   v7.6.1 and earlier: 23032/tcp, v8.0.0 and later: 22032/tcp

4. Back up the database.

   For details about how to back up the database, see Backing up the Global Link Manager database on page 3-8.

5. Insert the Global Link Manager installation DVD-ROM into the primary node.

   In the displayed window, click the **Install** button next to **Hitachi Global Link Manager Software**.

   If the window does not appear, directly execute the installer (`setup.exe`).

   The installer is stored in *drive-where-installation-DVD-ROM-is-set*`:\HGLM`.

   After the installer starts, the **Welcome to the Installation of Hitachi Global Link Manager (Overwrite)** dialog box appears.

6. Click the **Next** button.

   The **Dynamic Link Manager Installer File Download** dialog box appears.

   Select the check box to enable the function for downloading the HDLM installer. If the download functionality is enabled, the HDLM installer file can be stored on the Global Link Manager server, and then you will be able to download the HDLM installer by using the client Web browser.

   If the HDLM installer is already installed with the download function enabled, this dialog box is not displayed.

7. Click the **Next** button.

   If any other services of Hitachi Command Suite Common Component or of another Hitachi Command Suite product services are running, the **Stopping the Services of Hitachi Command Suite Products** dialog box appears.

   Click the **Next** button to stop those services.

   Note

   If new installation of Global Link Manager is canceled before the installation is started, the services of the Hitachi Command Suite products are placed offline and failovers are suppressed. If you do not perform a new installation of Global Link Manager and continue to operate the Hitachi Command Suite products, see Turning a service online in the cluster management application on page 4-25 to place the services of the Hitachi Command Suite products online and enable failovers.

8. Click the **Next** button.

   If this installation will install the 64-bit version of Hitachi Command Suite Common Component for the first time in an environment where the 32-bit version of Hitachi Command Suite Common Component exists, the **Setup of the data backup storage folder for database files** of Hitachi Command Suite dialog box appears.

   To upgrade the Hitachi Command Suite products from v7 or earlier to v8, specify a storage destination for the database files of Hitachi Command Suite products. If you want to use a folder different from the default, follow the rules below to specify the folder:

   - Absolute paths must be 150 bytes or less.

- Only the following characters can be used:

  A to Z, a to z, 0 to 9, period (.), underscore (_), and the space character.

  Note that you cannot specify a space character or a period at the beginning or end of a folder name.

  Furthermore, you cannot specify two or more space characters in a row.
- The path name must not contain any names reserved by the OS (CON, AUX, NUL, PRN, CLOCK$, COM1 to COM9, and LPT1 to LPT9).

The following is the default database storage destination for the Hitachi Command Suite products:

specified-installation-folder-for-Hitachi-Global-Link-Manager\databackup

9. Click the **Next** button.

   The property files of Hitachi Global Link Manager and the **Setup of the data backup storage folder for path status log and property files of Hitachi Global Link Manager** dialog box appear. If you want to use a folder different from the default, follow the rules below to specify the folder:

   - Absolute paths must be 140 bytes or less.
   - Only the following characters can be used:

     A to Z, a to z, 0 to 9, period (.), underscore (_), and the space character.

     Note that you cannot specify a space character or a period at the beginning or end of a folder name.

     Furthermore, you cannot specify two or more space characters in a row.
   - The path name must not contain any names reserved by the OS (CON, AUX, NUL, PRN, CLOCK$, COM1 to COM9, and LPT1 to LPT9).

   The following is the default storage destination for the property files of Hitachi Global Link Manager and the path availability information:

   specified-installation-folder-for-Hitachi-Global-Link-Manager\databackup

10. Click the **Next** button.

    If Windows Firewall is installed, the **Windows Firewall** dialog box appears. Check the settings in the dialog box, and then click the **Next** button. Hitachi Command Suite Common Component and the port that receives SNMP traps will be added to the Windows Firewall exceptions list.

    Note

    If you register Global Link Manager as an exception in the Windows Firewall exceptions list, it might take approximately 15 minutes more to install Global Link Manager. If you enabled Windows Firewall after installing Global Link Manager, you must manually add Global Link Manager to the exceptions list. For details on how to manually add Global Link Manager to the exception list, see Settings for Windows firewalls on page 3-67.

11. Confirm that the displayed installation settings are correct, and then click the **Install** button.

    Installation starts. During the installation, dialog boxes indicating the processing status appear. The Global Link Manager database is not initialized by an overwrite installation (except when the database files are damaged). When the **HGLM Settings Complete** dialog box appears, confirm the settings you specified during installation.

    If a value specified for **URL for the HGLM login window** does not match the information on the server on which Global Link Manager is installed, see the appropriate reference below and change the value:

    - For details on how to change the IP address, see Changing the Global Link Manager login URL on page 3-64.
    - For details on how to change the host name, see Changing the Global Link Manager server host name on page 3-56.
    - For details on how to change the port number of HBase 64 Storage Mgmt Web Service, see Changing port numbers for accessing the HBase 64 Storage Mgmt Web Service on page 3-60.

12. Click the **Next** button.

    When installation has been completed normally, the **Installation Complete** dialog box appears.

13. Click the **Finish** button to finish the installation.

    The Hitachi Command Suite Common Component services are now offline.

14. If you want to use a function that outputs path availability information in a report and the storage destination for the report is not a shared disk, edit the property file (`server.properties`).

    The `server.properties` file is stored in the following location:

    `Global-Link-Manager-installation-folder``\conf`

    Change the folder for storing reports to a folder on the shared disk.

    For `server.pathreport.log_location`, specify an absolute path (maximum of 150 bytes) for the folder that stores reports. Deploy this folder on the shared disk. To use a backslash (`\`) as the path delimiter, you must use two consecutive backslashes.

    The following shows a coding example:

    ```
    server.pathreport.log_location=E:\\HGLAM\\pathreport
    ```

    For details about the settings in the property file for path availability information, see Changing Global Link Manager server settings on page 3-34.

15. If the port number that HiRDB uses was changed from the default and used in the environment before the upgrade installation or the overwrite installation was performed, reset the port number.

    If the version of Global Link Manager is v8 or earlier, the default (22032/tcp) is set for the port number that HiRDB uses. Therefore, if the port number that HiRDB uses was changed from the default and used, set the same port number as the port number that was used in the environment

before the upgrade installation or the overwrite installation was performed (that is, the port number written down in the above step).

Important: If Hitachi File Services Manager is used, set a port number different from the port number that was used in the environment before the upgrade installation or the overwrite installation was performed (that is, the port number written down in the above step).

16. Migrate the owner of the resource group who registered the Global Link Manager services from the primary node to the secondary node.

    If Microsoft Failover Cluster is used (on OSs other than Windows Server 2012):

    In Failover Cluster Management, right-click the resource group to which the services used by Global Link Manager have been registered, and then choose **Move this service or application to another node**.

    If Microsoft Failover Cluster is used (on Windows Server 2012):

    In Failover Cluster Manager, right-click the role to which the services used by Global Link Manager have been registered, choose **Move**, and then **Select Node**.

17. On the secondary node, perform an overwrite or upgrade installation of Global Link Manager.

    In the **Select Cluster Configuration** dialog box, select **Standby node** for **Cluster mode**. For the other items, specify the same values as the primary node.

18. Start operations for Global Link Manager in the cluster environment.

    For details, see Starting operations for Global Link Manager in a cluster environment on page 4-22.

Installing a Global Link Manager cluster for an existing installation

This section describes how to change to a cluster configuration after the Global Link Manager system operations have started in a non-cluster configuration. In this example, the instance of Global Link Manager whose operations are already running is treated as the primary node.

If you want to change the cluster configuration from a non-cluster configuration to a cluster configuration, you need to perform the following steps to set up a Global Link Manager cluster:

- On a primary node: steps 2, 7 and 8
- On a secondary node: step 10

Caution

- Note that this procedure uninstalls Global Link Manager. Any settings customizations that were performed before a migration to a cluster configuration must be performed again after performing the migration. Make sure you take note of the customized settings before migrating.

- When migrating Tuning Manager and Hitachi Automation Director to a cluster environment, the product data cannot be migrated.
- Before performing the procedure, make sure that the cluster management IP address and shared disk are enabled on the primary node. If they are not enabled, first perform the following procedures to place the resources of the cluster management IP address and shared disk online.

  Setting up Microsoft Failover Cluster on page 4-12
- Make sure that the structure of the Global Link Manager installation folder is the same for the primary and secondary nodes.
- If this procedure is performed, the default (22032) is set to the port number that HiRDB uses. Therefore, if you are using a port number other than the default to perform operations, you need to reset the port number later. Write down the port number you are using so that you can set the port number again.

1. Execute the following command to export the database. The databases for the Hitachi Command Suite product will be exported as a batch operation:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder
   \Base64\bin\hcmds64dbtrans /export /workpath work-folder /file
   archive-file
    /auto
   ```

   For *work-folder*, specify an absolute path for the folder that temporarily stores the database information. Specify an empty folder on the local disk. If you do not specify an empty folder, export processing will be interrupted, in which case you will need to specify an empty folder and then re-execute the `hcmds64dbtrans` command.

   For *archive-file*, specify an absolute path for the archive file of the database to be exported.

   When the `/auto` option is specified, the Hitachi Command Suite product services start or stop automatically.
2. If you have been using the function that outputs path availability information in a report, move the output path availability information (path status log) to a shared disk.

   To export the path availability information (path status log):

   Execute the following command:

   ```
   Global-Link-Manager-installation-folder\bin\hglamexport /dir
   export-destination-folder-name
   ```

   Use an absolute path to specify *export-destination-folder-name*. When you specify an existing folder, make sure that the folder is empty.

   The following characters can be used for *export-destination-folder-name*:

   `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), and underscore (`_`). You can also use a backslash (`\`), colon (`:`), and forward slash (`/`) as the path delimiter. If you specify a path that includes a space character, enclose the path in double quotation marks (`"`).

   The following shows an example of executing the command:

```
"C:\Program Files\HiCommand\HGLAM\bin\hglamexport" /dir "C:
\hglam export"
```

3. If you changed the port number used by HiRDB in a non-cluster environment to a value other than default (22032/tcp), take note of that port number.
4. Remove Global Link Manager.

   If other Hitachi Command Suite products (v8) are installed, remove them also.
5. Install Global Link Manager on the primary node.

   For details, see Installing Global Link Manager clusters for new installations on page 4-6.
6. Execute the following command to import the database:

   ```
   Hitachi-Command-Suite-Common-Component-installation-folder
   \Base64\bin\hcmds64dbtrans /import /workpath work-folder /file
   archive-file /type ALL /auto
   ```

   For *work-folder*, specify an absolute path for the folder in which the archive file will be expanded. Specify an empty folder on the local disk. If you do not specify an empty folder, import processing will be interrupted, in which case you will need to specify an empty folder and then re-execute the `hcmds64dbtrans` command. For *archive-file*, specify an absolute path for the archive file of the database information that was transferred from the migration source server.

   Note the following if you do not use the archive file:

   - For *work-folder*, specify the folder that stores the database information transferred from the migration source. Do not change the structure of files under the transferred folder.
   - Do not specify the `/file` option.

   For the `/type` option, specify ALL as a general rule.

   To import the Global Link Manager database, specify `/type HGLAM` or `/type GlobalLinkAvailabilityManager`.

   To import the databases of all installed Hitachi Command Suite products, including Global Link Manager, execute the command by specifying either `/type ALL` or the names of the Hitachi Command Suite products to be imported, which are separated by using a comma as the delimiter. For the names of other Hitachi Command Suite products that can be specified in the `/type` option, see the manuals for each product.

   If you specify `ALL` in the `/type` option, databases of the Hitachi Command Suite products installed on the migration destination are automatically selected and migrated. If you want to specify multiple products, the databases of all the specified products must exist in the folder specified by the archive file or the `/workpath` option, and all the specified products must be installed on the migration destination server. If any of the products do not meet the conditions above, migration will not be performed.

   Caution

- The import procedure depends on the Hitachi Command Suite products. To migrate databases of Hitachi Command Suite products other than Global Link Manager, see the documentation for those products.
- If Replication Monitor version 4.2 or earlier is installed on the migration source machine, you cannot migrate the database. Therefore, upgrade Replication Monitor on the migration source and migration destination machines to version 5.0 or later, and then perform migration. If Replication Monitor cannot be upgraded to version 5.0 or later, or the Replication Monitor database does not have to be migrated, use the `/type` option and specify all products other than Replication Monitor when you execute the command.

7. Edit the property file (`server.properties`).

   The `server.properties` file is stored in the following location:

   Global-Link-Manager-installation-folder\conf

   Change the folder for storing reports to a folder on the shared disk.

   For `server.pathreport.log_location`, specify an absolute path (maximum of 150 bytes) for the folder that stores reports. Deploy this folder on the shared disk. To use a backslash (\) as the path delimiter, you must use two consecutive backslashes.

   The following shows a coding example:

   ```
   server.pathreport.log_location=E:\\HGLAM\\pathreport
   ```

8. Import the path availability information (path status log).

   Execute the following command:

   Global-Link-Manager-installation-folder\bin\hglamimport /report *export-destination-folder-name*

   For *export-destination-folder-name*, use an absolute path to specify the folder in which the data exported by using the `hglamexport` command is stored.

   Caution

   If the folder is not empty, subfolders and files in the folder will be deleted.

   Before executing the command, you must either delete the folder that you specified in step 7 or make sure that the folder is empty.

9. Install Global Link Manager on the secondary node.

   For details, see Installing Global Link Manager clusters for new installations on page 4-6.

10. When you want to use a function that outputs path availability information in a report, edit the property file (`server.properties`).

    If you do not use a function that outputs path availability information in a report, you do not need to perform this step.

    The `server.properties` file is stored in the following location:

    Global-Link-Manager-installation-folder\conf

Change the folder for storing reports to a folder on the shared disk.

For `server.pathreport.log_location`, specify the folder for saving reports. Specify the same folder as the one specified on the primary node.

11. If you changed the port number used by HiRDB in a non-cluster environment to a value other than default (22032/tcp), see the note of the port number you took in step 3, and re-specify the port number for both the primary and the secondary nodes.
12. Start operations for Global Link Manager in the cluster environment.

    For details, see Starting operations for Global Link Manager in a cluster environment on page 4-22.

Removing a Global Link Manager cluster

This section describes the procedure for removing Global Link Manager in a cluster configuration.

To remove Global Link Manager in a cluster environment, perform the following operations on both the primary and secondary nodes.

If other Hitachi Command Suite products have already been installed on the same machine, the services of these products are also stopped when you stop Hitachi Command Suite Common Component.

To remove Global Link Manager in a cluster environment:

1. Display cluster software.

   Select **Start**, **Control Panel**, **Administrative Tools**, and then **Failover Cluster Management**.
2. For the resource group in which the services of Global Link Manager are registered, move the owner of the resource group from the secondary node to the primary node.

   If Microsoft Failover Cluster is used (on OSs other than Windows Server 2012):

   In Failover Cluster Management, right-click the resource group to which the services used by Global Link Manager have been registered, and then choose **Move this service or application to another node**.

   If Microsoft Failover Cluster is used (on Windows Server 2012):

   In Failover Cluster Manager, right-click the role to which the services used by Global Link Manager have been registered, choose **Move**, and then **Select Node**.
3. On the primary node, remove Global Link Manager.

   For details about removing Global Link Manager, see Removing Global Link Manager on page 2-28.
4. Migrate the owner of the resource group who registered the Global Link Manager services from the primary node to the secondary node.
5. On the secondary node, remove Global Link Manager.

6. If the following resources are not being used by another application, from the cluster management application, place the corresponding resource offline, and then delete it:
   - Cluster management IP address
   - Shared disk

   If the resource groups that have the Hitachi Command Suite product services registered are no longer necessary, delete those resource groups also.
7. Start operations for Global Link Manager in the cluster environment.

   For details, see Starting operations for Global Link Manager in a cluster environment on page 4-22.

Starting operations for Global Link Manager in a cluster environment

This section describes the procedures (such as registering licenses or turning the services online) for starting operations after the cluster configuration is completed.

When a new installation or migration from a non-cluster environment is performed

1. Make sure that the owner of the resource group who registered the Global Link Manager service is set as the name of the host for the secondary node. If the name is not the host for the secondary node, the owner is migrated from the primary node to the secondary node.
2. Execute the `hcmds64clustersrvstate` command and turn the resource group and the services of Global Link Manager product online.

   For details about the commands, see Turning a service online in the cluster management application on page 4-25.
3. In the secondary node, register the licenses of the product you are using from the GUI. Access the logical host name. You need to enter a license key for each product you are installing.

   For details about how to set licenses, see Setting up license information during initial login on page 2-30.
4. Migrate the owner of the resource group who registered the Hitachi Command Suite product services from the secondary node to the primary node.
5. In the primary node, register the licenses of the product you are using from the GUI. Access the logical host name. You need to enter a license key for each product you are installing.

   For details about how to set licenses, see Setting up license information during initial login on page 2-30.

When an upgrade, overwrite installation, or removal (keeping other Hitachi Command Suite products after the removal) is performed

1. Migrate the owner of the resource group who registered the Global Link Manager services from the secondary node to the primary node.

2. Execute the `hcmds64clustersrvstate` command and turn the resource group and the services of Hitachi Command Suite products online.
   For details about the commands, see Turning a service online in the cluster management application on page 4-25.

Global Link Manager services registered in a cluster environment

The following table lists the Global Link Manager services to be registered in cluster management applications on the management server.

Table 4-2 Global Link Manager services to be registered in cluster management applications on the management server

Program product	Displayed service name	Service name
Global Link Manager	HiRDB/ClusterService _HD1	HiRDBClusterService _HD1
	HBase 64 Storage Mgmt Web Service	HBase64StgMgmtWebService
	HBase 64 Storage Mgmt Web SSO Service	HBase64StgMgmtWebSSOService
	HBase 64 Storage Mgmt SSO Service	HBase64StgMgmtSSOService
	Global Link Manager Web Service	GlobalLinkManagerWebService

Note

For other Hitachi Command Suite product services, see the applicable manuals.

Commands used in a cluster environment

This section describes the commands that are used in a cluster environment.

Cluster setup utility

The cluster setup utility enables you to perform operations for the cluster management application.

When a resource is accidentally deleted from the cluster management application, or when the registration of a service fails during the installation, this utility can register or delete resources, or turn a service online or offline automatically in the cluster management application.

Registering a service to the cluster management application

To register Hitachi Command Suite product services to a resource group in the cluster management application, execute the following command:

Hitachi-Command-Suite-Common-Component-installation-folder
`\Base64\ClusterSetup\hcmds64clustersrvupdate /sreg /r` *resource-group-name* `/sd` *drive-letter-name* `/ap` *resource-name-set-as-a-client-access-point*

- `/sreg`

  Registers Hitachi Command Suite product services in the specified resource group.

- `/r`

  Specifies a resource group name. If a resource group name includes any of the following characters, use double quotation marks to enclose the resource group name.

  `, ; =` spaces

  In addition, you cannot use the following characters:

  `! " & ) * ^ | < >`

- `/sd`

  Specifies the drive name of the shared disk that is registered in the resource group.

  You cannot specify multiple drive names for this option. If Hitachi Command Suite product data is divided over multiple shared disks, execute the `hcmds64clustersrvupdate` command for each shared disk.

- `/ap`

  Specify the resource name that was set as a client access point.

Deleting a service from the cluster management application

To delete Hitachi Command Suite product services from the resource group in the cluster management application, execute the following command:

Hitachi-Command-Suite-Common-Component-installation-folder
`\Base64\ClusterSetup\hcmds64clustersrvupdate /sdel /r` *resource-group-name*

- `/sdel`

  Deletes Hitachi Command Suite product services from the specified resource group. Services of versions v7.x.x and v8.x.x are deleted.

- `/r`

  Specifies a resource group name. If a resource group name includes any of the following characters, use double quotation marks to enclose the resource group name.

  `, ; =` spaces

  In addition, you cannot use the following characters:

  `! " & ) * ^ | < >`

Caution

- In an environment in which Hitachi File Services Manager is installed, services used by Hitachi File Services Manager are not deleted.
- If any names are assigned for services that have been registered in the resource group, the names before the deletion cannot be retained. Assign the names again the next time you register services.

Turning a service online in the cluster management application

To turn Hitachi Command Suite product services that were registered to the cluster management application online, and to enable failovers, execute the following command:

Hitachi-Command-Suite-Common-Component-installation-folder`\Base64\ClusterSetup\hcmds64clustersrvstate /son /r` *resource-group-name*

- `/son`

  Places a resource group that has been configured in cluster management applications online and enables failover.

- `/r`

  Specifies a resource group name. If a resource group name includes any of the following characters, use double quotation marks to enclose the resource group name.

  `, ; =` spaces

  In addition, you cannot use the following characters:

  `! " & ) * ^ | < >`

Note

Before starting Automation Director in a cluster environment, complete the following:

- In the cluster management software, right-click to select the resource script and set its dependence on the [property]-[Dependencies] tab.
- In addition, specify [HAutomation Engine HCSclustergroup-name] to the resources that must be brought online before bringing the script online.

Turning a service offline in the cluster management application

To turn Hitachi Command Suite product services that were registered to the cluster management application offline, and to suppress failovers, execute the following command:

Hitachi-Command-Suite-Common-Component-installation-folder`\Base64\ClusterSetup\hcmds64clustersrvstate /soff /r` *resource-group-name*

- `/soff`

  Places the Hitachi Command Suite product services that have been configured in cluster management applications offline and suppresses a failover.

- `/r`

  Specifies a resource group name. If a resource group name includes any of the following characters, use double quotation marks to enclose the resource group name.

  `, ; =` spaces

  In addition, you cannot use the following characters:

  `! " & ) * ^ | < >`

5

Security settings for communication

This chapter describes the communication security settings that can be used to operate Global Link Manager.

Security settings for communication between a server and clients

When you use the Global Link Manager GUI to access a Global Link Manager server remotely via the Internet or an intranet, the interception or falsification of data by third parties becomes a risk. To protect your data, we recommend that you use SSL to encrypt your data.

To use SSL:

1. On the Global Link Manager server, set up SSL for HBase 64 Storage Mgmt Web Service.
2. In the Global Link Manager GUI, specify a URL that begins with `https://` as the URL used to log in to Global Link Manager.

HBase 64 Storage Mgmt Web Service supports TLS version 1.2.

Configuring HBase 64 Storage Mgmt Web Service for SSL Communication

HBase 64 Storage Mgmt Web Service uses a public key cryptosystem. Set up SSL on the server.

When using a certificate signed by a certificate authority (CA):

1. Generate a private key and a certificate signing request (CSR).
2. Send the CSR to the certificate authority (CA).
3. Obtain a certificate from the CA.
4. Edit the property file.
5. Restart Hitachi Command Suite Common Component.

When using a self-signed certificated:

1. Generate a private key, a certificate signing request (CSR), and a self-signed certificate.
2. Edit the property file.
3. Restart Hitachi Command Suite Common Component.

Generating a private key, a certificate signing request, and a self-signed certificate

Use the `hcmds64ssltool` command to create a private key and a certificate signing request (CSR) in Common Component.

The `hcmds64ssltool` command creates two types of private keys: certificate signing requests, and self-signed certificates supporting RSA ciphers and elliptic curve ciphers (ECC). The certificate signing request is created in PEM format. Although you can use this command to create a self-signed certificate, we recommend that you use a self-signed certificate only to test encrypted communications.

Operations to complete in advance

- Log in as a user with Administrator permissions.

Information to collect in advance

- Requirements for the certificate signing request (ask the certificate authority)
- Version of the Web browser used on the management client

  The signature algorithm of the server certificates must be supported by the Web browser used on the management client (GUI).
- Existing storage directories for private keys, certificate signing requests, and self-signed certificates (if you recreate them)

  If a file with the same name already exists in the output location, the command does not overwrite the file. Therefore, when you recreate a private key, certificate signing request, or self-signed certificate, you must output it to a directory other than existing storage directories.

Format of the command

- *installation-folder-for-Common-Component*\bin\hcmds64ssltool [/key *private-key-file*] [/csr *certificate-signing-request-file*] [/cert *self-signed-certificate-file*] [/certtext *contents-of-a-self-signed-certificate*] [/validity *number-of-valid-days*] [/dname *DN*] [/sigalg *signature-algorithm-for-server-certificate-for-RSA-cipher*] [/keysize *key-size-of-the-private-key-for-the-RSA-cipher*] [/eccsigalg *signature-algorithm-for-server-certificate-for-elliptic-curve-cipher*] [/ecckeysize *key-size-of-private-key-for-elliptic-curve-cipher*]

Options

key

Specify the absolute path to the location to which a private key will be output.

The private key for an RSA cipher is output with the specified file name. The private key for an elliptic curve cipher is output with a file name consisting of the prefix ecc- and the specified file name.

The httpsdkey.pem file and the ecc-httpsdkey.pem file are output if the option is omitted.#

csr

Specify the absolute path to the location to which the certificate signing request will be output.

The certificate signing request for an RSA cipher is output with the specified file name. The certificate signing request for an elliptic curve cipher is output with a file name consisting of the prefix ecc- and the specified file name.

The `httpsd.csr` file and the `ecc-httpsd.csr` file are output if the option is omitted.#

`cert`

Specify the absolute path to the location to which the self-signed certificate will be output.

The self-signed certificate for an RSA cipher is output with the specified file name. The self-signed certificate for an elliptic curve cipher is output with a file name consisting of the prefix `ecc-` and the specified file name.

The `httpsd.pem` file and the `ecc-httpsd.pem` file are output if the option is omitted.#

`certtext`

Specify the absolute path to the location to which the contents of the self-signed certificate will be output in text format.

The content of the self-signed certificate for an RSA cipher is output with the specified file name. The content of the self-signed certificate for an elliptic curve cipher is output with a file name consisting of the prefix `ecc-` and the specified file name.

The `httpsd.txt` file and the `ecc-httpsd.txt` file are output if the option is omitted.#

`validity`

Specify the number of days during which the self-signed certificate is valid. If this option is specified, the same content is specified for the RSA cipher and the elliptic curve cipher. If this option is omitted, the valid period is set to 3,650 days.

`dname`

specify the DN to be included in the self-signed certificate and certificate signing request. If you execute the command without specifying this option, you will be prompted to specify the DN.

To specify the DN, combine each attribute type with the corresponding attribute value into one attribute by using an equal sign (`=`), and then specify the attributes by separating each by a comma. For the DN, you cannot specify a double quotation mark (`"`) or backslash (`\`). In addition, specify each attribute value as defined by RFC2253. For example, if the specified DN includes any of the following characters, escape each of them by using a backslash (`\`).

A space at the beginning of or at the end of the DN

A hash mark (`#`) at the beginning of the DN

A plus sign (`+`), comma (`,`), semicolon (`;`), left angle bracket (`<`), equal sign (`=`), or right angle bracket (`>`)

The following table lists and describes the attribute types and values specified for the DN.

Table 5-1 Attribute types and values specified for the DN (hcmds64ssltool)

Attribute type	Full name of attribute type	Attribute value
CN	Common Name	Specify the host name of the management server (HBase 64 Storage Mgmt Web Service). This attribute is required. Specify the host name used when connecting to the management server (HBase 64 Storage Mgmt Web Service of Common Component) from the management client (GUI). You can also specify the host name in FQDN format. If the management server is running in a cluster environment, specify the logical host name.
OU	Organizational Unit Name	Specify the name of the organizational unit.
O	Organization Name	Specify the organizational name. This attribute is required.
L	Locality Name	Specify the name of the city, town, or other locality.
ST	State or Province Name	Specify the name of the state or province.
C	Country Name	Specify the two-letter country code.

`sigalg`

Specify a signature algorithm for the server certificate for the RSA cipher. You can specify `SHA1withRSA`, `SHA256withRSA` or `SHA512withRSA`. If you omit this specification, SHA256withRSA is used as the signature algorithm.

`keysize`

Specify the size of the private key for the RSA cipher in bits. The specifiable values are `2048`, `3072`, and `4096`. If this option is not specified, the key size is 2048 bits.

The size of a private key for an RSA cipher is 2,048 bits (fixed).

`eccsigalg`

Specify a signature algorithm for the server certificate for the elliptic curve cipher. You can specify `SHA512withECDSA`, `SHA384withECDSA`, `SHA256withECDSA`, or `SHA1withECDSA`. If you omit this specification, SHA384withECDSA is used as the signature algorithm.

`ecckeysize`

Specify the size of the private key for the elliptic curve cipher in bits. The specifiable values are `256` and `384`. If this option is not specified, the key size is 384 bits.

#

If this option is not specified, the file is output to the following location:

- *Hitachi-Command-Suite-Common-Component-installation-folder* `\uCPSB\httpsd\conf\ssl\server\`

Applying to a certificate authority for a Common Component server certificate

Send the Common Component certificate signing request (CSR) that you created to a certificate authority to be digitally signed.

Operations to complete in advance

- Create a certificate signing request for Common Component.

Information to collect in advance

- How to apply to the certificate authority and what they support

  You need to have a server certificate issued in X.509 PEM format. For details about how to apply for a certificate, check the website of the certificate authority you will use.

  In addition, make sure that the certificate authority supports the signature algorithm.

To apply to a certificate authority for a Common Component server certificate:

1. Send the created certificate signing request to a certificate authority.

Make sure that you save the response from the certificate authority.

Note: Certificates issued by a certificate authority have an expiration date. You need to have a certificate reissued before your certificate expires. To check the expiration date, use the `hcmds64checkcerts` command.

Editing the user_httpsd.conf file to enable SSL/TLS

To enable SSL/TLS for Common Component or change the host name or port number of a management server, edit the `user_httpsd.conf` file.

Operations to complete in advance

- Create a private key for Common Component (required for enabling SSL/TLS).#
- Prepare a server certificate for Common Component (required for enabling SSL/TLS).#

Prepare the server certificate sent back from the certificate authority. When testing encrypted communications, you can use a self-signed certificate.

#:

We recommend that you copy the files into the following location.

Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\httpsd\conf\ssl\server

Information to collect in advance

- Host name specified for `Common Name` in the certificate signing request (required for enabling SSL/TLS).

To edit the user_httpsd.conf file:

1. Stop the services of the Hitachi Command Suite product.
2. Edit the `user_httpsd.conf` file.
3. Start the services of Hitachi Command Suite product.

Storage location of the `user_httpsd.conf` file

- *Hitachi-Command-Suite-Common-Component-installation-folder*\uCPSB\httpsd\conf\user_httpsd.conf

Example of the `user_httpsd.conf` file (default)

```
ServerName host-name          ●———— Host name of the management server
#Listen [::]:22015            ●———— Port number for non-SSL communication (for IPv6 environments)
Listen 22015                  ●———— Port number for non-SSL communication
#Listen 127.0.0.1:22015
SSLDisable
#Listen [::]:22016            ●———— Port number for SSL communication (for IPv6 environments)
#Listen 22016                 ●———— Port number for SSL communication
#<VirtualHost *:22016>        ●———— Port number for SSL communication
#  ServerName host-name       ●———— Host name of the management server
#  SSLEnable
#  SSLProtocol TLSv12
#  SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-GCM-SHA256
#  SSLRequireSSL
#  SSLCertificateKeyFile "installation-folder-for-Hitachi-Command-Suite-Common-
Component/uCPSB/httpsd/conf/ssl/server/httpsdkey.pem"
#  SSLCertificateFile "installation-folder-for-Hitachi-Command-Suite-Common-
Component/uCPSB/httpsd/conf/ssl/server/httpsd.pem"
#  SSLECCCertificateKeyFile "installation-folder-for-Hitachi-Command-Suite-
Common-Component/uCPSB/httpsd/conf/ssl/server/ecc-httpsdkey.pem"
#  SSLECCCertificateFile "installation-folder-for-Hitachi-Command-Suite-Common-
Component/uCPSB/httpsd/conf/ssl/server/ecc-httpsd.pem"
#  SSLCACertificateFile "installation-folder-for-Hitachi-Command-Suite-Common-
Component/uCPSB/httpsd/conf/ssl/cacert/anycert.pem"
#</VirtualHost>
#HWSLogSSLVerbose On
```

Note: For a non-cluster environment, make sure that the host name specified for `ServerName` at the beginning of the `user_httpsd.conf` file is entered for

VirtualHost and ServerName in the user_httpsd.conf file. If you changed the host name, you also need to change the settings of VirtualHost and ServerName (two places). For a cluster environment, make sure that the name specified for VirtualHost and ServerName is the same as the logical host name specified for virtualhost in the cluster.conf file. The logical host name to be specified for VirtualHost and ServerName is case sensitive.

Enabling SSL/TLS

To enable SSL:

If other Hitachi Command Suite products have already been installed on the same machine, the services of these products are also started or stopped at the same time when you start or stop Hitachi Command Suite Common Component. Note, however, that if the version of one (or more) of these other Hitachi Command Suite products is earlier than 5.7, you will need to manually start or stop the services of that product (or products). For details on how to start and stop the services of other Hitachi Command Suite products, see the manual for each product.

1. Execute the following command to stop Hitachi Command Suite Common Component:
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /stop

2. Copy the private key file and either the signed certificate file returned by the CA or the self-signed certificate file to the appropriate folder.
   We recommend that you copy these two files to the following folder:
   Hitachi-Command-Suite-Common-Component-installation-folder\uCPSB\httpsd\conf\ssl\server

3. Open the user_httpsd.conf file.
4. Make the directives for the SSL port and host name effective, by deleting the hash mark (#) at the beginning of the corresponding lines.
5. In SSLCertificateFile, specify the absolute path of either the certificate file returned by the CA or the self-signed certificate file.
6. In SSLCertificateKeyFile, specify the absolute path name of the private key file for the Web server.
7. To use a certificate issued by a chained CA, in SSLCACertificateFile, specify the absolute path name of the certificate file of the chained CA.
   Multiple PEM format certificates can be contained in one file by chaining multiple certificate files by using a text editor.
8. Execute the following command to start Hitachi Command Suite Common Component:
   Hitachi-Command-Suite-Common-Component-installation-folder\bin\hcmds64srv /start

The figure below shows an example of enabling SSL/TLS. In this example, the signed certificate (httpsd.pem) returned by the CA and the private key

(`httpsdkey.pem`) are stored in the folder *installation-folder-for-Common-Component*/`uCPSB/httpsd/conf/ssl/server`.

Note

A line that begins with a hash mark (#) is a comment line.

Settings required for enabling SSL/TLS

Note: When editing directives, be careful of the following:

- Do not specify the same directive twice.
- Do not enter a line break in the middle of a directive.
- Do not specify symbolic links or junctions in the paths specified for each directive.
- Specify a PEM file for the certificate and private key file specified for each directive.
- Do not edit the `httpsd.conf` and `hsso_httpsd.conf` files.

- Remove the hash mark (#) at the beginning of the following lines:

  If you use the RSA cipher only, you do not need to remove the hash mark (#) at the beginning of the lines for the `SSLECCCertificateKeyFile` directive and the `SSLECCCertificateFile` directive.

```
ServerName host-name
#Listen [::]:22015
Listen 22015
#Listen 127.0.0.1:22015
SSLDisable
#Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
  ServerName host-name
  SSLEnable
  SSLProtocol TLSv12
  SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-
SHA256:AES256-GCM-SHA384:AES128-GCM-SHA256
  SSLRequireSSL
  SSLCertificateKeyFile "installation-folder-for-Hitachi-Command-
Suite-Common-Component/uCPSB/httpsd/conf/ssl/server/httpsdkey.pem"
  SSLCertificateFile "installation-folder-for-Hitachi-Command-Suite-
Common-Component/uCPSB/httpsd/conf/ssl/server/httpsd.pem"
  SSLECCCertificateKeyFile "installation-folder-for-Hitachi-Command-
Suite-Common-Component/uCPSB/httpsd/conf/ssl/server/ecc-httpsdkey.pem"
  SSLECCCertificateFile "installation-folder-for-Hitachi-Command-
Suite-Common-Component/uCPSB/httpsd/conf/ssl/server/ecc-httpsd.pem"
#  SSLCACertificateFile "installation-folder-for-Hitachi-Command-
Suite-Common-Component/uCPSB/httpsd/conf/ssl/cacert/anycert.pem"
</VirtualHost>
HWSLogSSLVerbose On
```

Remove the hash mark (#) from the beginning of each of these 13 lines.

- For the `ServerName` directive on the top line and the `ServerName` directive within the `<VirtualHost>` tag, specify the host name (for cluster environments, specify the logical host name) that you specified for `Common Name` in the certificate signing request. Note that host names are case sensitive.

- For the `SSLCertificateKeyFile` directive, specify the absolute path to the private key file for Common Component for the RSA cipher.
- For the `SSLCertificateFile` directive, specify the absolute path of the server certificate for Common Component for the RSA cipher.
- For the `SSLECCCertificateKeyFile` directive, specify the absolute path to the private key file for the Common Component instance for the elliptic curve cipher. This setting is unnecessary if you use the RSA cipher only.
- For the `SSLECCCertificateFile` directive, specify the absolute path of the server certificate for the Common Component instance for the elliptic curve cipher. This setting is unnecessary if you use the RSA cipher only.
- If the certificate authority that issued the server certificate of the Common Component was an intermediate certificate authority, remove the hash mark (`#`) from the beginning of the line for the `SSLCACertificateFile` directive, and then specify the absolute path of all the intermediate certificate authorities. Multiple certificates can be contained in one file by chaining multiple PEM format certificates by using a text editor.
- For an IPv6 environment, remove the hash mark (`#`) at the beginning of the lines `#Listen [::]:22016`.

Note:

- Even if you enable SSL or use Global Link Manager in an IPv6 environment, do not remove or comment out the line `Listen 22015`.

  To interrupt non-SSL communication from outside the network to the management server, add a hash mark (`#`) at the beginning of the lines `Listen [::]:22015` and `Listen 22015` to comment them out, and then remove the hash mark at the beginning of the line `#Listen 127.0.0.1:22015`. In this case, if the system is linked with Hitachi File Services Manager or Storage Navigator Modular 2, execute the `hcmdsprmset` command for Hitachi File Services Manager or Storage Navigator Modular 2 with the `print` option specified, and then confirm that the output host name can be resolved to 127.0.0.1. If name resolution cannot be performed, specify the environment settings of the OS so that name resolution can be performed. If name resolution still cannot be performed, set a host name of your choice and 127.0.0.1 for the `hosts` file, and then execute the `hcmdsprmset` command by specifying the host name you set for the `hosts` file for the `host` option.

  If you want to close the port for non-SSL communication that is used for communication in the management server, set the port for non-SSL communication of HBase 64 Storage Mgmt Web Service to closed.
- The content of the elliptic curve cipher is not applied in the `user_httpsd.conf` file if Hitachi Command Suite is upgraded from version 8.2.1 or earlier. If you use the elliptic curve cipher, copy and use the contents of the `SSLRequiredCiphers`, `SSLECCCertificateKeyFile`, and `SSLECCCertificateFile` directives from the sample file stored in the location shown below.

Hitachi-Command-Suite-Common-Component-installation-folder\sample\httpsd\conf\user_httpsd.conf

- If the system is linked with Hitachi File Services Manager or Storage Navigator Modular 2, when you enable SSL/TLS, edit the `httpsd.conf` file that is stored in the following location.

  installation-folder-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2\Base\httpsd\conf\httpsd.conf

  For details on how to edit the file, see the manual for either Hitachi File Services Manager or Storage Navigator Modular 2.

Tip: To disable SSL/TLS, by referencing the example of the `user_httpsd.conf` file (default), add a hash mark (#) at the beginning of the lines from `Listen 22016` to `HWSLogSSLVerbose On` to comment them out.

Disabling SSL

To disable SSL, comment out the directives for the SSL port and host in the `user_httpsd.conf` file. Before editing the `user_httpsd.conf` file, stop other Hitachi Command Suite product services and Hitachi Command Suite Common Component. After the editing is complete, restart Hitachi Command Suite Common Component.

The following table shows an example of disabling SSL.

Note

A line that begins with a hash mark (#) is a comment line.

Table 5-2 Disabling SSL

```
ServerName www.example.com
#Listen [::]:22015
Listen 22015
#Listen 127.0.0.1:22015
SSLDisable
#Listen [::]:22016
#Listen 22016
#<VirtualHost *:22016>
#  ServerName www.example.com
#  SSLEnable
#  SSLProtocol TLSv12
#  SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-GCM-SHA256
#  SSLRequireSSL
#  SSLCertificateKeyFile C:/Program Files/HiCommand/Base64/uCPSB/httpsd/
conf/ssl/server/httpsdkey.pem
#  SSLCertificateFile C:/Program Files/HiCommand/Base64/uCPSB/httpsd/conf/ssl/
server/httpsd.pem
#  SSLECCCertificateKeyFile C:/Program Files/HiCommand/Base64/uCPSB/httpsd/
conf/ssl/server/ecc-httpsdkey.pem
#  SSLECCCertificateFile C:/Program Files/HiCommand/Base64/uCPSB/httpsd/
conf/ssl/server/ecc-httpsd.pem
#  SSLCACertificateFile C:/Program Files/HiCommand/Base64/uCPSB/httpsd/
conf/ssl/cacert/anycert.pem
#</VirtualHost>
#HWSLogSSLVerbose On
```

Changing a port number assigned to SSL

The default port of SSL for HBase 64 Storage Mgmt Web Service is 22016. To change the port, change the `Listen` directive and the port number of the host in the `user_httpsd.conf` file. Before editing the `user_httpsd.conf` file, stop other Hitachi Command Suite product services and Hitachi Command Suite Common Component. After the editing is complete, restart Hitachi Command Suite Common Component.

Closing the port for the non-SSL communication (HBase 64 Storage Mgmt Web Service)

To close the port for non-SSL communication for HBase 64 Storage Mgmt Web Service (default: 22015) that is used for communication in the management server, edit the `user_httpsd.conf` file, and then import the certificate to the truststore (`jssecacerts`).

Operations to complete in advance

- Checking the host name

  Make sure that the host name specified for `Common Name` in the server certificate is the same as the host name set to the `ServerName` directive at the beginning of the `user_httpsd.conf` file.
- Name resolution settings

  Make sure that name resolution can be performed from the host name (the host name of the management server) that is set to the `ServerName` directive at the beginning of the `user_httpsd.conf` file to the IP address. To do this, execute the following command on the management server.

  `ping` *`host-name-of-the-management-server`*
- Enabling SSL/TLS for Common Component

To close the port of the non-SSL communication for HBase 64 Storage Mgmt Web Service:

1. Stop the services of the Hitachi Command Suite product.
2. Edit the `user_httpsd.conf` file to comment out the non-SSL communication port settings.

   Add a hash mark (`#`) to the beginning of the line below to turn it into a comment. The following example shows the locations for where to add hash marks (`#`). This example indicates the default port number.

```
ServerName host-name
#Listen [::]:22015
#Listen 22015
#Listen 127.0.0.1:22015
SSLDisable
#Listen [::]:22016
Listen 22016
#<VirtualHost *:22016>
#  ServerName host-name
  SSLEnable
  SSLProtocol TLSv12
  SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-
AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-
SHA256:AES256-GCM-SHA384:AES128-GCM-SHA256
  SSLRequireSSL
  SSLCertificateKeyFile "installation-folder-for-Hitachi-Command-
Suite-Common-Component/uCPSB/httpsd/conf/ssl/server/httpsdkey.pem"
  SSLCertificateFile "installation-folder-for-Hitachi-Command-Suite-
Common-Component/uCPSB/httpsd/conf/ssl/server/httpsd.pem"
  SSLECCCertificateKeyFile "installation-folder-for-Hitachi-Command-
Suite-Common-Component/uCPSB/httpsd/conf/ssl/server/ecc-
httpsdkey.pem"
  SSLECCCertificateFile "installation-folder-for-Hitachi-Command-
Suite-Common-Component/uCPSB/httpsd/conf/ssl/server/ecc-httpsd.pem"
#  SSLCACertificateFile "installation-folder-for-Hitachi-Command-
Suite-Common-Component/uCPSB/httpsd/conf/ssl/cacert/anycert.pem"
#</VirtualHost>
HWSLogSSLVerbose On
```

Add the leading hash mark (#).

The `user_httpsd.conf` file is stored in the following locations:

Hitachi-Command-Suite-Common-Component-installation-folder
`\uCPSB\httpsd\conf\user_httpsd.conf`

Note: Do not edit the `httpsd.conf` file.

3. Import the certificate to the truststore (`jssecacerts`).
4. Make sure that the certificate is imported to the truststore.
5. Start the services of Hitachi Command Suite product.

Security settings for communication between a server and an LDAP directory server

In Hitachi Command Suite products, when performing user authentication by linking with an LDAP directory server, you can encrypt network transmissions between Common Component and the LDAP directory server by using StartTLS. To use StartTLS to protect communications between the management server and LDAP directory server, you need to perform the following operations:

- Obtain a certificate for the LDAP directory server
- Import the certificate into the truststore file

To encrypt network transmissions between Common Component and an LDAP directory server, you also need to set up the `exauth.properties` file. For

details on how to do this, see Setting the exauth.properties file (when the authentication method is LDAP) on page 3-92.

Caution

The CN of the certificate for the LDAP directory server must be the same as the value specified for the `auth.ldap.`*value-specified-for-auth.server.name*`.host` property in the `exauth.properties` file (the host name used to access the LDAP directory server).

Obtaining a certificate for the LDAP directory server

Obtain a server certificate for the LDAP directory server that communicates with the management server. For details, see the documentation for the LDAP directory server you use.

If you have obtained a certificate for the LDAP directory server from a well-known CA, the CA certificate might already be set up in the standard truststore referenced by Common Component. Execute the command below to check this. If the certificate for the LDAP directory server is authenticated by the already-registered CA certificate, you do not need to set up the truststore `jssecacerts` explained in section Importing the certificate to the truststore file on page 5-15.

```
hcmds64keytool -list -v -keystore truststore-file-name -storepass
password-to-access-the-truststore
```

- `-keystore` *truststore-file-name* specifies the truststore file to be referenced.

```
installation-folder-for-Common-Component\jdk\jre\lib\security\cacerts
```

- `-storepass` *password-to-access-the-truststore* specifies the password used to reference the truststore `cacerts`. The default is `changeit`.

The following shows an example of executing the command:

```
"C:\Program Files\HiCommand\Base64\jdk\bin\hcmds64keytool" -list -v -
keystore "C:\Program Files\HiCommand\Base64\jdk\jre\lib\security
\cacerts" -storepass changeit
```

Cautions

- Do not import and use your own certificate into the truststore `cacerts` because that truststore is updated when Common Component is upgraded.
- Server certificates issued by certificate authorities have expiration dates. Make sure that the certificates are not expired.

  For details about how to check the expiration date for a server certificate, see Checking the certificate expiration date on page 5-27.

Importing the certificate to the truststore file

Import the certificate for the LDAP directory server into the truststore used by Common Component. Store that truststore (`jssecacerts`) in the locations shown below. If no truststore file exists, create a truststore file.

```
installation-folder-for-Common-Component\uCPSB\jdk\jre\lib\security
\jssecacerts
```

To create a truststore file, import a certificate, and check the contents, use the `hcmds64keytool` utility. This utility is stored in the following location:

```
installation-folder-for-Common-Component\bin\hcmds64keytool.exe
```

To create a truststore file and import a certificate, execute the following command:

```
hcmds64keytool -import -alias unique-name-in-the-truststore -file
certificate-file -keystore truststore-file-name -storepass password-
to-access-the-truststore
```

- `-alias` *unique-name-in-the-truststore* specifies the name used to identify the certificate in the truststore
- `-file` *certificate-file* specifies the certificate file.
- `-keystore` *truststore-file-name* specifies `jssecacerts`, which is the truststore file to be registered and created.
- `-storepass` *password-to-access-the-truststore* specifies the password used to access the truststore (`jssecacerts`).

For example, to use the `hcmds64keytool` utility to import a certificate file when the certificate file is `C:\tmp\ldapcert.der`, the password to access the truststore is `changeit`, and the unique name in the truststore is `ldaphost`, you would execute the command as shown below.

```
"C:\Program Files\HiCommand\Base64\jdk\bin\hcmds64keytool" -import -
alias ldaphost -file C:\tmp\ldapcert.der -keystore "C:\Program Files
\HiCommand\Base64\uCPSB\jdk\jre\lib\security\jssecacerts" -storepass
changeit
```

To view the contents of the truststore, execute the following command:

```
hcmds64keytool -list -v -keystore truststore-file-name -storepass
password-to-access-the-truststore
```

- `-keystore` *truststore-file-name* specifies `jssecacerts`, which is the truststore file to be registered and created.
- `-storepass` *password-to-access-the-truststore* specifies the password used to update the truststore `jssecacerts`.

```
"C:\Program Files\HiCommand\Base64\jdk\bin\hcmds64keytool" -list -v -
keystore "C:\Program Files\HiCommand\Base64\uCPSB\jdk\jre\lib
\security\jssecacerts" -storepass changeit
```

Note that, to apply the truststore, you need to restart the Hitachi Command Suite product services and Common Component.

Cautions

- If there is more than one certificate file, import a certificate file by specifying an alias name that is not used in `jssecacerts`.
- Note the following when you use the `hcmds64keytool` utility to specify a unique name in the truststore, the truststore file name, and the password:
  - Do not use the following symbols in the file name:
    `: , ; * ? " < > |`
  - Specify the file name as a character string of no more than 255 bytes.
  - Do not include double quotation marks (") in the unique name in the truststore or the password.
- For closing the port (default: 20315) for the non-SSL communication of HBase 64 Storage Mgmt Web Service

  When using a certificate authority:

  The certificates issued by all the authorities from the authority which issued the Common Component server certificate to the root certificate authority must form a certificate chain

  When using a self-signed certificate:

  Obtain a Common Component self-signed certificate.

Security settings for communication between a server and HDLM

To perform SSL communication with an HDLM host, use the HDLM host's Hitachi Command Suite Common Agent Component as an SSL server. To use Hitachi Command Suite Common Agent Component as an SSL server, you need to prepare a key pair and server certificate.

The requirements for using Hitachi Command Suite Common Agent Component as an SSL server are shown below.

Host requirements

- The version of the HDLM must be 8.5.0 or later.
- If you use the Oracle or IBM JRE, you need to install the Java Cryptography Extension (JCE) unlimited strength jurisdiction policy files that correspond to the JRE version you are using.

Obtain the jurisdiction policy files from either Oracle's or IBM's website. For the installation method, see the documentation that comes with the jurisdiction policy files.

Cautions

JRE versions for both Windows and Linux come bundled with Hitachi Command Suite Common Agent Component.

However, the bundled JRE versions for Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, SUSE Linux Enterprise Server 11, Oracle Linux 6, and Oracle Unbreakable Enterprise Kernel 6 do not support the default encryption method specified in the `server.agent.ciphers` property of `server.properties`. To use a server running Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, SUSE Linux Enterprise Server 11, Oracle Linux 6, or Oracle Unbreakable Enterprise Kernel 6 as an SSL server, you need to use Oracle's JRE. For details on the usable Oracle JRE, see the HDLM manual. Note that a JRE that supports IPF machines has not been released, so a Linux IPF machine cannot be used as an SSL server.

Change the value of the `server.agent.JRE.location` property in Hitachi Command Suite Common Agent Component's `server.properties` file according to the JRE you are using.

Creating a key pair and a certificate signing request for Hitachi Command Suite Common Agent Component

To create a key pair and a self-signed certificate from the HDLM host machine, use the `hbsa_ssltool` command. A certificate signing request and self-signed certificate are created with a private key size of 2,048 bits, the key algorithm RSA, and the signature algorithm SHA256withRSA. Although you can use this command to create a self-signed certificate, we recommend that you use a self-signed certificate only to test encrypted communications.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX)
- Delete an existing keystore file of Hitachi Command Suite Common Agent Component (if you re-create the file)

  Hitachi Command Suite Common Agent Component can create only one keystore file.

Format of the command

In Windows:

```
installation-folder-for-Hitachi-Command-Suite-Common-Agent-
Component\bin\hbsa_ssltool.bat -key keystore-file-name -csr
certificate-signing-request-file -keypass private-keypassword
-storepass keystore-password [-cert self-signed-certificate-
```

file] [-validity *number-of-valid-days*] [-dname *entity-distinguished-name*]

Note: If the VMware edition of HDLM is used, execute the command from the Windows operating system running on the remote management client.

In UNIX:

installation-directory-for-Hitachi-Command-Suite-Common-Agent-Component/bin/hbsa_ssltool.sh -key *keystore-file-name* -csr *Ccertificate-signing-request-file* -keypass *private-keypassword* -storepass *keystore-password* [-cert *self-signed-certificate-file*] [-validity *number-of-valid-days*] [-dname *entity-distinguished-name*]

Options

`key`

Specify the absolute path to the location to which a keystore file will be output. If you specify a path including a space, enclose it in double quotation marks (`"`). If you are using Windows, specify a forward slash (`/`) as the path delimiter. Specify a string within 255 bytes. The following special characters cannot be specified:

: , ; * ? " < > | -

`csr`

Specify the absolute path to the location to which the certificate signing request will be output. If you specify a path including a space, enclose it in double quotation marks (`"`). If you are using Windows, specify a forward slash (`/`) as the path delimiter. Specify a string within 255 bytes. The following special characters cannot be specified:

: , ; * ? " < > | -

`keypass`

Specify a private key password that is at least six characters long. Specify the same password for both the `keypass` option and the `storepass` option. If you specify a path including a space, enclose it in double quotation marks (`"`). Specify the password using any of the following half-width characters:

A - Z, a - z, 0 - 9, space

`storepass`

Specify a keystore password that is at least six characters long. Specify the same password for both the `storepass` option and the `keypass` option. If you specify a path including a space, enclose it in double quotation marks (`"`). Specify the password using any of the following half-width characters:

A - Z, a - z, 0 - 9, space

`cert`

Specify the absolute path to the location to which the self-signed certificate will be output. If you specify a path including a space, enclose it in double quotation marks ("). If you are using Windows, specify a forward slash (/) as the path delimiter. Specify a string within 255 bytes. The following special characters cannot be specified:

: , ; * ? " < > | -

`validity`

Specify the number of days during which the self-signed certificate is valid. If this option is omitted, the valid period is set to 3,650 days.

`dname`

specify the DN to be included in the self-signed certificate and certificate signing request. If you execute the command without specifying this option, you will be prompted to specify the DN.

To specify the DN, combine each attribute type with the corresponding attribute value into one attribute by using an equal sign (=), and then specify the attributes by separating each by a comma. For the DN, you cannot specify a double quotation mark (") or backslash (\). In addition, specify each attribute value as defined by RFC2253. For example, if the specified DN includes any of the following characters, escape each of them by using a backslash (\).

A space at the beginning of or at the end of the DN

A hash mark (#) at the beginning of the DN

A plus sign (+), comma (,), semicolon (;), left angle bracket (<), equal sign (=), or right angle bracket (>)

The following table lists and describes the attribute types and values specified for the DN.

Table 5-3 Attribute types and values specified for the DN (hbsa_ssltool)

Attribute type	Full name of attribute type	Attribute value
CN	Common Name	Specify the host name of the management server (HBase 64 Storage Mgmt Web Service). This attribute is required. Specify the host name used when connecting to the management server (HBase 64 Storage Mgmt Web Service of Common Component) from the management client (GUI). You can also specify the host name in FQDN format. If the management server is running in a cluster environment, specify the logical host name.
OU	Organizational Unit Name	Specify the name of the organizational unit.

Attribute type	Full name of attribute type	Attribute value
O	Organization Name	Specify the organizational name. This attribute is required.
L	Locality Name	Specify the name of the city, town, or other locality.
S	State or Province Name	Specify the name of the state or province.
C	Country Name	Specify the two-letter country code.

Applying to a certificate authority for a Hitachi Command Suite Common Agent Component server certificate

Usually, you can apply to a certificate authority for a server certificate online. Send the Hitachi Command Suite Common Agent Component certificate signing request (CSR) that you created to a certificate authority to be digitally signed.

Before you begin

- Create a certificate signing request for Hitachi Command Suite Common Agent Component.
- Check the following information:
  - How to apply to the certificate authority and what they support

    Make sure that the certificate authority you use supports signatures using SHA256withRSA. For details about how to apply for a certificate, check the website of the certificate authority you will use.

Procedure

1. Send the created certificate signing request to a certificate authority.

Result

Usually, server certificates issued by a certificate authority are sent via email. Make sure that you save the response from the certificate authority.

Note: Certificates issued by a certificate authority have an expiration date. You need to have a certificate reissued before your certificate expires.

Importing the Hitachi Command Suite Common Agent Component server certificates into the keystore

To import the server certificates into the Hitachi Command Suite Common Agent Component keystore, use the `keytool` utility.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX)
- Obtain certificates for certificate authorities.

  Prepare the certificates for all certificate authorities including the certificate authority that issued the certificate, intermediate certificate authorities, and the root certificate authority.
- Obtain a Hitachi Command Suite Common Agent Component server certificate issued by a certificate authority.
- Check the following information:
  - Information of the keystore file

    You need the information of the keystore file prepared when creating a self-signed certificate.

    - Absolute path

    - Access password

Procedure

1. Execute the following command to import a certificate of a certificate authority or a certificate of the Hitachi Command Suite Common Agent Component server.

   Execute the command for each certificate.

   In Windows:

   ```
   installation-folder-for-Hitachi-Command-Suite-Common-Agent-Component\bin\hbsa_keytool.bat -import -alias alias -keystore keystore-file-name -file certificate-file-name
   ```

   Note: If the VMware edition of HDLM is used, execute the command from the Windows operating system running on the remote management client.

   In UNIX:

   ```
   installation-directory-for-JDK-or-JRE/bin/keytool -import -alias alias -keystore keystore-file-name -file certificate-file-name
   ```

   - `alias`: Specify the name used to identify the certificate in the keystore.
   - `keystore`: Specify the keystore file by using an absolute path.
   - `file`: Specify the file name of the certificate by using an absolute path.

Enabling SSL/TLS in Hitachi Command Suite Common Agent Component

To enable SSL/TLS, you need to set `server.properties` in Hitachi Command Suite Common Agent Component on the HDLM host.

Refer to Changing the settings of Hitachi Command Suite Common Agent Component on page A-3, and set the following properties as necessary:

- `server.https.port`
- `server.agent.secure`
- `server.agent.ciphers`

Checking a Hitachi Command Suite Common Agent Component server certificate

Use the `keytool` utility to check the Hitachi Command Suite Common Agent Component server certificate. The server certificate has an expiration date. Make sure that the certificate is not expired.

Procedure

1. Execute the following command:

   In Windows:

   installation-folder-for-Hitachi-Command-Suite-Common-Agent-Component\bin\hbsa_keytool.bat -printcert -v -file *certificate-file-name*

   Note: If the VMware edition of HDLM is used, execute the command from the Windows operating system running on the remote management client.

   In UNIX:

   installation-directory-for-JDK-or-JRE/bin/keytool -printcert -v -file *certificate-file-name*

Registering firewall exceptions

Register the port number used by Hitachi Command Suite Common Agent Component as a firewall exception. For information about how to register a firewall exception, see Changing firewall settings for HDLM on page A-2.

Security settings for communication between a server and Device Manager

To perform SSL communication with Device Manager, use Device Manager server as an SSL server.

For details on how to set up Device Manager server as an SSL server, see the *Hitachi Command Suite Administrator Guide*.

Configuring an SSL client

To perform SSL communication with an HDLM host or Device Manager server, you need to import the server certificate created by an SSL server into an SSL client (Global Link Manager server).

Caution

After you perform the following operations, you must restart Global Link Manager.

- Importing a certificate into the Global Link Manager server truststore on page 5-23
- Deleting a server certificate imported into the truststore for the Global Link Manager server on page 5-25

If you perform both operations, you do not need to restart Global Link Manager after each operation. You can restart Global Link Manager after you perform both operations.

Checking the certificate for the HDLM host or Device Manager server

Use the `hglamkeytool` utility to check the server certificate for the HDLM host or Device Manager server. The server certificate has an expiration date. Make sure that the certificate is not expired.

Procedure

1. Execute the following command:
   installation-folder-for-Hitachi-Global-Link-Manager\bin\hglamkeytool.bat -printcert -v -file *certificate-file-name*

Options

`file`

Specify the certificate file as an absolute path.

Importing a certificate into the Global Link Manager server truststore

To import a server certificate from an HDLM host or Device Manager server to the Global Link Manager server's truststore, use the `hglamkeytool` utility. To apply the truststore, you need to restart Global Link Manager.

Caution

When operating a cluster environment, to store a truststore file that is to be used for Global Link Manager in a place other than on the shared disk, you must import the certificate to the standby node as well by performing the same procedure as for the executing node.

Procedure

1. Execute the following command:
   installation-folder-for-Hitachi-Global-Link-Manager\bin\hglamkeytool.bat -importcert -alias *alias* -file *certificate-file-name* -keystore *truststore-file-name* -storepass *password-to-access-the-truststore*

Options

`alias`
: Specify a name that allows you to identify the certificate in the truststore.

`file`
: Specify the certificate file by using an absolute path.

`keystore`
: Specify the import destination truststore file by using an absolute path.
  If a truststore file does not exist in the specified location, the file will be automatically created.

`storepass`
: Specify a password for accessing the truststore.

Checking the certificate imported into the truststore of the Global Link Manager server

To display the contents of the truststore of Global Link Manager, use the `hglamkeytool` utility.

For details about how to check the expiration date for a server certificate, see Checking the certificate expiration date on page 5-27.

Procedure

1. Execute the following command:
   installation-folder-for-Hitachi-Global-Link-Manager\bin\hglamkeytool.bat -list -keystore *truststore-file-name* -storepass *password-to-access-the-truststore*

Options

`keystore`
: Specify the import destination truststore file by using an absolute path.

`storepass`
: Specify a password for accessing the truststore.

Changing the truststore password for the Global Link Manager server

To change the truststore password for the Global Link Manager server, use the `hglamkeytool` utility.

Procedure

1. Execute the following command:
   installation-folder-for-Hitachi-Global-Link-Manager\bin\hglamkeytool.bat -storepasswd -keystore *truststore-file-name*

Options

`keystore`
: Specify the truststore file whose password you want to change, by using an absolute path.

Deleting a server certificate imported into the truststore for the Global Link Manager server

To delete a server certificate imported into the truststore, use the `hglamkeytool` utility. To apply the truststore, you need to restart Global Link Manager.

Procedure

1. Execute the following command:
   installation-folder-for-Hitachi-Global-Link-Manager\bin\hglamkeytool.bat -delete -alias *alias* -keystore *truststore-file-name* -storepass *password-to-access-the-truststore*

Options

`alias`
: Specify a name that allows you to identify the certificate in the truststore.

`keystore`
: Specify the truststore file containing the server certificate you want to delete, by using an absolute path.

`storepass`
: Specify a password for accessing the truststore.

Enabling SSL/TLS on the Global Link Manager server

To enable SSL/TLS, you must set the following properties in the `server.properties` file of the Global Link Manager server.

When establishing SSL communication with the HDLM host:

- `server.https.enable`

- `server.https.truststore`

When establishing SSL communication with Device Manager:

- `server.https.enable`
- `server.https.truststore`
- `server.hdvm.https.ipaddr`

  For details on how to set each property, see Changing Global Link Manager server settings on page 3-34.

After each property is set, restart Global Link Manager.

Advanced security mode

To use Global Link Manager in a configuration that satisfies the following security requirements, you need to specify the settings for SSL/TLS communications and set user passwords.

Digital signature hash algorithm
: SHA-256 or higher

Cryptographic algorithms
: RSA (whose key size is 2,048 bits or more)
: AES (whose key size is 128 bits or more)
: 3KeyTDES

This section describes the tasks required to run Global Link Manager in the *advanced security mode*.

Common Component settings for management-client communication

To enable communication between the management server and management clients (GUI) in the advanced security mode, you need to perform the tasks described below in Common Component.

Creating a private key and a certificate signing request

Create a private key, certificate signing request (CSR) to be sent to a certificate authority (CA), and self-signed certificate by using the `hcmds64ssltool` command. Executing this command creates a CSR and self-signed certificate as follows:

- For the RSA cipher: The private key size is 2,048 bits, and the signature algorithm is SHA256withRSA.
- For the elliptic curve cipher: The private key size is the value (in bits) specified for `ecckeysize`, and the signature algorithm is SHA384withECDSA.

Then, submit the created CSR file to CA and have a signed certificate issued. A CSR is created in a form complying with PEM. For notes on the settings that you need to specify for a CSR, ask the CA that you will use. Note that

certificates issued by a CA have an expiration date. You need to have a certificate reissued before your certificate expires.

Cautions

- If you want to use an external CA, make sure that the CA supports signatures using SHA256withRSA and SHA384withECDSA.
- Although you can use the `hcmds64ssltool` command to create a self-signed certificate, we recommend that you use the command only to test encrypted communications.

For details about the `hcmds64ssltool` command, see Generating a private key, a certificate signing request, and a self-signed certificate on page 5-2.

Checking the certificate expiration date

To check the certificate or the expiration date of the certificate authority, use the `hcmds64checkcerts` command.

Server certificates have expiration dates. Make sure that the certificates are not expired.

Operations to complete in advance

- Log in as a user with Administrator permissions.

Information to collect in advance

- When checking the expiration date of a server certificate from Hitachi Command Suite Common Component or a certificate from a certification authority

  The `hcmds64checkcerts` command enables you to check the expiration date of the certificate specified in the `user_httpsd.conf` file. Therefore, specify the following path of the certificate in the `user_httpsd.conf` file.

  - Server certificate for the Common Component instance

    When a certificate for RSA cipher or elliptic curve cipher is used, the server certificate of the Common Component instance must be specified for each type.
  - Certificate of all of the intermediate certificate authorities
- When checking the expiration date of the server certificate of the HDLM host or Device Manager server imported into the truststore of the Global Link Manager server

  Set the following properties in the `server.properties` file:

  - Set the `server.https.enable` property to `true`
  - Set the trustfile for the `server.https.truststore` property

  The Global Link Manager service must be running.

Format of the command

- *installation-folder-for-Common-Component*\bin\hcmds64checkcerts { [/days *number-of-days*] [/log] | /all }

Options

days

Specify the number of days to check whether a certificate is expired, counting from the day when the command was executed. The specifiable value range is from 30 to 3652 days (10 years). When this option is specified, certificates that will expire within the specified number of days and certificates that have already expired will be displayed. When this option is not specified, 30 is specified as the number of days.

log

If a certificate to be displayed exists, a warning message will be displayed in the Windows event log. To regularly check the expiration date of a certificate by registering this command in an OS task, specify this option.

all

When the certificate is a server certificate from Hitachi Command Suite Common Component or a certificate from an certification authority, displays the expiration date of all certificates specified in the `user_httpsd.conf` file.

When the certificate is a server certificate from an HDLM host or Device Manager server imported into the truststore of the Global Link Manager server, the expiration dates for all the certificates in the truststore file set for the `server.https.truststore` property are displayed.

Management server settings for LDAP directory server communication

To enable StartTLS communication between the management server and an LDAP directory server in the advanced security mode, you need to import a certificate signed with SHA256withRSA and SHA384withECDSA to the truststore for Common Component.

For details on how to check and import server certificates, see Security settings for communication between a server and an LDAP directory server on page 5-13.

Hitachi Command Suite user passwords

In Hitachi Command Suite products, user passwords are hashed and then stored in the database. In version 6.4 or later, a safer and more secure hash method is used.

After performing an update installation of a Hitachi Command Suite product version 6.4 or later or importing a database that was exported in version 6.3 or earlier, if you want to save user passwords in the new hash method, you need to set them again by using the GUI.

Notes on system configuration

The Web browser used by the management client must support certificates signed with SHA256withRSA and SHA384withECDSA.

6

Using Global Link Manager with other products

This chapter describes the Global Link Manager settings for linking with other products.

Overview of single sign-on and user management integration for Hitachi Command Suite products

Single sign-on functionality and integrated user management are available when linkage with other Hitachi Command Suite products, such as Device Manager, has been set up. By using single sign-on functionality, you no longer need to specify a user ID and password when starting other Hitachi Command Suite products from the **Dashboard** menu in the Global Link Manager GUI. For details about the **Dashboard** menu, see the manual *Global Link Manager User Guide*.

When the Hitachi Command Suite products have been installed on one server, single sign-on functionality and integrated user management are available without any special settings. The following figure shows an example of a system configuration where Global Link Manager links with another Hitachi Command Suite product.

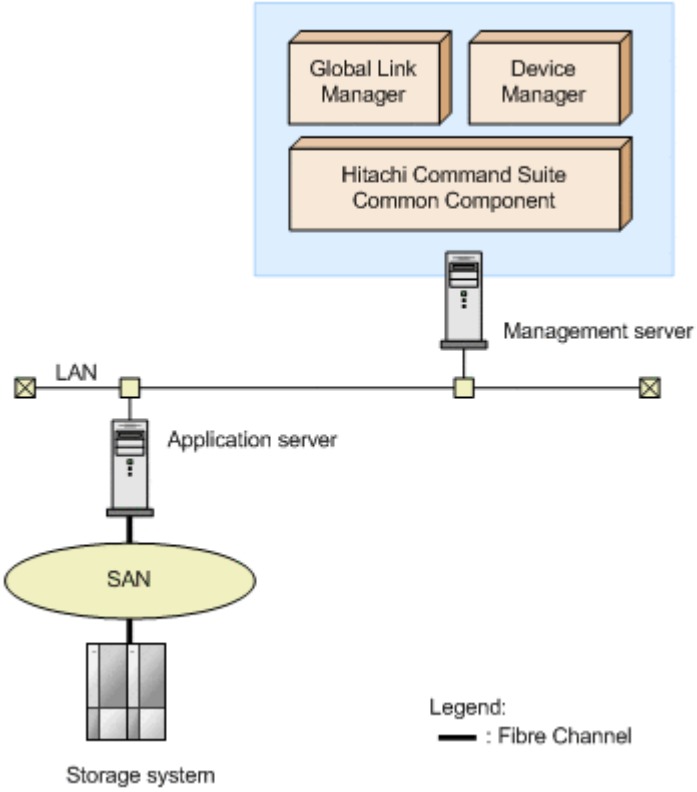

Figure 6-1 Sample configuration where Global Link Manager links with another Hitachi Command Suite product

When you install Global Link Manager and Device Manager on the same server, and use the reception of SNMP traps, check whether the reception of SNMP traps is enabled on Device Manger. If the reception of SNMP traps is also enabled on Device Manager, during the installation of Global Link Manager, specify a port number other than the default 162 number. To change the port number after the installation, modify the value for the `server.snmp.trap_port_num` property in the `server.properties` file.

Note

Single sign-on functionality and integrated user management are available for Hitachi Command Suite products of version 5.0 or later (excluding Tuning Manager 5.0) that are installed on the same server. They are not available for Hitachi Command Suite products whose version is earlier than version 5.0, or for Hitachi Command Suite products that are installed on other servers.

Settings for linking to Device Manager in order to display LDEV labels

You can link Global Link Manager and Device Manager 6.0 or later in order to display the LDEV labels managed by the Device Manager server on the Global Link Manager GUI. For details about the contents displayed for LDEV labels on the Global Link Manager GUI, see online Help.

Procedures for displaying LDEV labels

To display LDEV labels:

1. In the `server.properties` properties file, which is used for displaying LDEV labels, set the following properties:
   - `server.hdvm.ldevlabel.acquisition.enable`

     When this property is enabled, LDEV labels are displayed. By default, this property is disabled.
   - `server.hdvm.http.ipaddr`

     Use this property to specify which instance of the Device Manager server from which LDEV label information will be acquired. This property applies to instances of the Device Manager server where SSL communication has not been set up.
   - `server.hdvm.https.ipaddr`

     Use this property to specify which instance of the Device Manager server from which LDEV label information will be acquired. This property applies to instances of the Device Manager server where SSL communication has been set up. For details about using SSL communication with Device Manager, see Security settings for communication between a server and Device Manager on page 5-22 and Configuring an SSL client on page 5-23.
   - `server.hdvm.polling.time`

     Use this property to specify the interval used to determine the time at which LDEV label information is collected. If this property has been set, the latest LDEV label information can be acquired automatically at regular intervals in addition to the times that LDEV label items are displayed or updated manually. Note that the automatic acquisition of LDEV label information is not recorded in the audit log. For details on the items recorded in the audit log, see Categories of information output to audit logs in Global Link Manager, and audit events on page

3-76. For details on how to specify the above properties, see Changing Global Link Manager server settings on page 3-34.

2. Start Global Link Manager.

   For details on how to start Global Link Manager, see Starting Global Link Manager on page 3-3.

3. Start the instance of the Device Manager server from which LDEV label information will be acquired.

   For details on how to start the Device Manager server, see the *Hitachi Command Suite Administrator Guide*.

4. In the Device Manager server, register the user to be used by Global Link Manager.

   For details on the information to register, see Registering an account for use by Global Link Manager on page 6-4.

5. Make sure that HDLM hosts are managed by Global Link Manager.

   If the hosts are not managed, register them in Global Link Manager. For details on how to register a host in Global Link Manager, see the manual *Global Link Manager User Guide*.

6. Refresh the host information in Global Link Manager.

   For details on refreshing host information, see the manual *Global Link Manager User Guide*.

Registering an account for use by Global Link Manager

On the Device Manager server, register an account for Global Link Manager to use so that LDEV label information can be acquired from the Device Manager server. Register the account using the following:

- Account name: `hglm`
- Password: `hglm`
- Permission: `View`#

Which group the account belongs to depends on the Device Manager server version. The following table shows the relationship between account groups and Device Manager server versions.

Table 6-1 Account groups

Device Manager server version	Account group
6.4 or earlier	Any resource group
7.0	All Resources
7.1 or later	Any user group

For details about how to register an account, see the online Help for Device Manager.

#

If the version of Device Manager Server you are using is earlier than 7.1, register the `View` permission for the application `HDvM`.

Settings for starting HSSM from the Dashboard menu

To link with HSSM and start HSSM from the **Dashboard** menu, create the `StorageServicesManager.conf` file in the following folder if the file has not been created yet:
Hitachi-Command-Suite-Common-Component-installation-folder\common

In the `StorageServicesManager.conf` file, specify the `LaunchURL` parameter in the format shown as follows:

Format of the StorageServicesManager.conf file

```
LaunchURL=HSSM-URL
```

In *HSSM-URL*, specify the URL used to start HSSM. For details about this URL, see the HSSM documentation.

For example, if the name of the HSSM management server is *machinename*, configure the `StorageServicesManager.conf` as follows:

For secure connections:

```
LaunchURL=https://machinename
```

For nonsecure connections:

```
LaunchURL=http://machinename
```

7

Troubleshooting Global Link Manager

This chapter explains how to troubleshoot problems that might occur during Global Link Manager operation. If you need technical support, see Getting help on page xiii.

Procedure for troubleshooting Global Link Manager

To troubleshoot when an error occurs:

1. Check the output messages.

   If no messages have been output, check for similar errors in the examples provided in Global Link Manager troubleshooting examples on page 7-2.

2. If you cannot determine the cause of the error after checking the output messages and checking for similar errors in the troubleshooting examples, collect the diagnostic information.

   For details on how to collect diagnostic information, see Collecting Global Link Manager diagnostic information on page 7-6.

3. Check the contents of the log files you collected in step 2.

   For details on how to check the contents of log files, see Managing Global Link Manager log files on page 7-10.

4. If you cannot determine the cause of the error after checking the contents of the log files, contact the Support Center.

   When contacting the Support Center, provide the diagnostic information you collected in step 2.

Global Link Manager troubleshooting examples

This section provides examples of problems that might occur during Global Link Manager installation, environment setup, and during GUI operation. This section also describes the causes of such problems and the corrective actions you should take for them.

Installing Global Link Manager

Table 7-1 Troubleshooting examples (during Global Link Manager installation)

Problem	Cause	Action
Installation fails.	A user without administrator privileges attempted to perform an installation.	Log on as a user with administrator privileges, and then perform the installation.
	The server machine OS (or OS version) on the installation target server is not supported.	Make sure that a supported OS (or a supported version of the OS) is running on the installation target server, and then perform the installation.
	The amount of free disk space was insufficient on the installation target server.	Increase the amount of free disk space on the installation target server, and then perform the installation.

Setting up Global Link Manager

Table 7-2 Troubleshooting examples (during Global Link Manager environment setup)

Problem	Cause	Action
The specified settings were not applied to the property file.	Global Link Manager was not restarted after the property file was updated.	Restart Global Link Manager.
	Default values were used because incorrect values were set in the property file.	See Changing Global Link Manager environment settings on page 3-33 and make sure the values set in the property file are correct.

Using the Global Link Manager GUI

Table 7-3 Troubleshooting examples (during Global Link Manager GUI operation)

Problem	Cause	Action
The Global Link Manager pages cannot be displayed with a Web browser.	Hitachi Command Suite Common Component is not running.	Start Hitachi Command Suite Common Component. For details on how to do this, see Starting Global Link Manager on page 3-3.
	An attempt to start Hitachi Command Suite Common Component has failed because there is insufficient disk space on the Global Link Manager server.	Ensure that there is enough disk space on the Global Link Manager server, and then start Hitachi Command Suite Common Component. For details on how to start Hitachi Command Suite Common Component, see Starting Global Link Manager on page 3-3.
A host cannot be added.	On an AIX host that is to be added, no paths have been set.	Check the operating environment of HDLM on the host, add necessary paths, and then perform the operation again. For details on how to change the configuration of the HDLM operating environment, see the HDLM manual.
	The settings for the Device Manger agent installed on the host are incorrect.	Execute the `hdvmagt_account` command for Device Manager agents whose

Problem	Cause	Action
		version is earlier than 7.0, or execute the `hdvmagt_setting` command for Device Manager agents whose version is 7.0 or later, in order to set up the Device Manager server information or host information. For details on how to do this, see the manual *Global Link Manager User Guide*.
	Hitachi Command Suite Common Agent Component is not running.	Start Hitachi Command Suite Common Agent Component. For details on how to do this, see Starting Hitachi Command Suite Common Agent Component on page A-10.
The host information cannot be updated.	One or more of the HDLM components installed on the host are not running.	Start any HDLM components that are not running on the host. For details on how to do this, see the HDLM manual.
	The settings of one or more HDLM components installed on the host are invalid.	Correct the settings for the HDLM components installed on the host. For details on how to specify the settings, see the HDLM manual.
	The HDLM version installed on the host is not supported by Global Link Manager.	Install HDLM whose version is supported by Global Link Manager. For details about the HDLM system requirements, see the HDLM manual. Also, check the operating systems not supported by Global Link Manager in HDLM requirements on page 1-12.
	Any of the following errors might have occurred during communication between the Global Link Manager server and the hosts. • The network cable is damaged or not connected properly. • The router or hub is broken. • The network interface card is broken.	Correct the network error depending on the cause of the error. • Connect the network cable properly or replace it. • Replace the router or hub. • Replace the network interface card.

Problem	Cause	Action
	• Packets are lost due to incorrect routing settings. • Packets are blocked by packet filtering such as firewalls. • Communication is poor due to IP address collision. • The specified IP address or subnet mask of the default gateway is invalid.	• Review the routing settings. • Reconfigure packet filtering so that packets for HDLM and Global Link Manager can go through. • Reset the IP addresses. • Revise the settings for the IP address or subnet mask of the default gateway. For troubleshooting procedures other than the above, contact the network administrator.
	In the `server.properties` file of Hitachi Command Suite Common Agent Component on the host, the port number for the port specified in the `server.agent.port` property (agent service port) has been changed.	Temporarily delete the host, and then add it again. For details on how to add and delete hosts, see the manual *Global Link Manager User Guide*.
	The settings for the Device Manger agent installed on the host are incorrect.	Execute the `hdvmagt_account` command for Device Manager agents whose version is earlier than 7.0, or execute the `hdvmagt_setting` command for Device Manager agents whose version is 7.0 or later, in order to set up the Device Manager server information or host information. For details on how to do this, see the manual *Global Link Manager User Guide*.
	On an AIX host, no paths have been set.	Check the operating environment of HDLM on the host, add necessary paths, and then perform the operation again. For details on how to change the configuration of the HDLM operating environment, see the HDLM manual.

Problem	Cause	Action
	Hitachi Command Suite Common Agent Component is not running.	Start Hitachi Command Suite Common Agent Component. For details on how to do this, see Starting Hitachi Command Suite Common Agent Component on page A-10.
In message KAIF22102-E, `The header information is invalid.` is displayed as the detailed information.	The Hitachi Command Suite Common Agent Component is currently stopping its service (or daemon process), or is executing other application processing.	Check the status of the Hitachi Command Suite Common Agent Component service (or daemon process). If it is stopped, start it. If it is running, wait a while, and then retry the operation.
Host information is not displayed.	The logged-in user does not have access permissions for the host.	Change the access permissions for the logged-in user.
Storage information is not displayed.	The logged-in user does not have access permissions for the storage system.	Change the access permissions for the logged-in user.
`n/a` is displayed for the LDEV label.	The IP address and port number specified for `server.hdvm.http.ipaddr` in the `server.properties` file link to a version of Device Manager that is earlier than 6.0.0.	To display the LDEV label, upgrade Device Manager to 6.0.0 or later.

Collecting Global Link Manager diagnostic information

If you cannot identify the cause of an error from the output messages and there are no similarities with the examples shown in Global Link Manager troubleshooting examples on page 7-2, you must collect diagnostic information about the Global Link Manager server. If an error occurs while you are using the single sign-on function, you must collect a thread dump. The following sections describe how to collect diagnostic information and a thread dump.

Diagnostic batch collection about the Global Link Manager server

To collect diagnostic information about Global Link Manager, use the `hcmds64getlogs` command.

Note that you can use the `hcmds64getlogs` command only when an error has occurred.

Types of diagnostic information files

The command collects files and archives them into archive files. The following table lists the files that the command collects and the archive files that it creates.

Table 7-4 Information collected by the hcmds64getlogs command

No.	File type	Archive file name (default)
1	Event log file	`HiCommand_log.jar`
2	Message log file	
3	Installer trace log file	
4	Removal function trace log file	
5	Trace log file	
6	Property file	
7	InstallShield log file	
8	Version file	
9	Database error analysis log file	
10	Path availability information (path status log)	
11	Database detailed log file	`HiCommand_log.hdb.jar`
12	Database file	`HiCommand_log.db.jar`
13	Database table data file	`HiCommand_log.csv.jar`

If you cannot determine the cause of the error after referring to log files No.1 to No. 4 in the above list, send the archive file that contains files No.1 to No. 10 to the Support Center for analysis. At this time, ask the Support Center whether you need to send the archive files for files No.11 to No. 13 as well. Note that Hitachi Command Suite Common Component must be running to obtain the archive file for file No.12.

For details on how to check log files No.1 to No. 4, see Managing Global Link Manager log files on page 7-10.

When acquiring the path availability information (path status log)

When an error occurs during addition or update of a host or during output of a report, and you need diagnostic information, acquire the path availability information (path status log) listed in No.11 of Table 7-4 Information collected by the hcmds64getlogs command on page 7-7. When acquiring the path availability information (path status log), change the property file (`server.properties`). If you change the following property values when acquiring the path availability information as diagnostic information, you do not have to restart Global Link Manager.

- `getlogs.pathreport.get_mode`
- `getlogs.pathreport.host`

- `getlogs.pathreport.startDate`
- `getlogs.pathreport.endDate`

By default, the path availability information (path status log) is not set to be acquired, because it might make the size of the archive file bigger. For details about the property file, see Changing Global Link Manager environment settings on page 3-33.

Format of the hcmds64getlogs command

Command format

`hcmds64getlogs /dir`*folder-name* `[/type HGLAM] [/arc` *archive-file-name*`] [/logtypes` *log-file-type*`[` *log-file-type* `...]]`

Options

Table 7-5 Options and arguments of the hcmds64getlogs command

Options and arguments	Description
`/dir` *folder-name*	Specifies the name of the folder on the local disk for storing collected diagnostic information. To specify an existing folder, make sure that the folder is empty. Characters that can be used: You can use `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), and underscore (`_`). You can also use a backslash (`\`), colon (`:`), and forward slash (`/`) as the path delimiter. If you specify a path that includes a space character, enclose the path in double quotation marks (`"`). If you use a character not listed above, a message is output and the command is terminated. Path length that can be specified: The length of the path you can specify depends on the following: • When the `/type` option is specified: 13 bytes • When the `/type` option is not specified: 71 bytes
`/type HGLAM` or `GlobalLinkAvailabilityManager`	Specifies that only Global Link Manager diagnostic information be collected. If this option is not specified, the command also collects diagnostic information about the other Hitachi Command Suite products installed on the same server.
`/arc` *archive-file-name*	Specifies the name of the archive file in which collected information will be stored. If this option is not specified, the

Options and arguments	Description
	command creates the archive files with the default names shown in Table 7-4 Information collected by the hcmds64getlogs command on page 7-7. The archive file is output to the folder specified for the `/dir` option. Characters that can be used: You can use `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), and underscore (`_`). If you use a character not listed above, a message is output and the command is terminated.
`/logtypes` *log-file-type*`[` *log-file-type* `...]`	Specify the types of log files to acquire when log files of a particular type cannot be collected due to a failure. `log`: Specify this to acquire `.jar` files and `.hdb.jar` files only. `db`: Specify this to acquire `.db.jar` files only. `csv`: Specify this to acquire `.csv.jar` files only. To specify multiple types, separate them by a space. If you omit this option, all log files will be acquired.

Note

If the KAPM05318-I or KAPM05319-E message is not output after the `hcmds64getlogs` command is executed, the command did not complete because sufficient free space was not available for the folder specified in the `/dir` option. Free up sufficient space in the folder, and then re-execute the `hcmds64getlogs` command.

Batch collection of diagnostic information about the host

If the output error is caused by a host, you need to collect diagnostic information about the host.

Use the `DLMgetras` utility to collect diagnostic information. For details on the `DLMgetras` utility, see the HDLM manual.

Thread dump collection of diagnostic information

If any of the following problems occur while the single sign-on function is being used, collect a Java VM thread dump to check for the cause of the problem:

- An attempt was made to start Global Link Manager, but the User Login window did not appear.

- An attempt to log on to Global Link Manager was successful, but the main window did not appear.
- An attempt was made to start Global Link Manager from another Hitachi Command Suite product, but the main window did not appear.

To collect a Java VM thread dump:

1. Create a file with the name `dump` in the following folder: *Hitachi-Command-Suite-Common-Component-installation-folder*`\uCPSB\CC\server\public\ejb\GlobalLinkManagerWebService`
2. In Control Panel in Windows, double-click **Administrative Tools**, and then **Services**. From the displayed Services window, stop **Global Link Manager Web Service**.

   The following file is output to the folder *Hitachi-Command-Suite-Common-Component-installation-folder*`\uCPSB\CC\web\containers\HiCommand64`.

   When the JDK included with Global Link Manager is used:

   `javacore`*xxx.xxxx*`.txt`

   When the Oracle JDK is used:

   `HiCommand64.log`
3. From the Services window, start **Global Link Manager Web Service**.

Managing Global Link Manager log files

After you collect diagnostic information as described in Diagnostic batch collection about the Global Link Manager server on page 7-6, check the log files listed in the following table.

Table 7-6 Types of log files to be checked by the user

Log file	Description
Event log file (`ApplicationLog.evt`)	Stores important messages that are output to the message log file. When other Hitachi Command Suite products have also been installed on the same server, they are also subject to logging. The event log file also stores operations performed by the user and information about Global Link Manager as audit logs. This log file should be checked to audit accesses to Global Link Manager and operations performed by the user.
Message log file (`HGLAM_Message`*n*`.log`)	Stores the messages output while Global Link Manager is starting, stopping, and being operated. This log file should be checked if an error occurs while Global Link Manager is starting, stopping, or being operated.

Log file	Description
Installer trace log file or removal function trace log file (`HGLAM_TL_Install_`*yyyy-mm-dd_hh-mm-ss*`.log` or `HGLAM_TL_Remove_`*yyyy-mm-dd_hh-mm-ss*`.log`)	Stores the messages output during Global Link Manager installation or removal. This log file should be checked if an error occurs during installation or removal.

Output format of the event log files

This section shows the format of entries output to the Windows Event log, and describes the elements in an entry.

Event output format:

date time type user computer source category event-ID explanation

Table 7-7 Information output to the Windows event log

Item	Description
date	The date this entry was logged is output here in `yyyy/mm/dd` format.
time	The time this entry was logged is output here in `hh:mm` format.
type	One of the following strings is output here to indicate the type of message: • Information • Warning • Error
user	`N/A` is always output here.
computer	The computer name is output here.
source	`HBase64 Event` is always output here.
category	`None` is always output here.
event-ID	`1` is always output here.
explanation	A message is output here in the following format: *program-name* [*process-ID*]: *message-ID message-text* For details on the cause and what action to take for each message, see the manual *Global Link Manager Messages*. A message beginning with *program-name* [*process-ID*]: `CELFSS` is an audit log message. For details on the audit logs, see Generating audit logs on page 3-74.

Output format of the message log files

This section shows the format of entries output to the Global Link Manager message log file, and describes the contents of each entry.

Output format:

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

Table 7-8 Information output to the Global Link Manager message log file

Item	Description
serial-number	The serial number of this entry in the message log file is output here.
date	The date this entry was logged is output here in `yyyy/mm/dd` format.
time	The time this entry was logged is output here in `hh:mm:ss.sss` format.
program-name	The Global Link Manager component name or command name is output here.
process-ID	The process ID is output here.
thread-ID	The thread ID is output here.
message-ID	The message ID is output here.
event-type	The type of event that caused this entry to be logged is output here.
user-ID	The user ID of the user who performed the operation is output here. This item is not output for all operations.
message-text	A message is output here. For details on the cause and what action to take for each message, see the manual *Global Link Manager Messages*.

Output format of the installer and removal function trace log files

Output format:

*** begin Hitachi Global Link Manager (Windows) setup process Trace Log
date-and-time : (*level*) *trace-information* [*supplementary-information*]
*** end Hitachi Global Link Manager (Windows) setup process Trace Log

Table 7-9 Information output to the installer trace log and the removal function trace log files

Item	Description
date-and-time	The date and time this entry was logged is output here in `yyyy/mm/dd hh:mm:ss` format.
level	One of the following severity levels is output here: • I: Normal trace information • W: Warning • E: Error to be reported to the user
trace-information	A message is output here.
supplementary-information	The parameters and the return value for an executed command are output here.

A

The settings of Hitachi Command Suite Common Agent Component

This appendix provides information about Hitachi Command Suite Common Agent Component, which must be installed on hosts that will use Global Link Manager. This information includes the settings of Hitachi Command Suite Common Agent Component, as well as the procedure for starting the component.

Hitachi Command Suite Common Agent Component

Hitachi Command Suite Common Agent Component refers to the component included in HDLM.

When the host OS is Windows:

The installation folder for Hitachi Command Suite Common Agent Component varies depending on the environment, such as whether the host is managed by Device Manager. When you want to check the installation folder, use the following registry key to refer to the data.

- Key name: `HKEY_LOCAL_MACHINE\SOFTWARE\Hitachi\HBaseAgent\`*`version`*`\PathName`

  version indicates the version of Hitachi Command Suite Common Agent Component. Check the latest version key name.
- Name: `Path00`

When the host OS is Windows Server 2012 (x64) or Windows Server 2012 R2:

When other Hitachi Command Suite products installed on the host frequently access the Hitachi Command Suite Common Agent Component, JavaVM might finish abnormally. In this case, edit the following file:

installation-folder-for-Hitachi-Command-Suite-Common-Agent-Component`\agent\bin\Server.cmd`

Use a text editor to open the `Server.cmd` file, and then add `-Djava.compiler=NONE` to the java startup options. The following shows an example of editing the `Server.cmd` file:

```
..java -Dalet.msglang -Djava.compiler=NONE -Xss5M -classpath "C:
\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar\agent4.jar;C:
\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar\jdom.jar;C:
\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar\xerces.jar;C:
\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar\servlet.jar;C:
\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar
\log4j-1.2.3.jar"
com.Hitachi.soft.HiCommand.DVM.agent4.as.export.Server %*
exit /b %ERRORLEVEL%
```

Changing firewall settings for HDLM

On a host where HDLM has been installed, if the firewall is active, you need to add Hitachi Command Suite Common Agent Component to the firewall exceptions list so that you can add hosts on the Global Link Manager server.

Windows host where HDLM version 6.6 or later

Registering an exception

Execute the following command to register the Hitachi Command Suite Common Agent Component as an exception:

"*installation-folder-for-Hitachi-Command-Suite-Common-Agent-Component* `\bin\firewall_setup.bat" -set`

For a details on a service port to be registered in the exceptions list, refer to Table A-1 Properties for changing the settings of Hitachi Command Suite Common Agent Component (server.properties) on page A-4.

Deactivating the setting for an exception

Execute the following command to deactivate the setting for an exception:

"*installation-folder-for-Hitachi-Command-Suite-Common-Agent-Component* `\bin\firewall_setup.bat" -unset`

Note

If the port number of the service port in Table A-1 Properties for changing the settings of Hitachi Command Suite Common Agent Component (server.properties) on page A-4 was changed after registering the exception, retry an execution of the `firewall_setup` command.

HDLM for Linux

If the host OS is Linux, register in the Firewall exceptions list by the manual procedure.

For details on a port to be registered, refer to Table A-1 Properties for changing the settings of Hitachi Command Suite Common Agent Component (server.properties) on page A-4.

Changing the settings of Hitachi Command Suite Common Agent Component

In Hitachi Command Suite Common Agent Component, by default, 24041 to 24043 are set for the port numbers that are used to communicate with Global Link Manager. If other products are using these port numbers, change the port numbers of Hitachi Command Suite Common Agent Component.

Also, if multiple network interface cards are installed on the host to connect to the same network, you have to specify the IP address that is used to communicate with Global Link Manager.

To change the settings, edit the property files of each host.

Note

If HDLM and a Device Manager agent are installed on the same host, the two products share the property file and use common properties. Therefore, the specified value used by Hitachi Command Suite Common Agent Component of HDLM and a Device Manager agent is the same.

Location of property files:

In Windows:

```
Hitachi-Command-Suite-Common-Agent-Component-installation-folder
\agent\config\server.properties
Hitachi-Command-Suite-Common-Agent-Component-installation-folder
\agent\config\logger.properties
```

In Solaris or Linux:

```
/opt/HDVM/HBaseAgent/agent/config/server.properties
/opt/HDVM/HBaseAgent/agent/config/logger.properties
```

In AIX:

```
/usr/HDVM/HBaseAgent/agent/config/server.properties
/usr/HDVM/HBaseAgent/agent/config/logger.properties
```

Contents of property files:

The following tables list the properties that are used for changing the settings of Hitachi Command Suite Common Agent Component.

Table A-1 Properties for changing the settings of Hitachi Command Suite Common Agent Component (server.properties)

No.	Property name	Description
Settings for the ports used by the service (or daemon process) and the Web server function		
1	`server.agent.port`#	Specifies the port number for Hitachi Command Suite Common Agent Component's service (or daemon process). When you add a host as a Global Link Manager management-target in the Global Link Manager GUI, specify the **Agent Service Port** to this port number. Default: `24041`
2	`server.http.port`#	Specifies the port number that Hitachi Command Suite Common Agent Component's WebServer uses for non-SSL communication. Default: `24042`
3	`server.http.localPort`#	Specifies the port number for communication between Hitachi Command Suite Common Agent Component's service (or daemon process) and the WebServer process. Default: `24043`

No.	Property name	Description
4	`server.https.port`#	Specifies the port number that Hitachi Command Suite Common Agent Component's WebServer uses for SSL communication. Default: `24045`
Settings for the host name, IP address, and network interface cards that are used by the Web server function		
5	`server.http.host`	Specifies the host name. If you do not specify a host name or specify the default, Hitachi Command Suite Common Agent Component automatically acquires the host name. If the host name cannot be acquired, you must set it manually so that Global Link Manager can access Hitachi Command Suite Common Agent Component. Default: `localhost`
6	`server.http.socket.agentAddres s`	Specifies the IP address of the host. When operating in an IPv6 environment, specify a global address. IPv4 addresses are used when a site-local address or link-local address is specified. If you do not specify an IP address, Hitachi Command Suite Common Agent Component automatically acquires the IP address. If the IP address cannot be acquired, you must set it manually so that Global Link Manager can access Hitachi Command Suite Common Agent Component. If the host on which HDLM is installed has multiple network interface cards and is connected to the same network, specify the IP address of one of the installed network interface cards. If this setting is not configured, the host might not be added properly. If you do not specify this property in the above case, you can register as many hosts as the number of network interface cards, but a number of host and paths might be displayed redundantly. Default: Not specified
7	`server.http.socket.bindAddress`	If the host on which HDLM is installed has multiple network interface cards and is connected to the same network, specify the IP address of one of the installed network interface cards. If this setting is not configured, the host might not be added properly. If you do not specify this property in the above case, you can register as many hosts as the number of network interface cards,

No.	Property name	Description
		but a number of host and paths might be displayed redundantly. Default: Not specified
Settings for the basic operations of the Web server function		
8	`server.agent.maxMemorySize`	Specifies the maximum memory heap size (MB) for the process for the Web server function of the Hitachi Command Suite Common Agent Component. If processing stops because the memory heap size is too small, you can correct the problem by increasing this value. Specifiable range: 32 to 4096. Default: Not specified (the process runs with a maximum memory heap size of 64 MB)
9	`server.agent.shutDownTime`	Specifies the period (in milliseconds) to shutdown the Hitachi Command Suite Common Agent Component's Web Server since it received or sent the last http message. If a value of zero or less is specified, the waiting period is unlimited. Increasing this value results in a faster response from Hitachi Command Suite Common Agent Component to Global Link Manager, but also increases the resources used by Hitachi Command Suite Common Agent Component. Default: `600000` [msec]
10	`server.agent.JRE.location`	Specify the installation destination of the Java program used by the Hitachi Command Suite Common Agent Component. Default for Windows or Linux: None Default for Solaris or AIX Installation path for the Java program that had been installed on the host when you installed the Hitachi Command Suite Common Agent Component
Security settings for the Web server function		
11	`server.http.security.clientIP`	Specify the IPv4 and IPv6 addresses for which access is to be permitted. Specify the IP address of the Global Link Manager server, or do not specify the IP address so that the Hitachi Command Suite Common Agent Component can accept connections from all IP addresses. Note that when the Global Link Manager server shares property files with the Device Manager agent, you must also specify the IP address of the server to be connected to the Device

No.	Property name	Description

		Manager agent, in addition to the IP address of the Global Link Manager server.
		This setting limits the IP addresses permitted for connection, thus preventing denial-of-service attacks or other attacks that intend to overflow buffers.
		For IPv4 addresses, asterisks (`*`) can be used as wildcard characters. Use commas (`,`) to separate multiple IP addresses. Invalid specifications and space characters are disregarded without any errors for IP addresses using decimal numbers with dots.
		In the following example, the specification permits `191.0.0.2` and `192.168.0.0` to `192.168.255.255` to connect to the Hitachi Command Suite Common Agent Component:
		`server.http.security.clientIP=191.0.0.2, 192.168.*.*.`
		The following gives an example for permitting `2001::203:baff:fe36:109a` and `2001::203:baff:fe5b:7bac`:
		`server.http.security.clientIP=2001::203:baff:fe36:109a, 2001::203:baff:fe5b:7bac`
		Default: No specification (all IP addresses can be connected).

12	`server.http.entity.maxLength`	Specifies the maximum length (in bytes) of an XML file that the Global Link Manager server sends to Hitachi Command Suite Common Agent Component. If an error occurs during sending of a large XML file, such as for changing the statuses of many paths concurrently, increasing this value might correct the problem. Default: `32768`
13	`server.agent.secure`	Specifies the security level of the communication channel. 1: When only non-SSL communication is used 2: When both non-SSL and SSL communication is used 3: When only SSL communication is used Default: `1` Note If the Device Manager agent is installed, do not specify "3".
14	`server.agent.ciphers`	Specifies the encryption method used for SSL communication. Specify one or more encryption algorithms by using their

No.	Property name	Description
		corresponding strings for the Java settings. When making multiple specifications, use commas as delimiters. Default value in the case of AIX (for IBM Java) SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384,SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256,SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384,SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384,SSL_RSA_WITH_AES_128_GCM_SHA256,SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_128_CBC_SHA256 Default value in cases other than AIX (for Oracle Java) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256

#

Avoid specifying small port numbers for each property because such numbers might conflict with other services (or daemon process). The normal range is 1024 to 49151.

Note

Default value properties might not be coded in the property file in the initial status after installation. To change the default setting, add the property in the *property-name*=*value* format.

Table A-2 Properties for changing the settings of Hitachi Command Suite Common Agent Component log file (logger.properties)

No.	Property name	Description
1	`logger.loglevel`	Specifies the log level for data that the Hitachi Command Suite Common Agent Component outputs to the files `error.log` and `trace.log`. When the default value is used, INFO, WARN, ERROR, and FATAL entries are output to the log but DEBUG entries are not. Log levels: DEBUG, INFO, WARN, ERROR, and FATAL.

No.	Property name	Description
		Default: `INFO`
2	`logger.MaxBackupIndex`	Specifies the maximum number of log file backups. If more log files are generated than specified, the Hitachi Command Suite Common Agent Component writes over the oldest one. If a log file reaches the maximum size, the file is renamed by adding a counter (which represents the version) to the file name. For example, `access.log` becomes `access.log.1`. If additional backup log files are created, the counter increases until the specified number of backup log files is generated (for example, `access.log.1` becomes `access.log.2`). After the specified number of backup log files is created, each time a new backup file is created, the oldest backup file is deleted. Specifiable range: `1` through `20`. Default: `10`
3	`logger.MaxFileSize`	Specifies the maximum size of each log file. If a log file becomes larger than you specified here, the Hitachi Command Suite Common Agent Component creates a new file and writes logs to it. Unless `KB` is specified for kilobytes or `MB` for megabytes, a specified size is interpreted to mean bytes. Specifiable range: `512 KB` to `32 MB` Default: `1 MB`

File format:

```
property-name=value
#comment
```

- Separate the property name and the value by using an equal sign (`=`).
- When inserting a comment line, begin the line by using a hash mark (`#`).

To edit the property file:

1. Use an application such as a text editor to open the property file, and then edit the file.

   In the `server.properties` file or `logger.properties` file, change the settings of Hitachi Command Suite Common Agent Component.

   Caution

   Do not change the specified value for any properties other than the properties shown in Table A-1 Properties for changing the settings of Hitachi Command Suite Common Agent Component

(server.properties) on page A-4 and Table A-2 Properties for changing the settings of Hitachi Command Suite Common Agent Component log file (logger.properties) on page A-8.

2. Restart Hitachi Command Suite Common Agent Component.

   Stop Hitachi Command Suite Common Agent Component, and then start the component again. For details on how to start and stop Hitachi Command Suite Common Agent Component, see Starting and stopping Hitachi Command Suite Common Agent Component on page A-10.

Starting and stopping Hitachi Command Suite Common Agent Component

When you add a host of HDLM as a resource of Global Link Manager and place the host under Global Link Manager management, Hitachi Command Suite Common Agent Component must be running. The HDLM must also be running.

This section describes how to start and stop Hitachi Command Suite Common Agent Component, and check the operating status.

Although Hitachi Command Suite Common Agent Component starts automatically during HDLM installation, in the following cases, you have to manually stop and then restart the component:

- When you changed the IP address of the host where HDLM was installed
- When you modified the property file of Hitachi Command Suite Common Agent Component

Note

The Hitachi Command Suite Common Agent Component runs on WOW64 when the host is Windows Server 2012 (x64) or Windows Server 2012 R2. Execute the commands provided by the Hitachi Command Suite Common Agent Component from the command prompt for WOW64. The following shows an example of executing the command prompt:

```
C:\WINDOWS\SysWOW64\cmd.exe
```

Starting Hitachi Command Suite Common Agent Component

To start Hitachi Command Suite Common Agent Component, execute the following command, corresponding to the host OS. This operation requires Administrator or root privileges.

In Windows:

```
installation-folder-for-Hitachi-Command-Suite-Common-Agent-Component\bin\hbsasrv.exe start
```

In Solaris or Linux:

```
/opt/HDVM/HBaseAgent/bin/hbsasrv start
```

In AIX:

```
/usr/HDVM/HBaseAgent/bin/hbsasrv start
```

Stopping Hitachi Command Suite Common Agent Component

To stop Hitachi Command Suite Common Agent Component, execute the following command, corresponding to the host OS. This operation requires Administrator or root privileges.

In Windows:

```
installation-folder-for-Hitachi-Command-Suite-Common-Agent-Component\bin\hbsasrv.exe stop
```

In Solaris or Linux:

```
/opt/HDVM/HBaseAgent/bin/hbsasrv stop
```

In AIX:

```
/usr/HDVM/HBaseAgent/bin/hbsasrv stop
```

Checking Hitachi Command Suite Common Agent Component operating status

To check the Hitachi Command Suite Common Agent Component operating status, execute the command below, according to the host OS. This operation requires Administrator or root privileges.

In Windows:

```
installation-folder-for-Hitachi-Command-Suite-Common-Agent-Component\bin\hbsasrv.exe status
```

In Solaris or Linux:

```
/opt/HDVM/HBaseAgent/bin/hbsasrv status
```

In AIX:

```
/usr/HDVM/HBaseAgent/bin/hbsasrv status
```

If the command execution result displays `Status` as `Running`, it means Hitachi Command Suite Common Agent Component service (or daemon process) is operating. If the result displays `Status` as `Stop`, the service (or daemon process) has stopped.

hbsasrv command syntax

This section describes the syntax of the `hbsasrv` command used when starting and stopping Hitachi Command Suite Common Agent Component, and checking the component's operating status.

The following table describes the `hbsasrv` command syntax.

Table A-3 hbsasrv command syntax

Item	Description
Synopsis	`hbsasrv [start | stop [-f] | status]`

Item	Description
Description	Starts or stops the service (or daemon process) of the Hitachi Command Suite Common Agent Component. Also, this command displays the status of the service (or daemon process).
Options	`start`: Starts the service (or daemon process). `stop [-f]`: Stops the service (or daemon process). If other Hitachi Command Suite products are installed on the host, you might not be able to stop Hitachi Command Suite Common Agent Component. In such a case, the error message `KAIE62604-E` appears. Wait until those products complete their operations, and then execute the command again. If you urgently need to stop the Hitachi Command Suite Common Agent Component, you can force the Hitachi Command Suite Common Agent Component to shut down by executing the `hbsasrv` command with the stop `-f` option. In such a case, all processing is forced to terminate, thus ongoing processing of jobs is not guaranteed. `status`: Displays the service (or daemon process) operating status. Note If you execute the command without specifying an argument, the command usage information is displayed.

Setting for changing the Java program used by Hitachi Command Suite Common Agent

Use the following procedure to change the Java program used by Hitachi Command Suite Common Agent.

In Solaris or AIX, see the explanation of `server.agent.JRE.location` in Table A-1 Properties for changing the settings of Hitachi Command Suite Common Agent Component (server.properties) on page A-4 and then specify the installation destination of the Java program.

1. Execute the following command to change the Java program to be used.

   In Windows:

   "*installation-folder-for-Hitachi-Command-Suite-Common-Agent-Component*`\bin\javapath_setup.exe`

   In Linux:

   `/opt/HDVM/HBaseAgent/bin/javapath_setup.sh`

   You can specify the following options in the `javapath_setup` command.

   Command format

   `javapath_setup {-set [new|bundle|` *Java-execution-environment-installation-path*`]|-check}`

   Options

Table A-4 Options and arguments of the javapath_setup command

Item	Description
`-set`	Specify this option to switch the Java execution environment. If you do not specify an argument for this option, the command assumes that you have specified "new " as an argument.
`new`	Specify this argument to select the latest version of the Java execution environment from Oracle JDK and Oracle JRE installed on the host. If the versions of the installed JDK and JRE are the same, the JDK takes precedence. #
`bundle`	Specify this argument to select the Java execution environment bundled with the Device Manager agent.
Java-execution-environment-installation-path	If you want to use a specific Java execution environment, specify the absolute path of the installation path. #
`-check`	Specify this option to check the latest version of the Java execution environment from Oracle JDK and Oracle JRE installed on the host.

#

For details about Java execution environments supported by Dynamic Link Manager, see the *Hitachi Dynamic Link Manager User Guide*.

If Dynamic Link Manager is installed on the host, use a 32-bit Java execution environment.

2. After executing the command, Restart Hitachi Command Suite Common Agent Component.

   For details on how to start and stop Hitachi Command Suite Common Agent Component, see Starting and stopping Hitachi Command Suite Common Agent Component on page A-10.

3. If HDLM GUI has already been booted, reboot HDLM GUI.

Notes

- If you re-install or update the Java program, the command must be re-executed because the installation destination of the Java program is changed.
- If you remove the running Java program that was changed, HDLM for Windows cannot be removed. The Java program must be changed back before removing HDLM for Windows.

Acronyms and abbreviations

The following acronyms and abbreviations might be used in this guide.

A

ASCII
American Standard Code for Information Interchange

C

CA
Certificate Authority

CHA
Channel Adapter

CN
Common Name

CPU
Central Processing Unit

CSR
Certificate Signing Request

CSV
Comma Separated Value

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

D

DEP
Data Execution Prevention

DHCP
Dynamic Host Configuration Protocol

DN
Distinguished Name

DNS
Domain Name System

E

ECC
Elliptic Curve Cryptography

F

FC
Fibre Channel

FC-SP
Fibre Channel Security Protocol

FQDN
Fully Qualified Domain Name

G

GUI
Graphical User Interface

H

HBA
Host Bus Adapter

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

HTTP
Hypertext Transfer Protocol

I

I/O
Input/Output

IP
Internet Protocol

IPF
Itanium® Processor Family

IPv4
Internet Protocol Version 4

IPv6
Internet Protocol Version 6

iSCSI
Internet Small Computer System Interface

L

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

LDEV
Logical Device

LU
Logical Unit

M

MIB
Management Information Base

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

N

NAS
Network Attached Storage

NTP
Network Time Protocol

O

OS
Operating System

R

RADIUS
Remote Authentication Dial In User Service

S

SAN
Storage Area Network

SMTP
Simple Mail Transfer Protocol

SNMP
Simple Network Management Protocol

SP
Service Pack

SSL
Secure Sockets Layer

SSO
Single Sign-on

T

TLS
Transport Layer Security

U

URL
Uniform Resource Locator

X

XML
Extensible Markup Language

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact