HITACHI
DATA SYSTEMS

HiCommand® Global Link Availability Manager Installation and Configuration Guide

MK-95HC107-01

Trademarks

RC4 is a registered trademark or trademark of RSA Security Inc. in the United States and/or other countries.

RSA is a registered trademark or trademark of RSA Security Inc. in the United States and/or other countries.

Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

Windows is a registered trademark of Microsoft Corp. in the U.S. and other countries.

Windows Server is a registered trademark of Microsoft Corp. in the U.S. and other countries.

This product includes software developed by the JDOM Project (http://www.jdom.org/).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).

This product includes software developed by Greg Stein <gstein@lyra.org> for use in the mod_dav module for Apache (http://www.webdav.org/mod_dav/).

HiCommand® Global Link Availability Manager includes RSA BSAFE Cryptographic software from RSA Security Inc.

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

This product includes altered versions of software originally developed by Henry Spencer.

All other brand or product names are or may be trademarks or service marks of and are used to identify products or services of their respective owners.

Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Please contact the Hitachi Data Systems Legal Department for any export compliance questions.

Document Revision Level

Revision	Date	Description
MK-95HC107-00	March 2006	Initial Release
MK-95HC107-01	January 2007	Revision 1, supersedes and replaces MK-95HC107-00

Preface

This manual describes installation, setup, server operation, user management, and resource management of the HiCommand® Global Link Availability Manager program (abbreviated hereafter to *HGLAM*).

This manual is intended for those who want to create or operate an HGLAM system. The reader is assumed to have the following:

- Knowledge of HDLM installation and setup
- Knowledge of the server OS (Windows)

Note: The use of the HiCommand® Global Link Availability Manager and all other Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

Software Version

This document revision applies to HiCommand® Global Link Availability Manager version 5.6 and higher.

Convention for Storage Capacity Values

Storage capacity values displayed by HiCommand® Global Link Availability Manager are calculated based on the following values:

1 KB (kilobyte) = 1,024 bytes
1 MB (megabyte) = $1,024^2$ bytes
1 GB (gigabyte) = $1,024^3$ bytes
1 TB (terabyte) = $1,024^4$ bytes

Referenced Documents

- *HiCommand® Global Link Availability Manager User's Guide*, MK-95HC106
- *HiCommand® Global Link Availability Manager Messages*, MK-95HC108
- *HiCommand® Device Manager Web Client User's Guide*, MK-91HC001
- *HiCommand® Device Manager Command Line Interface (CLI) User's Guide,* MK-91HC007
- *HiCommand® Device Manager Agent User's Guide*, MK-92HC019
- *HiCommand® Device Manager Server Installation and Configuration Guide,* MK-92HC002

Readme and Release Notes Contents

These files can be found on the installation CD. They contain requirements and notes for use of HiCommand® Global Link Availability Manager that may not be fully described in the manual. Be sure to review these files before installing HiCommand® Global Link Availability Manager.

Comments

Please send us your comments on this document. Make sure to include the document title, number, and revision. Please refer to specific section(s) and paragraph(s) whenever possible.

- **E-mail:** doc.comments@hds.com
- **Fax:** 858-695-1186
- **Mail:**
  Technical Writing, M/S 35-10
  Hitachi Data Systems
  10277 Scripps Ranch Blvd.
  San Diego, CA 92131

Thank you! (All comments become the property of Hitachi Data Systems Corporation.)

Contents

List of Figures

List of Tables

Chapter 1 HGLAM System Configuration and Requirements

This chapter describes the HGLAM system configuration and requirements.

- HGLAM Overview (section 1.1)
- HGLAM System Configuration (section 1.2)
- HGLAM System Requirements (section 1.3)
- HGLAM Operation Overview (section 1.4)

1.1 HGLAM Overview

HGLAM uses HiCommand® Dynamic Link Manager (HDLM) path control functionality to provide integrated path management for large-sized system configurations. While HDLM manages paths for a host, HGLAM 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. HGLAM enables you to reduce the workload by providing unified management of the path information for multiple hosts. HGLAM 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.

HGLAM collects information about paths from multiple HDLM-installed hosts and the HGLAM 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 an HGLAM system configuration.

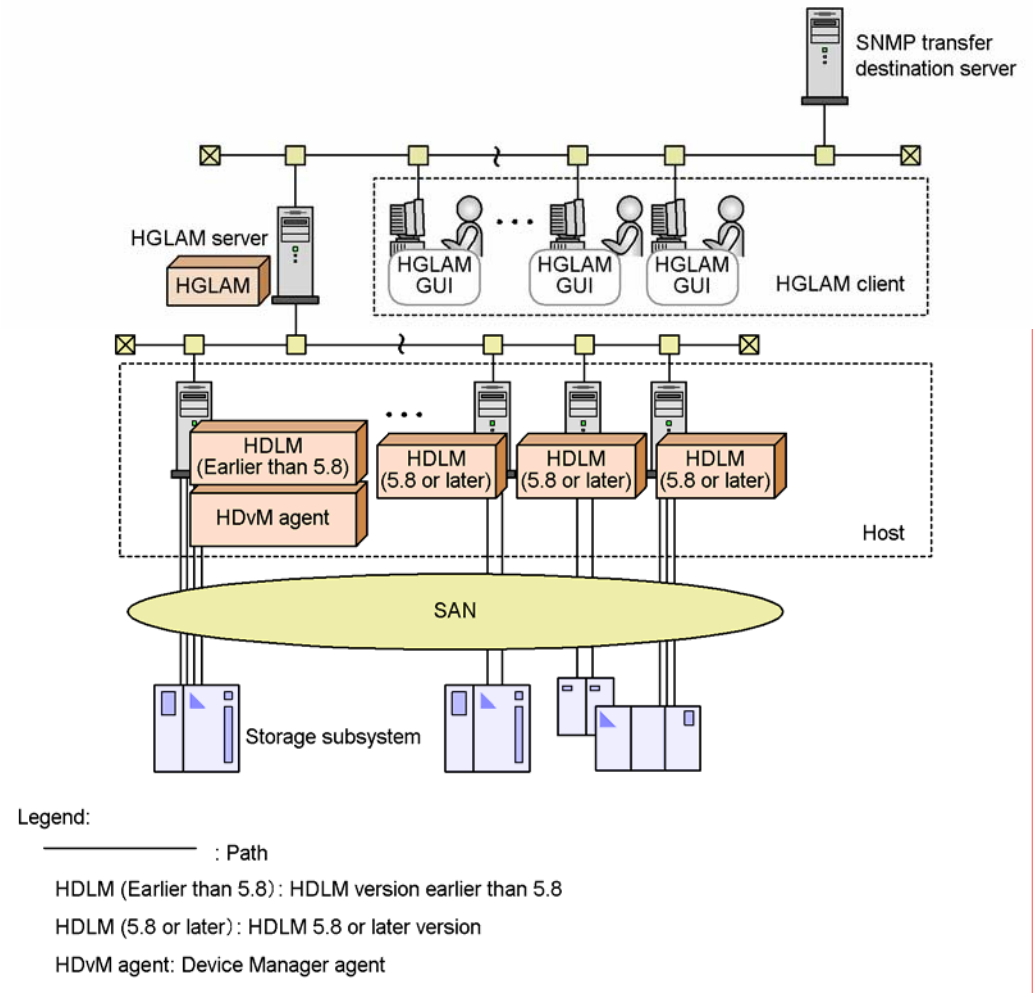

Figure 1.1 Example of an HGLAM System Configuration

HGLAM supports the following features:

Collectively Manages Path Information of Multiple Hosts

By remote operations using the HGLAM 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 subsystems, CHA ports, or by path status.

Summarizes the Path Statuses for the Whole System

HGLAM 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.

Supports Path Bandwidth Control

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

Collectively Manages the Error Information from Multiple Hosts

To quickly detect errors that occur on many hosts and take appropriate action, you need to set up the environment to inform you about the error cause and location. You can set up HGLAM to send an alert when the HDLM on any host detects an error, thereby facilitating central management of error information. You can use an application of your choosing to manage alert information that was transferred from the HGLAM server to another SNMP management server.

1.2 HGLAM System Configuration

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

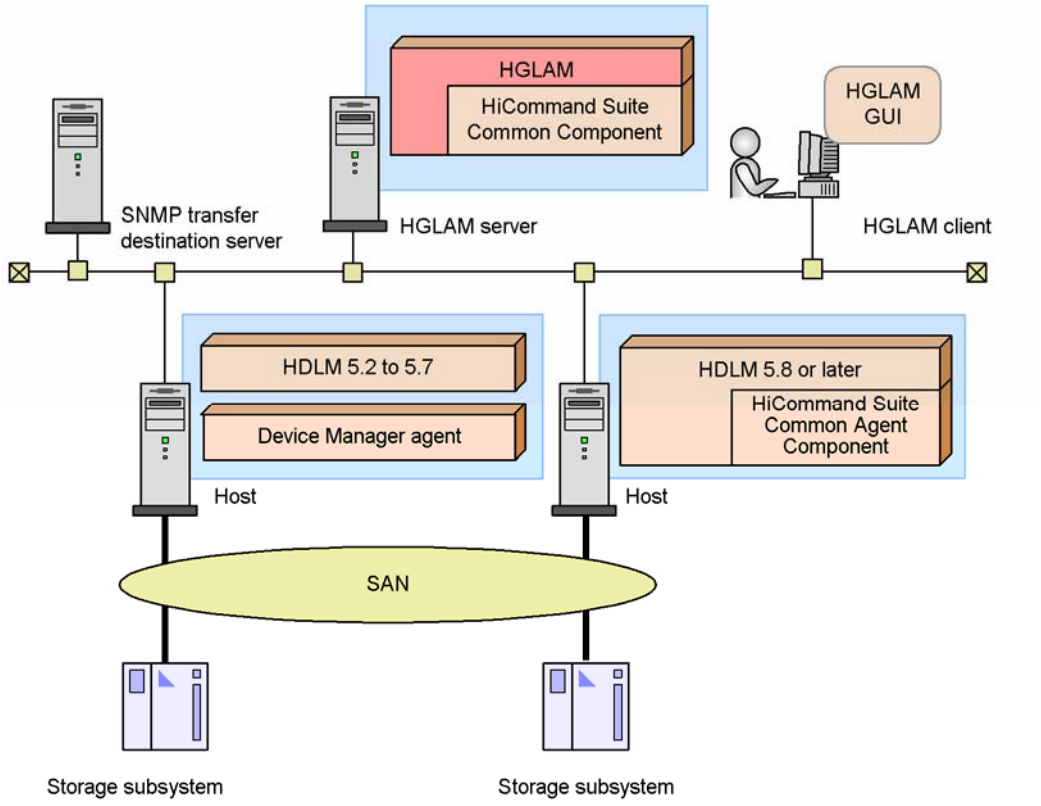

Figure 1.2 Basic HGLAM System Configuration

The system components in this figure are explained below.

HGLAM server

The machine on which the HGLAM program is installed. The HGLAM server collects system configuration information from each host, and provides the information to the HGLAM client.

The HGLAM receives requests from the HGLAM GUI, and performs the appropriate operations, such as collecting information from hosts and setting up hosts.

HiCommand® Suite Common Component provides HiCommand® server functionality and the basic functionality of the GUI. HiCommand® Suite Common Component is installed as part of HGLAM, Device Manager, Tuning Manager, and other HiCommand® server products, and is always updated to the latest version.

HGLAM client

A machine on which the HGLAM GUI is used. The HGLAM GUI provides a user interface for managing hosts with HGLAM.

Host

A machine on which application programs are installed. In the system in which HGLAM is used, each host uses a storage subsystem as an external storage device, and HDLM manages the paths between hosts and storage subsystems. HDLM improves the reliability of the system by balancing the loads on paths and switching paths when a problem occurs.

If the HDLM version is earlier than 5.8, a Device Manager agent is required for communication between the HGLAM server and the host.

If the HDLM version is 5.8 or later, HDLM includes a component called HiCommand® Suite Common Agent Component that is used for communication between the HGLAM server and the host.

Storage subsystem

An external storage device connected to a host. The storage subsystems whose paths are managed by HDLM are subject to HGLAM management.

SNMP transfer destination server

A machine that receives alert information transferred from the HGLAM server by means of SNMP traps. You must set up the HGLAM server to transfer alert information to the SNMP transfer destination server. For details about the setup for transferring alert information, see section 3.11.

The HGLAM system configuration is also explained in the following sections. See the appropriate section for your environment.

- System configuration in a cluster environment, see section 4.1
- System configurations where HGLAM links with other HiCommand® products, see section 6.1

1.3 HGLAM System Requirements

This section describes the HGLAM system requirements.

1.3.1 HGLAM Server Requirements

The following table describes the requirements for the machine on which the HGLAM server program is installed.

Table 1.1 Requirements for the Machine on Which the HGLAM Server Program is Installed

Item	Requirements
Applicable OSs	▪ Windows 2000 (SP3 or SP4) ▪ Windows Server 2003 x86 (no SP or SP1) ▪ Windows Server 2003 R2 x86 ▪ Windows XP (no SP, SP1, or SP2)
Monitor resolution	SVGA (800 x 600) or higher
Free disk space (for a new installation)	Disk for installing the HGLAM program: 1.5 GB Disk for storing the database files: 200 MB
Cluster software (when a cluster system is to be created)	One of the cluster services of the following OSs: ▪ Windows 2000 Advanced Server ▪ Windows 2000 Datacenter Server ▪ Windows Server 2003, Enterprise Edition# ▪ Windows Server 2003, Datacenter Edition# ▪ Windows Server 2003 R2, Enterprise Edition# ▪ Windows Server 2003 R2, Datacenter Edition#

#: Majority Node Set is not included.

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

Table 1.2 Guide to maximum numbers for HGLAM management targets

Management Target Type	Maximum Number
Hosts	1000
Multipath LUs#1	10000
Paths#1#2	40000

#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 section 3.3.

For details on how to output reports on path availability information, see Help.

Notes:

- HGLAM cannot coexist with a HiCommand® product whose version is earlier than 4.0. Therefore, do not install HGLAM on a machine in which a HiCommand® product whose version is earlier than 4.0 is already installed.
- You cannot install HGLAM on a machine in which Tuning Manager is already installed in a large configuration. If you attempt to install HGLAM in such an environment, the installation stops. In this case, install HGLAM and Tuning Manager on different machines.

- HGLAM cannot coexist with the HiRDB products listed below. Therefore, do not install HGLAM 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 HGLAM 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 HGLAM server. Do not use DHCP.
- Before installing HGLAM, make sure that you set the current time for the local time of the machine on which you are going to install HGLAM. If the current time is not set, path availability information (path status log) might not be acquired correctly.

1.3.2 HGLAM Client Requirements

The following table describes the system requirements for using the HGLAM GUI.

Table 1.3 Requirements of Client System for Using the HGLAM GUI

Item	Requirements
Applicable OSs	▪ Windows 2000 (SP3 or SP4) ▪ Windows Server 2003 x86 (no SP or SP1) ▪ Windows Server 2003 R2 x86 ▪ Windows XP (no SP, SP1, or SP2)
Applicable Web browsers	Microsoft Internet Explorer 6.0 or later

1.3.3 HDLM Host Requirements

To manage hosts by HGLAM, installation and environment setup of HDLM must be completed on the hosts. If the installed HDLM version is earlier than 5.8, a Device Manager agent must also be installed. The following table describes the requirements of each host to be managed with HGLAM.

Table 1.4 Requirements of Each Host to Be Managed with HGLAM

Item	Requirements
Prerequisite programs	▪ HDLM 5.2 or later (When the OS is Linux, x86 is 5.3 or later, IPF is 5.4 or later, AMD64 is 5.8 or later, EM64T is 5.8 or later) ▪ Device Manager agent 3.5 or later (only when the HDLM version is earlier than 5.8)
Applicable OSs	Same as the applicable OSs of HDLM: ▪ AIX (excluding version 4.3.3) ▪ HP-UX ▪ Linux (excluding Red Hat Enterprise Linux AS 2.1 (IPF), SUSE LINUX Enterprise Server 8, and SUSE LINUX Enterprise Server 9 (AMD64, EM64T, and IPF)) ▪ Solaris (excluding version 2.6) ▪ Windows (excluding Windows NT) For details about the applicable OS versions for HDLM, see the manual *HiCommand ®Dynamic Link Manager User's Guide*, which is supplied with the HDLM product.

Note:

- HGLAM supports the IPv4 network configuration. If IPv6 is enabled on a host in which HDLM is installed, you cannot start a Device Manager agent service or the HiCommand® Suite Common Agent Component service. To use HGLAM, disable IPv6 on the host.
- If multiple NICs are installed on a host, specify the IP address for the `server.http.socket.bindAddress` property# in the `server.properties` file for the Device Manager agent or HiCommand® Suite Common Agent Component.

  You can avoid registering a single host redundantly because you can register a host only by using the IP address specified for this property.

  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.bindAddress` property.

  #:

  For information about the `server.http.socket.bindAddress` property in the `server.properties` file, when the HDLM version of the host is earlier than 5.8, see the manual *HiCommand® Device Manager Agent Installation Guide*. If the HDLM version of the host is 5.8 or later, see Appendix A in this manual.
- 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 HDLM. If the current time is not set, path availability information (path status log) might not be acquired correctly.

For details about the installation and environment settings of HDLM, see the manual *HiCommand® Dynamic Link Manager User's Guide*, and Appendix A in this manual.

1.4 HGLAM Operation Overview

This section describes the overall flow of tasks for HGLAM, from setup to operations. Also, the settings necessary to start the operations and the procedures for logging in to HGLAM are described.

The following figure shows the flow of tasks for operating HGLAM.

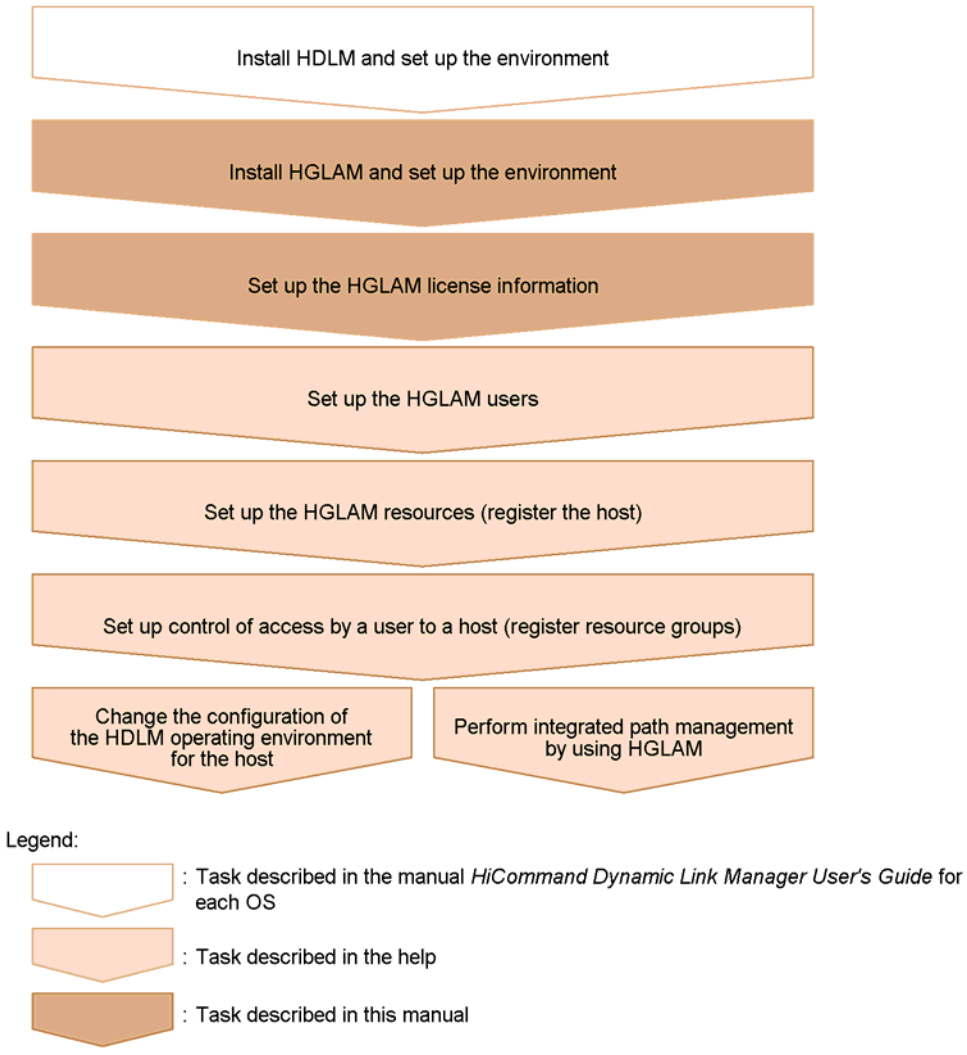

Figure 1.3 Flow of HGLAM Tasks

Installing HDLM and setting up its environment

Set up HDLM on all hosts that are managed, in an integrated way, by HGLAM. For details about the requirements for installing HDLM and the Device Manager agent on a host, see section 1.3.3. For details about the procedures for installation and environment setup of HDLM at each host, see the manual HiCommand® Dynamic Link Manager User's Guide for the applicable host OS.

Configure the following on all hosts, according to the version of HDLM that has been set up:

- When the HDLM version of a host is earlier than 5.8:

  To use HGLAM to manage HDLM, you must use a Device Manager agent. The procedure for setting up the Device Manager agent differs depending on the version of the Device Manager agent and the host OS. For details about the installation and setup procedures, see the manual HiCommand® Device Manager Agent Installation Guide.

  Note: If you are installing a Device Manager agent solely to use HGLAM, you must configure the host information necessary for HGLAM, instead of the Device Manager server information, when you install or set up the Device Manager agent. For details about how to configure the host information necessary for HGLAM, see Help.

- When the HDLM version of a host is 5.8 or later:

  To use HGLAM to manage HDLM, you have to configure the settings to use HiCommand® Suite Common Agent Component after setting up HDLM. For details about how to configure the settings, see Appendix A.

Note: If you install the Device Manager agent or HDLM version 5.8 or later on a host who's OS is Windows Server 2003 (IPF) for which SP1 has not been installed, operations might become unstable while linking with HGLAM. To avoid this, we recommend that you first install SP1, and then install the Device Manager agent or HDLM version 5.8 or later.

Installing HGLAM and setting up its environment

Set up HGLAM and start the HGLAM server. For details about the installation and environment setup of the HGLAM server, see Chapter 2 through Chapter 6 for the appropriate server environment.

Setting up HGLAM license information during initial login

After setting up HGLAM, in the HGLAM GUI specify the initial license. For details about how to specify the initial license, see section 2.2.

For details about the flow of operations of other tasks, description of functions, and procedure details, see Help.

Chapter 2 Installing HGLAM

This chapter describes HGLAM installation. When installing HGLAM in a cluster environment, see Chapter 4.

- Types of HGLAM Installations (section 2.1)
- Setting Up License Information During Initial Login (section 2.2)

2.1 Types of HGLAM Installations

This section explains how to install HGLAM. The following types of installation are available:

- New installation
- Reinstallation
- Upgrade installation
- Uninstallation

After checking the items described in section 2.1.1, follow the installation procedure.

Reference: A service pack for HGLAM is provided. For details on how to install a service pack, see the documentation provided with the service pack.

2.1.1 Preparing to Install HGLAM

Make sure of the following on the server in which HGLAM 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 4.0
  - Tuning Manager that has a Large configuration
  - HiRDB products (HiRDB/Single Server, HiRDB/Parallel Server, HiRDB/Workgroup Server, HiRDB/Run Time, HiRDB/Developer's Kit, and HiRDB SQL Executer)
- Port number 162 is not being used by another product.

  In HGLAM, the default value for the port number for receiving SNMP traps is set to 162. If this port number is already used by another product, specify a different port number when installing HGLAM. If the same port number is shared by HGLAM and another product, even if the installation of HGLAM has finished successfully, you will not be able to start HGLAM. 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 section 3.3.
- Products other than HiCommand® products are not using port numbers 23015, 23016, 23017, 23018, 23032, and 45001 to 49000.

  If other products are using these ports, you cannot start HGLAM, even if the installation of HGLAM has finished normally. Make sure that no other products are using these ports, and then begin the installation. You can change the port numbers 23015 to 23018, and 23032 after the installation. For details on how to change a port number, see section 3.5. If these port numbers have already been changed and used in an environment where HiCommand® Suite Common Component is installed, you can use the changed port numbers to install HGLAM. You do not have to change the port numbers back to the default.

- No other HiCommand® product is running.
- Dialog boxes used for operating Windows services, such as Computer Management or Services, are not displayed.
- If a HiCommand® product has already been installed, HiRDB/EmbeddedEdition _HD0 is already running.

  To use HiCommand® products, HiRDB/EmbeddedEdition _HD0 must be always running. In the list in the Services panel, check whether HiRDB/EmbeddedEdition _HD0 is running. If it is not running, start HiRDB/EmbeddedEdition _HD0.

Note: Before installing HGLAM on a machine in which another HiCommand® product has already been installed, back up the database. For details about how to do this, see section 3.2.1.

When installing HGLAM in Windows Server 2003 SP1 or Windows XP SP2 or later, you need to specify the following settings if Data Execution Prevention is being used:

2.1.1.1 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, Settings, 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 select the **Turn on DEP for all programs and services except those I select** radio button.

4. Click the **Add** button and specify the HGLAM installer (`setup.exe`).

   The HGLAM installer (`setup.exe`) is added to the list.

5. Select the checkbox next to the HGLAM installer (`setup.exe`) and click the **OK** button.

2.1.2 Installing HGLAM for the First Time

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

- Host name or IP address of the server
- Number of the port for HBase Storage Mgmt Web Service
- Whether to receive SNMP traps
- Number of the port for receiving SNMP traps

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 HGLAM. Check the IP address or host name of the server on which HGLAM is to be installed, and check the port number for HBase Storage Mgmt Web Service. The default value for the port number is 23015. This information is not required when another HiCommand® product has been installed.
Number of the port for HBase Storage Mgmt Web Service	
Whether to receive SNMP traps	Determine in advance whether to use the function that notifies HGLAM 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 receiver function, check the IP address of the SNMP trap destination. The default IP address is the IP address of the HGLAM server.
Number of the port for receiving SNMP traps	When you use the SNMP trap reception function, check the port number to be used exclusively by SNMP traps. The default value for the port number is162. If port number 162 is already used by another program, use another port number.

To perform a new installation:

1. Insert the HGLAM installation CD-ROM.
2. Use Explorer to view the contents of the CD-ROM, and then execute `setup.exe`.

   The **Welcome to the Installation of HiCommand® Global Link Availability Manager (New)** dialog box appears.

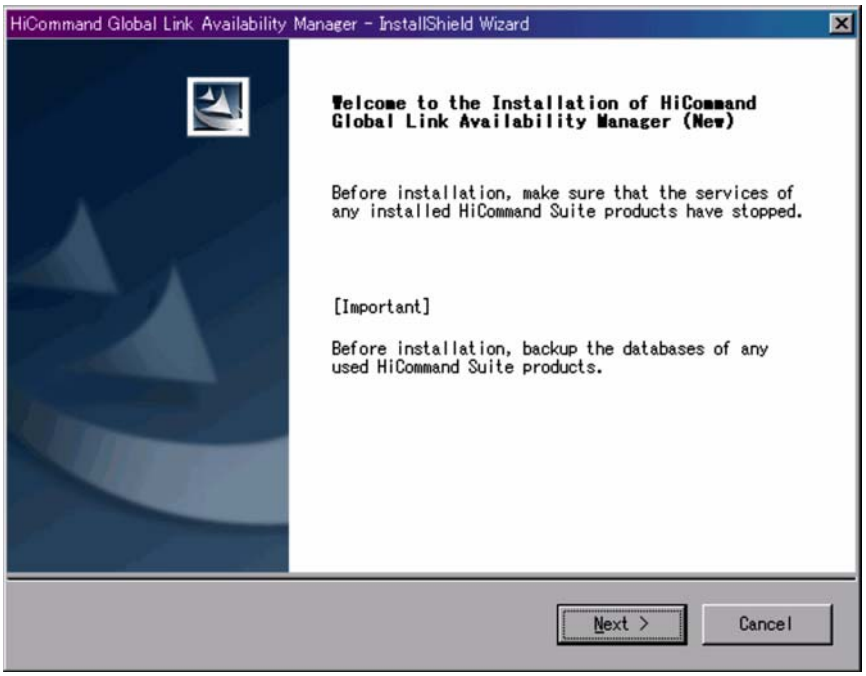

Figure 2.1 Welcome to the Installation of HiCommand® Global Link Availability Manager (New) Dialog Box

3. Click the **Next** button.

   If other HiCommand® Suite products have already been installed, the **Confirmation of Setup Status of Common Component Database of HiCommand® Suite** dialog box appears. Check the setup status in this dialog box, and then click the **Next** button. The three setup statuses are:

   - Non-cluster configuration
   - Execution system node of cluster configuration
   - Standby node in a cluster configuration

   Click the **Next** button to display the **Setup of the Installation Folder** dialog box.

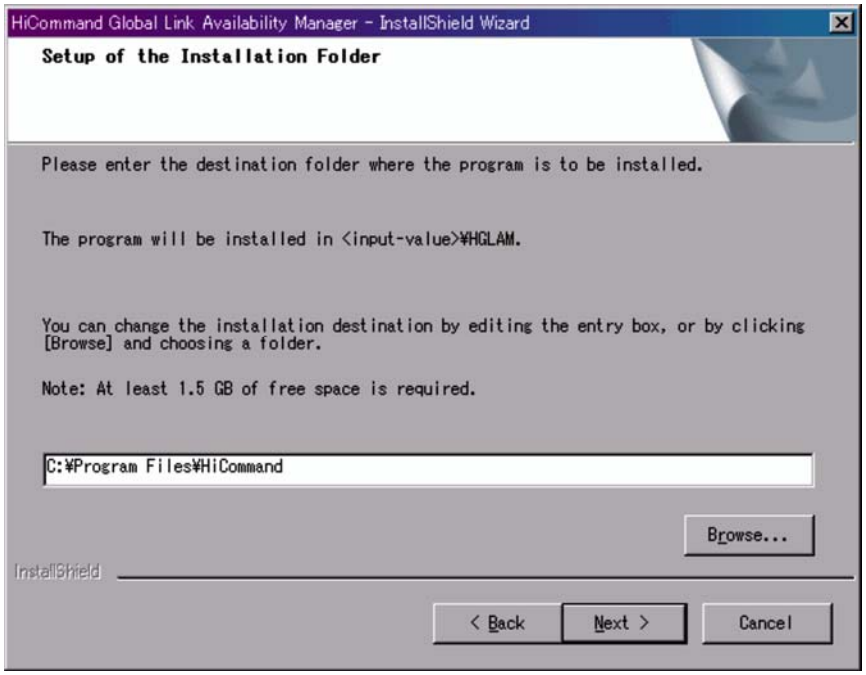

Figure 2.2 Setup of the Installation Folder Dialog Box

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:

- 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, hash mark (#), plus sign (+), hyphen (-), period (.), at mark (@), underscore (_), and the space character.

  Note that a space character cannot be used at the beginning or end of a folder name.
- 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 default installation folder for HGLAM is as follows:

system-drive:\Program Files\HiCommand\HGLAM

The default installation folder for HiCommand® Suite Common Component is as follows:

system-drive:\Program Files\HiCommand\Base

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

HKEY_LOCAL_MACHINE\SOFTWARE\Hitachi\HiCommand Base\InstallPath

4. Click the **Next** button.

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

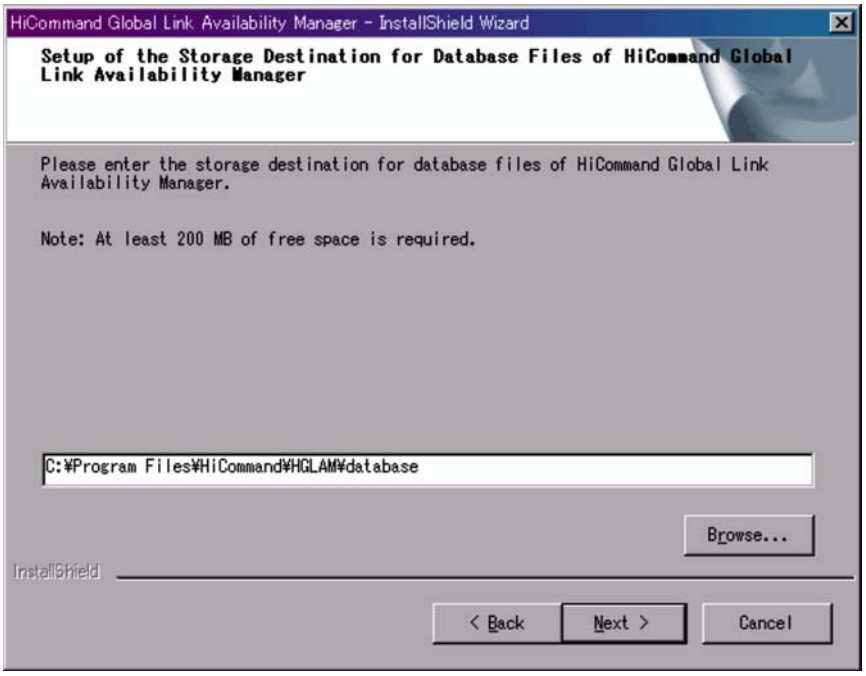

Figure 2.3 Setup of the Storage Destination for Database Files of HiCommand® Global Link Availability Manager Dialog Box

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

- 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 a space character cannot be used at the beginning or end of a folder name.
- The path name must not contain any names reserved by the OS (CON, AUX, NUL, PRN, CLOCK$, COM1 to COM9, and LPT1 to LPT9).

5. Click the **Next** button.

   The **Setup of Information about the Server of HiCommand® Global Link Availability Manager** dialog box appears.

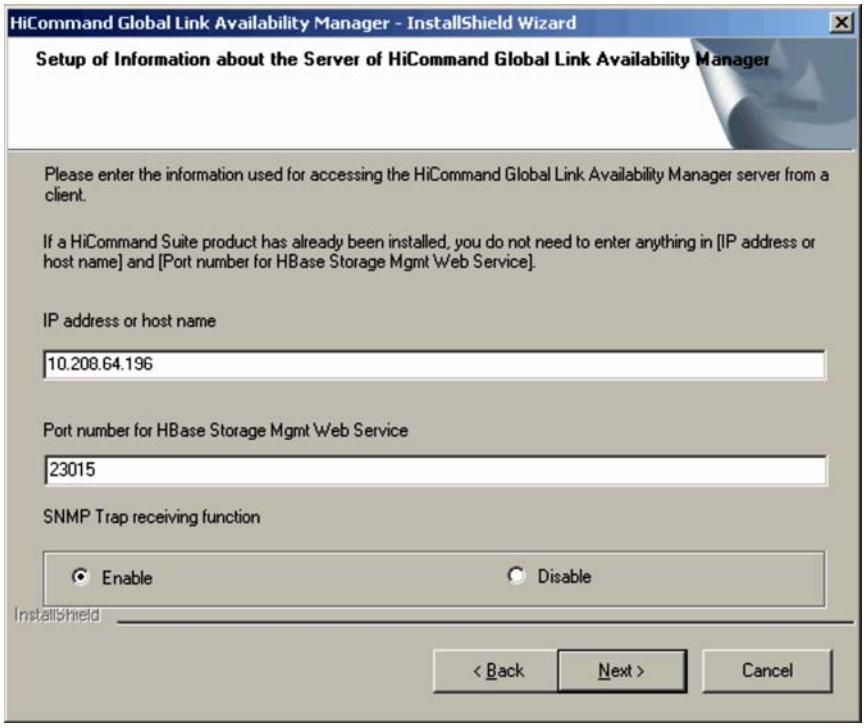

Figure 2.4 Setup of Information about the Server of HiCommand® Global Link Availability Manager Dialog Box

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

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

When you install HGLAM in an environment in which no other HiCommand® 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.

If another HiCommand® 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 Storage Mgmt Web Service

Make sure that the URL value is correct after the installation. To check the set value, execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdschgurl /print
```

Executing the above command displays the URL. The following shows the URL format:

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

If the value set for the URL is different from the information of the server on which HGLAM is installed, see the following and change the value:

– For changing the IP address, see section 3.6.1.

– For changing the host name, see section 3.4.

– For changing the port number of HBase Storage Mgmt Web Service, see section 3.5.1.

Note: In some network environments, the host may 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.

6. Click the **Next** button.

If you have enabled the SNMP trap receiver function, the **SNMP Trap Connection Settings for HiCommand® Global Link Availability Manager** dialog box appears. If you have disabled this function, go to step 7.

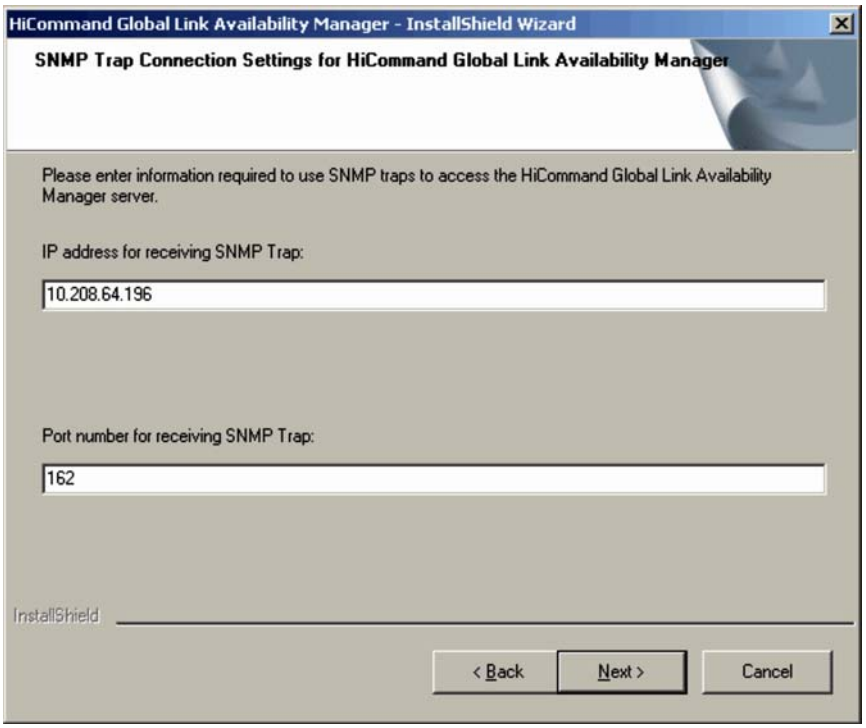

Figure 2.5 SNMP Trap Connection Settings for HiCommand® Global Link Availability Manager Dialog Box

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

– IP address for receiving SNMP traps

– Port number for receiving SNMP traps

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

Note: When you install HGLAM on a server in 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 HGLAM, you will no longer be able to start Device Manager.

7. 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. HiCommand® Suite Common Component and the port that receives SNMP traps will be added to the Windows Firewall exceptions list.

   Note: If you register HGLAM as an exception in the Windows Firewall exceptions list, it might take approximately 15 minutes more to install HGLAM. If you have enabled Windows Firewall after installing HGLAM, you must manually add HGLAM to the exceptions list. For details on how to manually add HGLAM to the exception list, see section 3.7.2.

   Clicking the **Next** button displays the **Confirmation Before Installation** dialog box.

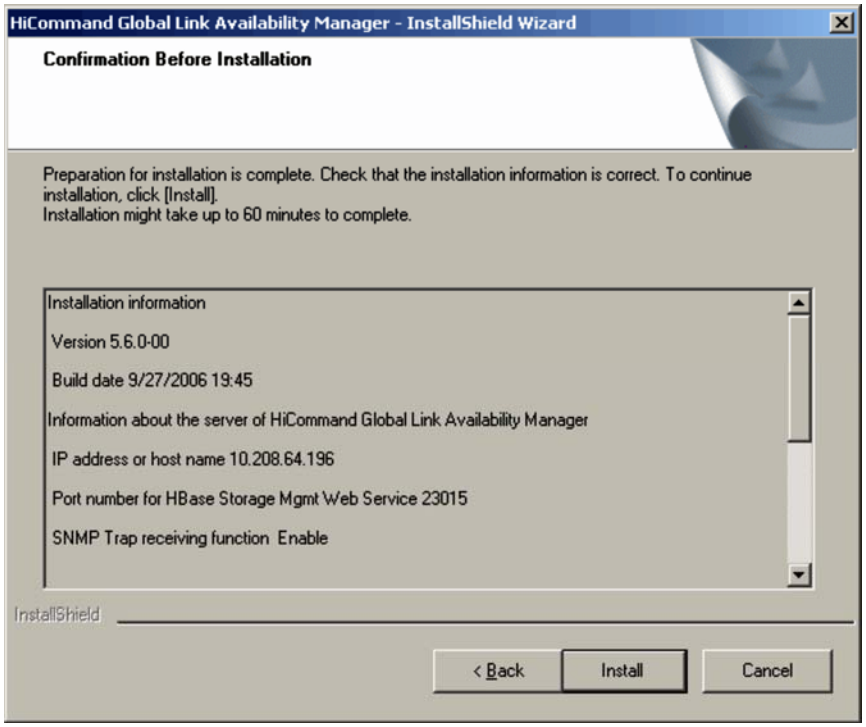

Figure 2.6 Confirmation Before Installation Dialog Box

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. When installation is complete, the **Installation Complete** dialog box appears.

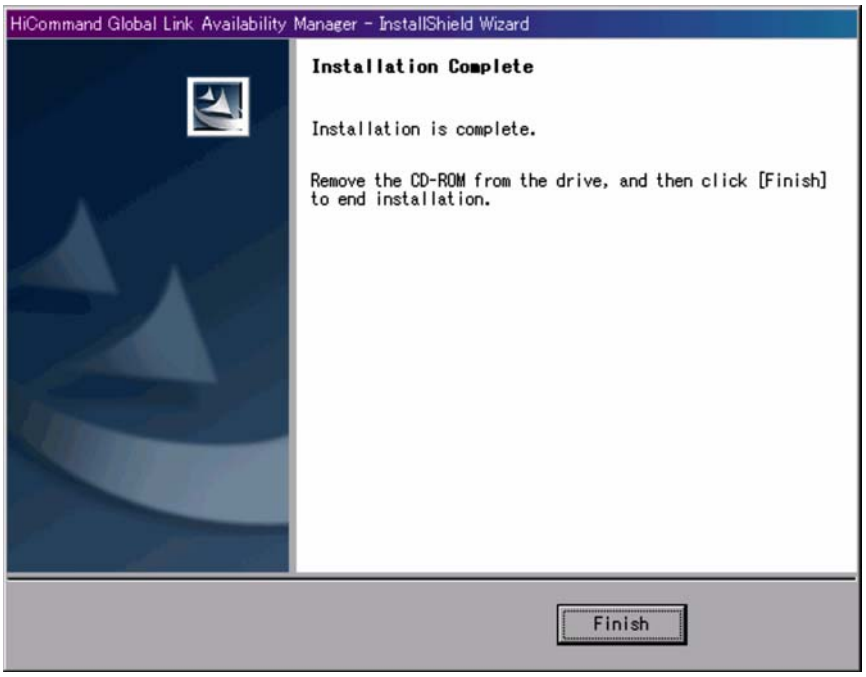

Figure 2.7 Installation Complete Dialog Box

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

   When the installation completes normally, the operating status of the HiCommand® Suite Common Component services vary depending on the setup state of the database:

   - When the setup state is a non-cluster configuration: Services start automatically, and HGLAM enters an operational state.
   - When the setup state is a cluster configuration: Services on the standby node will not start. Specify the settings for operating HGLAM in a cluster configuration.

   To log in to HGLAM and start operations, you must set up the initial license information. See section 2.2.

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 section 3.3.

2.1.3 Reinstalling HGLAM

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

Make sure of the following before starting a reinstallation:

- HGLAM has stopped.
- Preparation for installation has been completed.

For details on how to stop HGLAM, see section 3.1.2. To verify that the preparation for installation has been completed, see section 2.1.1.

To perform a reinstallation:

1. Insert the HGLAM installation CD-ROM.
2. Use Explorer to view the contents of the CD-ROM, and then execute `setup.exe`.

   The **Welcome to the Installation of HiCommand® Global Link Availability Manager (Overwrite)** dialog box appears.

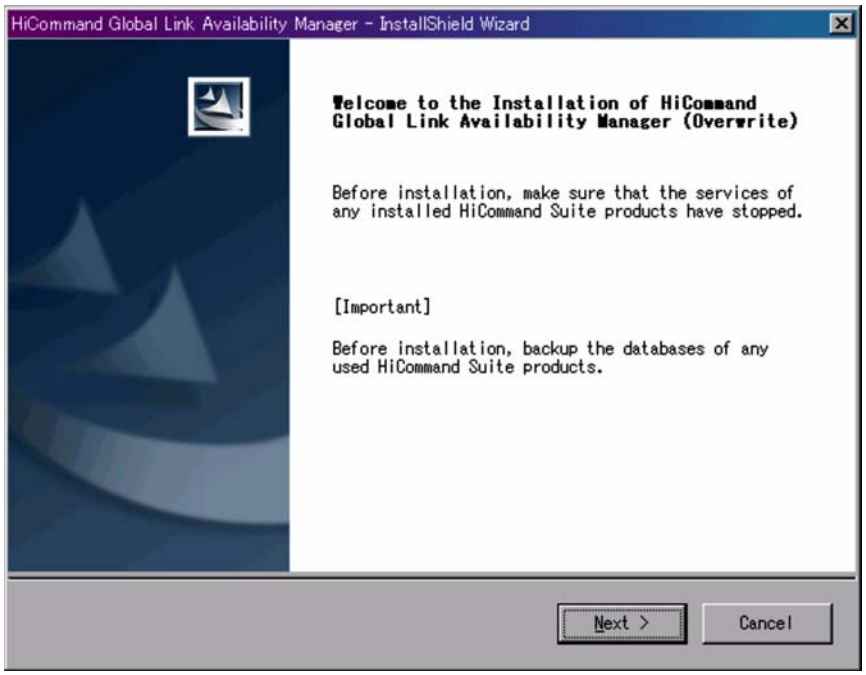

Figure 2.8 Welcome to the Installation of HiCommand® Global Link Availability Manager (Overwrite) Dialog Box

3. Click the **Next** button.

   The **Confirmation of Setup Status of Common Component Database of HiCommand® Suite** dialog box appears.

4. Check the setup status in this dialog box, and then click the **Next** button.

   The three setup statuses are:

   - Non-cluster configuration
   - Execution system node of cluster configuration
   - Standby node in a cluster configuration

   Clicking the **Next** button displays the **Confirmation Before Installation** dialog box.

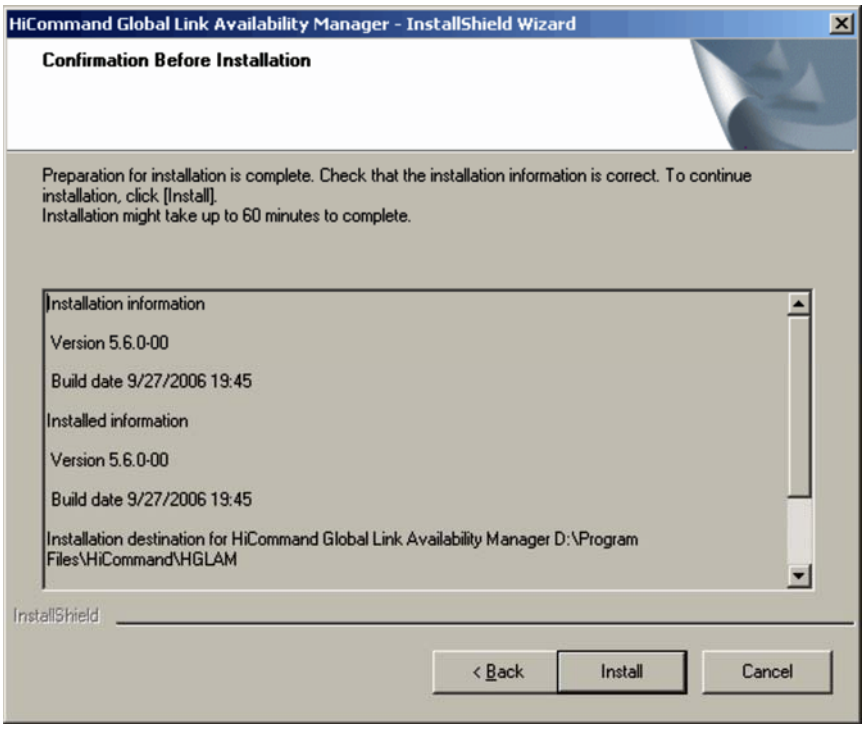

Figure 2.9 Confirmation Before Installation Dialog Box

5. After confirming that the installation settings are correct, click the **Install** button.

   Installation starts. During the installation, dialog boxes indicating the processing status appear. The HGLAM database is not initialized by an overwrite installation (except when the database files are damaged). When the installation is complete, the **Installation Complete** dialog box appears.

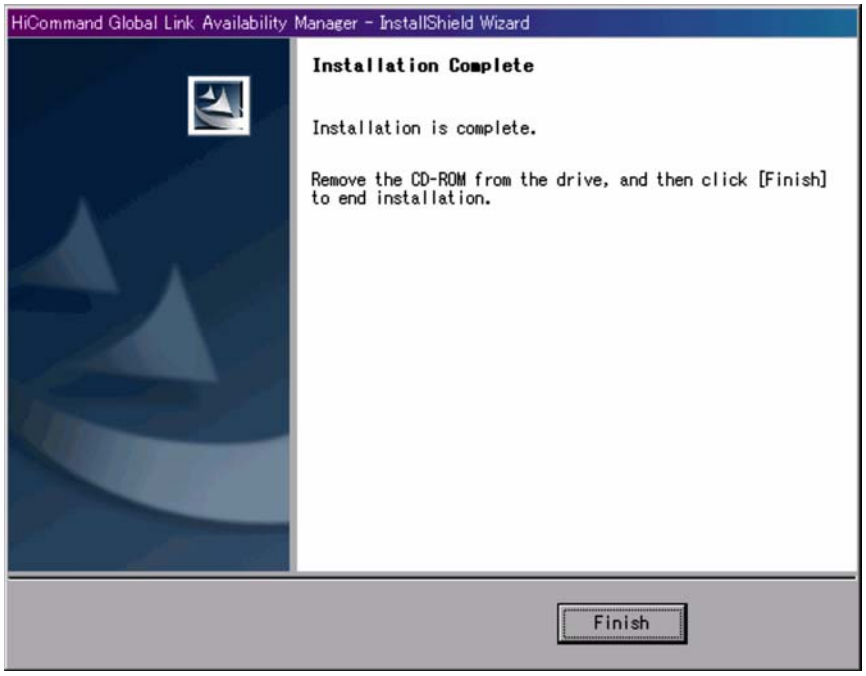

Figure 2.10 Installation Complete Dialog Box

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

   When the installation completes normally, the operating status of the HiCommand® Suite Common Component services vary depending on the setup state of the database:

   - When the setup state is a non-cluster configuration: Services start automatically, and HGLAM enters an operational state.
   - When the setup state is a cluster configuration: Services on the standby node will not start. Specify the settings for operating HGLAM in a cluster configuration.

   Make sure that the URL value is correct after the installation. To check the set value, execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdschgurl /print
```

   Executing the above command displays the URL. The following shows the URL format:

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

   If the value set for the URL is different from the information of the server on which HGLAM is installed, see the following and change the value:

   - For changing the IP address, see section 3.6.1.
   - For changing the host name, see section 3.4.
   - For changing the port number of HBase Storage Mgmt Web Service, see section 3.5.1.

2.1.4 Upgrade Installation of HGLAM

When you want to update the version of HGLAM that is already installed, perform an upgrade installation.

Make sure of the following before starting an upgrade installation:

- HGLAM has stopped.
- Preparation for installation is completed.

For details on how to stop HGLAM, see section 3.1.2. To make sure that the preparation for installation is completed, see section 2.1.1.

To perform an upgrade installation:

1. Insert the HGLAM installation CD-ROM.
2. Use Explorer to view the contents of the CD-ROM, and then execute `setup.exe`.

   The **Welcome to the Installation of HiCommand® Global Link Availability Manager (Upgrade)** dialog box appears.

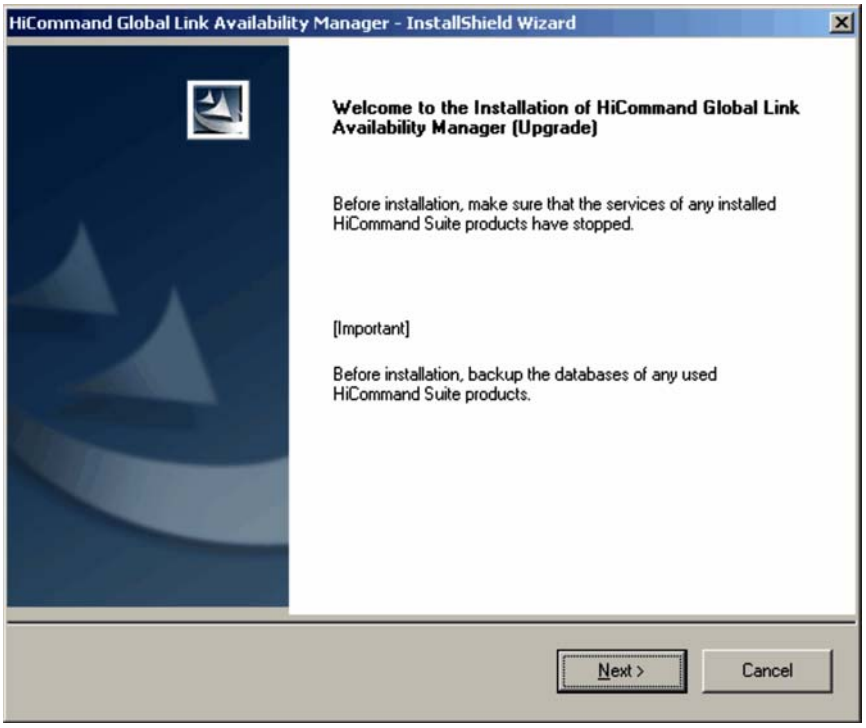

Figure 2.11 Welcome to the Installation of HiCommand® Global Link Availability Manager (Upgrade) Dialog Box

3. Click the **Next** button.

   The **Confirmation of Setup Status of Common Component Database of HiCommand® Suite** dialog box appears.

4. Check the setup status in this dialog box, and then click the **Next** button.

   The three setup statuses are:

   - Non-cluster configuration
   - Execution system node of cluster configuration
   - Standby node in a cluster configuration

   Clicking the **Next** button displays the **Confirmation Before Installation** dialog box.

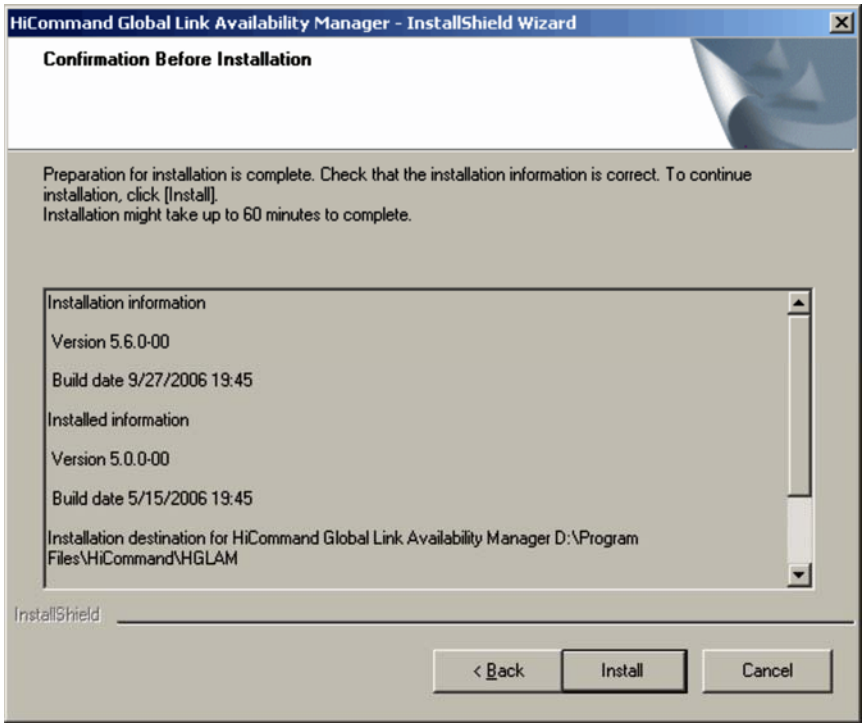

Figure 2.12 Confirmation Before Installation Dialog Box

5. After confirming that the installation settings are correct, click the **Install** button.

   Installation starts. During the installation, dialog boxes indicating the processing status appear. The HGLAM database is updated by running an upgrade installation (except when the database files are damaged). When the installation is complete, the **Installation Complete** dialog box appears.

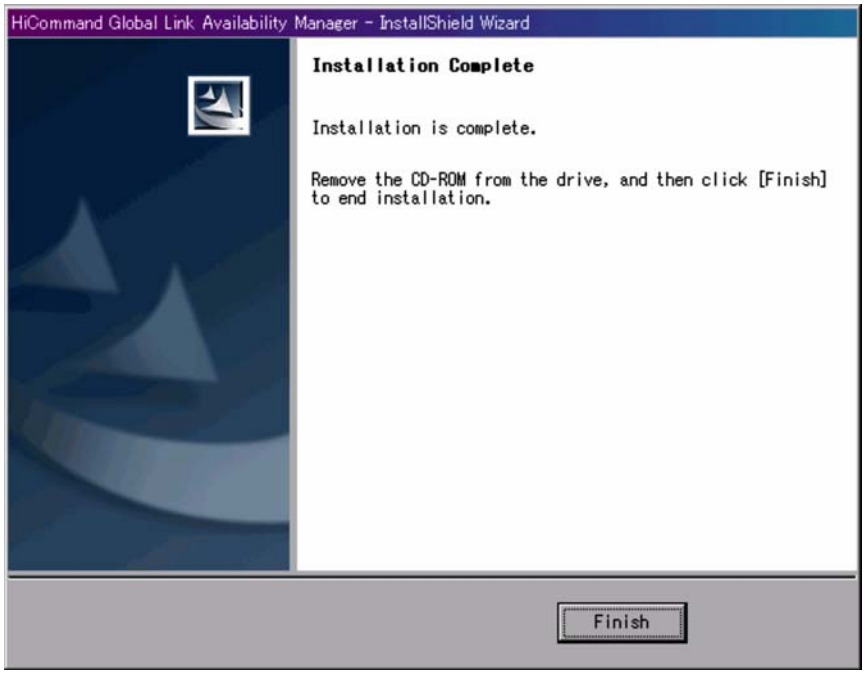

Figure 2.13 Installation Complete Dialog Box

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

   When the installation completes normally, the operating status of the HiCommand® Suite Common Component services vary depending on the setup state of the database:

   - When the setup state is a non-cluster configuration: Services start automatically, and HGLAM enters an operational state.
   - When the setup state is a cluster configuration: Services on the standby node will not start. Specify the settings for operating HGLAM in a cluster configuration.

   Make sure that the URL value is correct after the installation. To check the set value, execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdschgurl /print
   ```

   Executing the above command displays the URL. The following shows the URL format:

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

   If the value set for the URL is different from the information of the server on which HGLAM is installed, see the following and change the value:

   - For changing the IP address, see section 3.6.1.
   - For changing the host name, see section 3.4.
   - For changing the port number of HBase Storage Mgmt Web Service, see section 3.5.1.

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 section 3.3.

When an Attempt to Update the Database Has Failed

If the message ID `KAIF40094-E` appears, you must update the database.

To update the HGLAM database:

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

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /status
   ```

   If it is not running, execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /start
   ```

2. Execute the following command to update the HGLAM database:

   ```
   HGLAM-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 2.2 hglamdbupdate Command Options

Item	Description
`-x`	Specify this option to suppress the output of messages. 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 to a file. You can specify a relative path or an absolute path. Specify a path within 255 bytes. 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.

3. If services of other HiCommand® products are running, stop them.

   For details on how to check the statuses and stop services of other products, see the manuals for those products.

4. Restart HiCommand® Suite Common Component.

   To restart HiCommand® Suite Common Component, stop the services and then restart them. For details on how to start and stop the services, see section 3.1.

2.1.5 Uninstalling HGLAM

Make sure of the following before performing an uninstallation.

- You are logged on to Windows as an Administrator or a member of the Administrators group.
- No other HiCommand® product is running.
- Dialog boxes used for operating Windows services, such as Computer Management or Services, are not displayed.
- HGLAM has stopped.

For details on how to stop HGLAM, see section 3.1.2.

To uninstall HiCommand® Global Link Availability Manager:

1. In the Windows **Start** menu, choose **Programs**, **HiCommand**, **Global Link Availability Manager**, and then **Uninstall GlobalLinkAvailabilityManager**.

   The **Uninstallation of HiCommand® Global Link Availability Manager** dialog box appears.

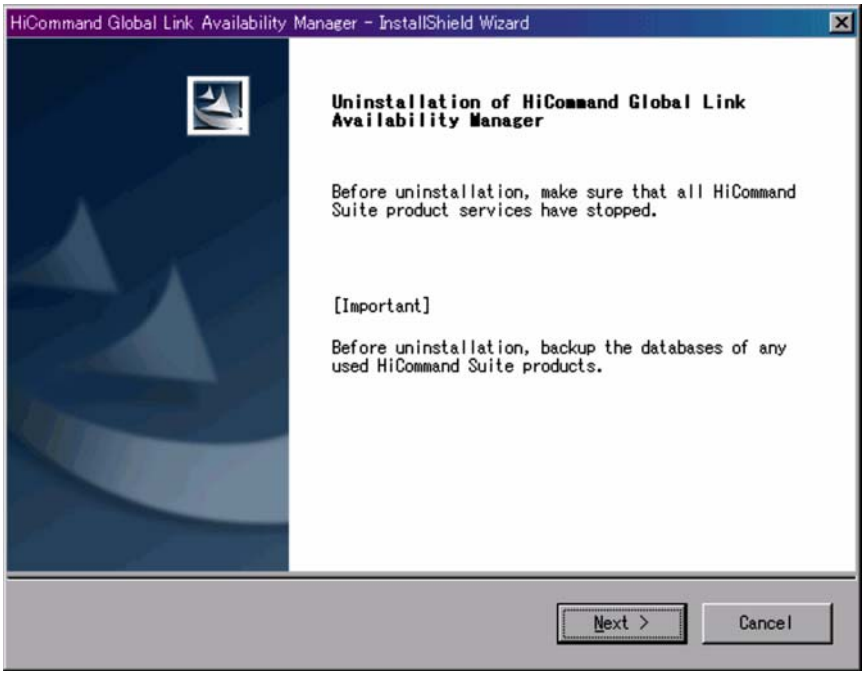

Figure 2.14 Uninstallation of HiCommand® Global Link Availability Manager Dialog Box

If the **Uninstall GlobalLinkAvailabilityManager** menu is not displayed then, in Control Panel, select **Add/Remove applications**. In the displayed dialog box, select **HiCommand® Global Link Availability Manager** and then click the **Change and Delete** button.

2. Click the **Next** button.

   If other HiCommand® Suite products have already been installed, the **Confirmation of Setup Status of Common Component Database of HiCommand® Suite** dialog box appears. Check the setup status in this dialog box, and then click the **Next** button. The three setup statuses are:

   - Non-cluster configuration
   - Execution system node of cluster configuration
   - Standby node in a cluster configuration

   Click the **Next** button to display the **Confirmation before Uninstallation** dialog box.

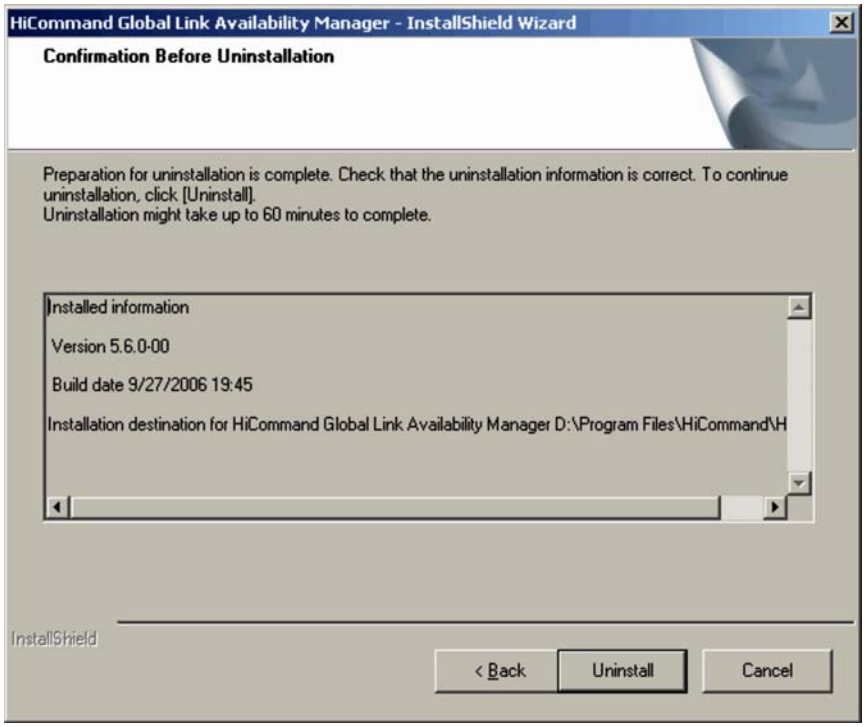

Figure 2.15 Confirmation Before Uninstallation Dialog Box

3. Click the **Uninstall** button.

   The registered software information is removed, the HGLAM database is deleted, and uninstallation starts. When the uninstallation completes normally, the **Uninstallation complete** dialog box appears.

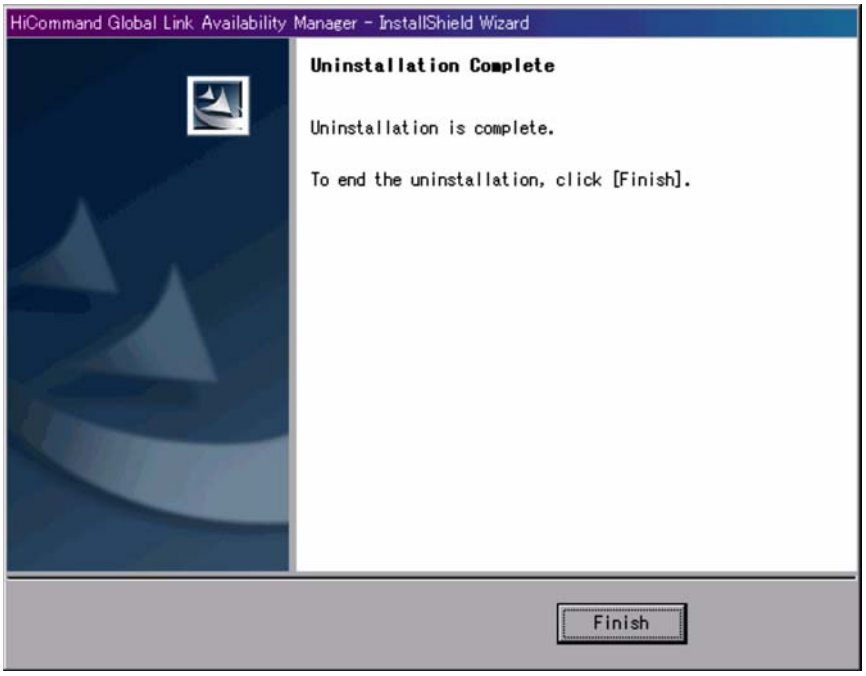

Figure 2.16 Uninstallation Complete Dialog Box

4. Click the **Finish** button to finish the uninstallation.

Note: When using Windows Firewall, make sure that the number of the port that receives SNMP traps is not added to the Windows Firewall exception list.

2.2 Setting Up License Information During Initial Login

To log in to HGLAM and start operation, set up HGLAM and then specify initial settings for the license.

To specify initial license information for HGLAM:

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

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

Example:
http://127.0.0.1:23015/GlobalLinkAvailabilityManager/
```

To check the login URL, execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdschgurl /print
```

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 2.3 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.

Chapter 3 Setting Up HGLAM

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

- Starting and Stopping HGLAM (section 3.1)
- Maintaining the HGLAM Database (section 3.2)
- Changing HGLAM Environment Settings (section 3.3)
- Changing the HGLAM Server Host Name (section 3.4)
- Changing HiCommand® Suite Common Component Port Numbers (section 3.5)
- Setting Up the HGLAM Server to use the HGLAM GUI (section 3.6)
- Setup When a Firewall is Used (section 3.7)
- Security Settings for User Accounts (section 3.8)
- Setting a Warning Banner (section 3.9)
- Generating Audit Logs (section 3.10)
- Setting Up Alert Transfer (section 3.11)

3.1 Starting and Stopping HGLAM

HGLAM is started or stopped by starting or stopping HiCommand® Suite Common Component.

HGLAM starts automatically when it is installed in a non-cluster environment. However, in the following cases, HGLAM needs to be manually started and stopped:

- When a cluster is configured
- When the property file is updated

3.1.1 Starting HGLAM

To start HGLAM, start HiCommand® Suite Common Component by executing the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /start
```

3.1.2 Stopping HGLAM

To stop HGLAM, stop HiCommand® Suite Common Component. If other HiCommand® products have already been installed on the same server machine, stop the services of those products, and then stop HiCommand® Suite Common Component by executing the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
```

3.1.3 Checking HGLAM Status

To check the HGLAM status, check the HiCommand® Suite Common Component status by executing the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /status
```

When the following messages are displayed, HiCommand® Suite Common Component is running properly.

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

3.2 Maintaining the HGLAM Database

This section describes the following operations for the HGLAM database:

- Backing up and restoring the database
- Migrating (exporting and importing) the database

To perform database operations, you need to execute a backup and restore of the HGLAM 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 3.1 Backing Up and Restoring Versus Exporting and Importing

Item	Backing up and restoring	Exporting and importing
Conditions of the HiCommand® Suite Common Component version	No limitation.	HiCommand® 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 HiCommand® products ▪ The HiCommand® Suite Common Component database	▪ Databases for HiCommand® products ▪ User information included in the HiCommand® 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 HiCommand® products ▪ Installation locations for each HiCommand® product, HiCommand® Suite Common Component, each HiCommand® product database, and HiCommand® Suite Common Component database ▪ The IP address and host name of the machine	▪ The HiCommand® products whose databases to be imported must be installed. ▪ The versions of the installed HiCommand® products must be the same as or higher than the ones on the export source machine.

3.2.1 Backing Up the HGLAM Database

Hitachi recommends that you back up the database of HGLAM and the databases of HiCommand® products regularly. In addition, you should always back up these databases before performing the following operations:

- Reinstallation or version upgrade installation of HGLAM
- Installing or uninstalling another HiCommand® product on a server in which HGLAM has been installed
- Installing or uninstalling HGLAM on a server in which another HiCommand® product has been installed

The following procedure describes how to back up the HGLAM database and other HiCommand® product databases. In this procedure, you also acquire a backup of the HGLAM property files and the path availability information (path status log), in addition to the databases.

To back up the HGLAM database and other HiCommand product databases:

1. Stop HiCommand® Suite Common Component.

   If other HiCommand® products are installed, stop other HiCommand product services, and then stop HiCommand® Suite Common Component.

   For details on how to stop other HiCommand® product services, see the documentation for those products.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

2. Start HiRDB.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbsrv /start
   ```

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

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsbackups /dir
   backup-destination-folder-name
   ```

   Use an absolute path on the local disk to specify *backup-destination-folder-name*. 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 HiCommand® products installed on the server on which the above command is executed. At the same time, the setting files for HiCommand® Suite Common Component and other HiCommand® products are also backed up.

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

   ```
   HGLAM-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*.

3.2.2 Restoring the HGLAM Database

This section describes how to restore the HGLAM database and the databases of all installed HiCommand® products. In this procedure, you also restore the HGLAM property files and the path availability information (path status log), in addition to the databases.

To restore the HGLAM database or to restore the databases of all installed HiCommand® products:

1. If services of other HiCommand® products are running, stop them.

   For details about how to check statuses and stop services of other products, see the documentation for those products.

2. Execute the following command to stop HiCommand® Suite Common Component:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

3. Execute the following command to restore the HGLAM database:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdb /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 HGLAM database, specify /type HGLAM or /type GlobalLinkAvailabilityManager.

   To restore the databases of all installed HiCommand® products, including HGLAM, execute the command by specifying /type ALL.

   To restore the databases after uninstalling and then re-installing all the HiCommand® products, specify /type ALL.

   Note: If you restore the databases by specifying /type ALL, the states of other HiCommand® 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.

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

   ```
   HGLAM-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.

5. Execute the following command to start HiCommand® Suite Common Component:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /start
```

3.2.3 Migrating the HGLAM Database

If HiCommand® products are used for an extended period of time, you may need a higher performance machine in order to accommodate product version upgrades and the increased number of objects to be managed. If this occurs, database migration will be one important component of the machine replacement process. In HiCommand® products, you can migrate the database by using the `hcmdsdbtrans` command. The `hcmdsdbtrans` command migrates all information stored in the database of each HiCommand® product as well as user information managed by the HiCommand® Suite Common Component.

In the following two cases, you can use the `hcmdsdbtrans` command to migrate the HGLAM 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 HiCommand® products are different from the ones on the migration source
- Migration to a machine on which the versions of HiCommand® products are newer than the ones on the migration source

3.2.3.1 Notes When Migrating the Database

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

Notes for types and versions of the HiCommand® products on the migration source and migration destination servers:

- The database of a HiCommand® product that is not installed on the migration destination server cannot be migrated. Install all necessary HiCommand products on the migration destination server.
- If any of the versions of the HiCommand® 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 HiCommand® products whose versions are the same as or higher than the ones on the migration source server.
- The database of Replication Monitor version 4.2 or earlier cannot be migrated. If you need to migrate this database, upgrade the Replication Monitor to version 5.0 or later on both the migration source and destination servers beforehand.
- The following limitations apply when you migrate the Tuning Manager database:

  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 HiCommand® products already exists.
- If the databases of several HiCommand® 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 every product can be migrated.
- You cannot perform migration to integrate the HiCommand® products that were running on multiple management servers on to one management server because user information will be overwritten with each successive migration.

3.2.3.2 General Procedure for Migrating Databases

To migrate databases:

1. Install, on the migration destination server, the HiCommand® 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.

3.2.3.3 Installing the HiCommand® Products on the Migration Destination Server

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

3.2.3.4 Exporting the Database at the Migration Source Server

To export the database of HGLAM, 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 HGLAM database

- The folder storing the HiCommand® Common Component database (excluding the `SYS` folder and the folders beneath it)

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

The folder storing the HiCommand® Suite Common Component database is *HiCommand-Suite-Component-installation-folder*`\database`.

This capacity is a guideline value applied when only the HGLAM database is installed. If HiCommand® products other than HGLAM are also installed, take the capacities of those databases into account as well.

Caution: If the total capacity of the database exceeds 2 GB, an attempt to create the archive file fails when the database is exported. In this case, instead of using the archive file, transfer to the migration destination the database information collected when exporting the database.

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

#: If the HGLAM version on the migration source server is 5.0, step 4 and 6 are not necessary.

To export the database at the migration source server:

1. Stop HiCommand® Suite Common Component.

   If other HiCommand® products are installed, stop other HiCommand® product services, and then stop HiCommand® Suite Common Component.

   For details on how to stop other HiCommand® product services, see the documentation for those products.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

2. Start HiRDB.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbsrv /start
   ```

3. Execute the following command to export the database:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbtrans /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 `hcmdsdbtrans` 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\Base\bin\hcmdsdbtrans /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):

```
HGLAM-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, it should be an empty folder.

   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*.

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*.

3.2.3.5 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.

To import the database at the migration destination server:

1. Stop HiCommand® Suite Common Component.

   If other HiCommand® products are installed, stop other HiCommand® product services, and then stop HiCommand® Suite Common Component.

   For details on how to stop other HiCommand® product services, see the documentation for those products.

   Execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
```

2. Start HiRDB.

   Execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbsrv /start
```

3. Execute the following command to import the database:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbtrans /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 `hcmdsdbtrans` 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 HGLAM database, specify `/type HGLAM` or `/type GlobalLinkAvailabilityManager`.

To import the databases of all installed HiCommand® products, including HGLAM, execute the command by specifying either `/type ALL` or the names of the HiCommand® products to be imported, which are separated by using a comma as the delimiter. For the names of other HiCommand® 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 HiCommand® 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 HiCommand® products. To migrate databases of HiCommand® products other than HGLAM, 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:

```
HGLAM-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.

To migrate the database from HGLAM version 5.0 to version 5.6, execute the following command:

```
HGLAM-installation-folder\bin\hglamimport /dbupdate
```

After the import processing is complete, the HGLAM 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 HiCommand® Suite Common Component:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /start
```

3.3 Changing HGLAM Environment Settings

To change the HGLAM environment settings, edit the appropriate property files.

Location of files:

```
HGLAM-installation-folder\conf
```

Files:

- `server.properties` (HGLAM server settings file)
- `logger.properties` (HGLAM log file settings file)
- `database.properties` (HGLAM 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:

   - 3.3.1
   - 3.3.2
   - 3.3.3

2. Restart HGLAM.

   To restart HGLAM, stop the services, and then start them again. For details on how to start and stop the services, see section 3.1.

Note: If the format or value of the properties in the `server.properties` or `database.properties` file is incorrect, even if HiCommand® Suite Common Component starts, HGLAM will not start. Check if the `KAIF10002-E` message has been output to the HGLAM message log (`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 HGLAM. 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 HGLAM will start.

The HGLAM message log is stored in the following location:

```
HGLAM-installation-folder\logs
```

3.3.1 Changing HGLAM Server Settings

To change the HGLAM 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 HGLAM server settings.

Table 3.2 HGLAM Server Properties (server.properties)

No.	Property Name	Description
1	`server.status.check_interval`	Specifies the interval for checking the available period of status management. Specifiable value: 1 to 3600 (minutes) Default: 10 (minutes)
2	`server.status.available_period`	Specifies the available period of status management. Specifiable value: 1 to 3600 (minutes) Default: 60
3	`server.thread.max_size`	Specifies the maximum number of threads that can be executed concurrently. Specifiable value: 1 to 50 Default: 15

No.	Property Name	Description
4	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 HGLAM 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
5	server.dbms.sweep_init	Specifies the time from server startup until free-page collection starts. Specifiable value: 1 to 60 (minutes) Default: 5
6	server.dbms.sweep_interval	Specifies the interval between free-page collections. Specifiable value: 60 to 100000 (minutes) Default: 10080
7	server.agent.max_retry_count	Specifies the maximum number of retries for checking whether HiCommand® Suite Common Agent Component has finished processing. Specifiable value: 1 to 60 Default: 3
8	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
9	server.snmp.trap	Specifies whether to enable the SNMP trap reception function. Specify `true` to enable the function. Specify `false` to disable it. Specifiable value: `true` or `false` Default: `true`[#1]
10	server.snmp.trap_port_num	Specifies the port number for receiving SNMP traps. *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: 162[#1]
11	server.snmp.trap_thread_num	Specifies the number of threads for processing SNMP traps. Specifiable value: 1 to 10 Default: 3
12	server.snmp.trap_max	Specifies the maximum number of SNMP traps (alerts) to be retained. Specifiable value: 1000 to 30000 Default: 10000

No.	Property Name	Description
13	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 Default: true
14	server.snmp.trap_community	Specifies the SNMP Community value. Specifiable value: String of 15 or fewer characters Default: public
15	server.snmp.trap_ip_address	Specifies the IP address of the SNMP trap destination. The SNMP trap destination is the server in which HGLAM is installed. If you change the IP address for the server in which HGLAM is installed, make sure to change the value of this property. *Note:* If you do not change the value of this property when the IP address for the server in which HGLAM is installed is changed, reception of SNMP traps becomes unavailable. Specifiable value: String of 15 or fewer characters Default: --[#1]
16	gui.indicator.auto_refresh_interval	Specifies the automatic refresh interval for the Dashboard menu in the HGLAM GUI. Specifiable value: 1 to 10000 (minutes) Default: 1
17	gui.table.selectable_rows_per_page	This value is used in the internal processing of HGLAM. Do not change this value. Default: 100, 200
18	server.snmp_transfer.enable	Specifies whether to enable alert transfer. Specify true to enable alert transfer. Specify false to disable it. Specifiable value: true or false Default: false
19	server.snmp_transfer.ip_address	Specifies the IP address of the alert transfer destination server. Specifiable value: Character string Default: None
20	server.snmp_transfer.port_num	Specifies the port number of the alert transfer destination server. Specifiable value: Number from 1 to 65535 Default: 162
21	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

No.	Property Name	Description
22	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
23	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
24	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
25	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
26	server.auto_refresh.interval	Specifies the automatic update interval for the host. Specifiable value: 180 to 2880(minutes) Default: 180
27	server.auto_refresh.thread_num	Specifies the maximum number of automatic update operations that can be performed concurrently on the hosts. Specifiable value: 1 to 50 Default: 5

No.	Property Name	Description
28	server.pathreport.enable	Specifies whether to allow HGLAM to acquire the path availability information (path status log) from HDLM for output in a report. Specify true to allow HGLAM to acquire the information. Specify false to not allow HGLAM to acquire the information. *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 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
29	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: PathStatusLog_*host-IP-address_date*.csv 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 section 3.3.1.1. If you use the default value for the folder, that folder is automatically deleted when HGLAM is uninstalled. 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 HGLAM starts. ▪ Do not edit the file stored in this folder because it is used for the report output in the HGLAM GUI. If you edit the file, the report might not be output correctly. Specifiable value: Valid absolute path of 150 or fewer bytes[#2] Default: *HGLAM-installation-folder*\\pathreport

No.	Property Name	Description
30	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 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
31	getlogs.pathreport.get_mode	Specifies the method of acquiring the path availability information (path status log), as the HGLAM diagnostic information[#3]. 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 proceeding 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 a value for the properties in No. 31 and No. 33 of this table.) 3: Acquires all of the folders specified for server.pathreport.log_location.. Default: 0
32	getlogs.pathreport.host	Specifies the IP address of the target host or hosts when acquiring the path availability information (path status log), as the HGLAM diagnostic information[#3]. 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)
33	getlogs.pathreport.startDate	Specifies the start date for acquisition of the path availability information (path status log), as the HGLAM diagnostic information[#3]. 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.)
34	getlogs.pathreport.endDate	Specifies the end date for acquisition of the path availability information (path status log), as the HGLAM diagnostic information[#3]. 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.)

#1: These values are replaced with the values that are specified during the installation.

#2: 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 HGLAM administrator.

#3: For details about how to acquire HGLAM diagnostic information, see section 7.3.1.

3.3.1.1 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.

To move the output path availability information (path status log) to a new folder:

1. Stop HiCommand® Suite Common Component.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

2. Export the path availability information (path status log).

   Execute the following command:

   ```
   HGLAM-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 section 3.3.

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

   Execute the following command:

   ```
   HGLAM-installation-folder\bin\hglamimport /report export-destination-folder-name
   ```

   Before executing the command, you must either delete the folder that you specified in step 3 or make sure that the folder is empty.

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

   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.

5. Start HiCommand® Suite Common Component.

   Execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /start
```

3.3.2 Changing HGLAM Log File Settings

To change the settings for HGLAM log files (`HGLAM_Message`*n*`.log`), edit the `logger.properties` file. The following table describes the properties that are used to change the HGLAM log file settings.

Table 3.3 HGLAM 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 syslog. Specifiable value: 0, 10, 20, or 30 Default: 0
4	`logger.log_level`	Specifies the logging level (threshold) for output to the log file. Specifiable value: 0, 10, 20, or 30 Default: 20

3.3.3 Changing HGLAM Database Settings

To change the HGLAM database settings, edit the `database.properties` file. The following table describes the properties that are used to change the HGLAM database settings.

Table 3.4 HGLAM 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

3.4 Changing the HGLAM Server Host Name

To change the host name for the management server on which HGLAM is installed, you must edit several settings files beforehand.

To edit the settings files:

1. Before changing the host name, write down the host name as a precaution.

   Execute the `hostname` command to check the host name. The host name to be specified in the settings file is case sensitive.

2. Stop all services for other HiCommand® products.

   For details on how to stop services for other HiCommand® products, see the manual for each product.

3. Execute the following command to stop HiCommand® Suite Common Component:

   HiCommand-Suite-Common-Component-installation-folder`\bin\hcmdssrv /stop`

4. If the SSL settings have been configured, configure them again.

   Use the new host name to reconfigure the SSL settings. For details on how to configure SSL settings, see Chapter 5.

5. Edit the `httpsd.conf` file.

   Change the value for the `ServerName` parameter to the new host name.

   The following describes the storage destination for the `httpsd.conf` file.

   HiCommand-Suite-Common-Component-installation-folder`\httpsd\conf\`

   If SSL is set, you must also do the following:

   - Change the host name specified for the `<VirtualHost>` tag to the new host name.
   - Change the value for the `ServerName` parameter in the `<VirtualHost>` tag to the new host name.

6. Edit the `pdsys` file and `def_pdsys` file.

   Change the value for the `-x` option of the `pdunit` parameter to the new host name or change the loopback address (127.0.0.1). Specify a virtual host name for a cluster configuration. If you change the value to 127.0.0.1, this step is no longer required even if any changes are made to the host name in the future.

   The following describes the storage destinations for the `pdsys` file and `def_pdsys` file.

   - *HiCommand-Suite-Common-Component-installation-folder*`\HDB\conf\pdsys`
   - *HiCommand-Suite-Common-Component-installation-folder*`\database\work\def_pdsys`

7. Edit the pdutsys file and def_pdutsys file.

   Change the value for the pd_hostname parameter to the new host name or change the loopback address (127.0.0.1). If you change the value to 127.0.0.1, this step is no longer required even if any changes are made to the host name in the future. If the pd_hostname parameter does not exist, add the pd_hostname parameter and specify the new host name or loopback address.

   For a cluster configuration, edit the pdutsys file and def_pdutsys file on both the primary node and secondary node. In such a case, for pd_hostname, specify the host name for the primary node.

   The following describes the storage destinations for the pdutsys file and def_pdutsys file.

   - *HiCommand-Suite-Common-Component-installation-folder*\HDB\conf\pdutsys
   - *HiCommand-Suite-Common-Component-installation-folder*\database\work\def_pdutsys

8. Edit the HiRDB.ini file.

   Change the value for the PDHOST parameter to the new host name or change the loopback address (127.0.0.1). If you change the value to 127.0.0.1, this step is no longer required even if any changes are made to the host name in the future. Specify a virtual host name for a cluster configuration.

   The following describes the storage destination for the HiRDB.ini file.

   - *HiCommand-Suite-Common-Component-installation-folder*\HDB\conf\emb\HiRDB.ini

9. 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 describes the storage destination for the cluster.conf file.

   - *HiCommand-Suite-Common-Component-installation-folder*\conf\cluster.conf

10. Change the host name for the management server, and then restart the machine.

11. Execute the following command to make sure that HiCommand® Suite Common Component is running:

    ```
    HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /status
    ```

12. Execute the hcmdschgurl command to change the host name in the URL for starting HGLAM GUI.

    For details on how to use the hcmdschgurl command, see section 3.6.1.

3.5 Changing HiCommand® Suite Common Component Port Numbers

The following table lists and describes the port numbers used by HiCommand® Suite Common Component:

Table 3.5 Ports Used by HiCommand® Suite Common Component

Network Port	Description
23015/tcp	This port is used to access non-SSL HBase Storage Mgmt Web Service. If you want to change this port number after installation, see section 3.5.1.
23016/tcp	This port is used by Web browsers to access SSL HBase Storage Mgmt Web Service. If you want to change this port number after installation, see section 3.5.1.
23017/tcp	This port is used by HBase Storage Mgmt Web Service to access HBase Storage Mgmt Common Service through an AJP connection. If you want to change this port number after installation, see section 3.5.2.
23018/tcp	This port is used by HBase Storage Mgmt Common Service to receive a stop request. If you want to change this port number after installation, see section 3.5.4.
23032/tcp	This port is used by HiRDB. If you want to change this port number after installation, see section. 3.5.4.
23019/tcp to 23031/tcp, 23033/tcp, and 23034/tcp	These port numbers are reserved.
45001/tcp to 49000/tcp	These ports are used by HiRDB internal communication. Do not use these ports.

To change the HiCommand® Suite Common Component port numbers after HGLAM server installation:

1. If services of other HiCommand® products are running on the server machine, stop them.

   For details about how to stop services of other HiCommand® products, see the documentation for those products.

2. Execute the following command to stop HiCommand® Suite Common Component:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

3. 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:

   - 3.5.1
   - 3.5.2
   - 3.5.3
   - 3.5.4

4. Execute the following command to start HiCommand® Suite Common Component:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /start
   ```

5. If other HiCommand® products have been installed on the server, start the service of each product.

   To start the services, see the documentation for those products.

3.5.1 Changing Port Numbers for Accessing the HBase Storage Mgmt Web Service

To change the port used to access the HBase Storage Mgmt Web Service, change the port number specified in the `httpsd.conf` file.

To change the port number:

1. Open the `httpsd.conf` file at the following location:

```
HiCommand-Suite-Common-Component-installation-folder\httpsd\conf\httpsd.conf
```

2. If you want to change the port number for HTTP communication, change the port number in the `Listen` directive where 23015 is specified by default. To change the port number for HTTPS communication (using SSL), change the port number for the `Listen` directive where 23016 is specified by default, and the value for `VirtualHost`.

```
Listen 23015
SSLDisable

Listen 23016
<VirtualHost www.example.com:23016>
```

To use SSL, perform SSL setup in addition to changing the port number. For details about SSL setup, see Chapter 5.

3.5.2 Changing the Port Number Used to Access the HBase Storage Mgmt Common Service

To change the port used by HBase Storage Mgmt Common Service that uses the AJP (Apache JServ Protocol) for connection, change the port number in the `workers.properties` and `usrconf.properties` files.

3.5.2.1 Editing the workers.properties file

1. Open the `workers.properties` file at the following location:

   HiCommand-Suite-Common-Component-installation-folder`\CC\web\redirector\workers.properties`

2. Change the port number in the entry `worker.worker1.port=23017`.

3.5.2.2 Editing the usrconf.properties file

1. Open the `usrconf.properties` file at the following location:

   HiCommand-Suite-Common-Component-installation-folder`\CC\web\containers\HiCommand\usrconf\usrconf.properties`

2. Change the port number in the entry `webserver.connector.ajp13.port=23017`.

3.5.3 Changing the Port Number Used to Stop the HBase Storage Mgmt Common Service

To set the port that receives a stop request for HBase Storage Mgmt Common Service, specify the port number in the `usrconf.properties` file.

To specify the port used to stop HBase Storage Mgmt Common Service:

1. Open the `usrconf.properties` file at the following location:

   HiCommand-Suite-Common-Component-installation-folder`\CC\web\containers\HiCommand\usrconf\usrconf.properties`

2. Specify the port number in the entry `webserver.shutdown.port=`.

3.5.4 Changing Port Numbers for Accessing HiRDB

To change the port used by HiRDB, change the port number specified in the `HiRDB.ini`, `pdsys`, and `def_pdsys` files.

3.5.4.1 Editing the HiRDB.ini file

1. Open the `HiRDB.ini` file at the following location:

   HiCommand-Suite-Common-Component-installation-folder\HDB\CONF\emb\HiRDB.ini

2. Change the port number in the entry `PDNAMEPORT=23032`.

3.5.4.2 Editing the pdsys file

1. Open the `pdsys` file at the following location:

   HiCommand-Suite-Common-Component-installation-folder\HDB\CONF\pdsys

2. Change the port number in the entry `pd_name_port=23032`.

3.5.4.3 Editing the def_pdsys file

1. Open the `def_pdsys` file at the following location:

   HiCommand-Suite-Common-Component-installation-folder\database\work\def_pdsys

2. Change the port number in the entry `pd_name_port=23032`.

3.6 Setting Up the HGLAM Server to Use the HGLAM GUI

This section describes the settings for changing the URL used for starting the HGLAM GUI, and the settings for adding the **Go** menu and the **Links** menu item to the HGLAM GUI.

3.6.1 Changing the HGLAM Login URL

If you have changed the following HGLAM settings, you must change the URL that is used for starting the HGLAM GUI.

- The IP address or host name of the server on which HGLAM is installed
- The port number used by HBase Storage Mgmt Web Service
- The settings for using SSL, or for stopping the use of SSL

To change the URL used for starting the HGLAM GUI, execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdschgurl /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
```

To check *old-URL*, execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdschgurl /print
```

3.6.2 Adding the Go and Links Menus

On the HGLAM 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 on the HGLAM GUI.

To register links, execute the following command:

```
hcmdslink {/add | /delete } /file user-setup-application-file[/nolog] /user user-ID /pass
password
```

Option

Table 3.6 hcmdslink 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 HGLAM. Specify the ID for the user who has the Admin permission for the HGLAM management.

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:

```
@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
```

Figure 3.1 Format of the User Setup Application File

Table 3.7 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 HGLAM GUI (maximum 256 bytes).
@DISPLAYNAME *display-in-links-dialog-box*	Specify the link name to be displayed in the Links dialog box (maximum 60 bytes). If you do not specify this item, the value specified in @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).
@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.

```
@TOOL-LINK
@NAME SampleApp
@URL http://SampleApp/index.html
@DISPLAYNAME SampleApplication
@DISPLAYORDER 1
@ICONURL http://SampleApp/graphic/icon.gif
@TOOL-END
```

Figure 3.2 Example of the User Setup Application File

3.7 Setup When a Firewall is Used

When a firewall is already configured, if you enable Windows Firewall after installing HGLAM, you need to perform the following setup:

3.7.1 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 3.8 Port Numbers Required for Communications between a Management Server and Management Client

Port Number	Source of Communication	Destination of Communication	Remarks
23015/tcp#	Management client	Management server	This setting is required for non-SSL communications.
23016/tcp#	Management client	Management server	This setting is required for SSL communication.

#: The port number is changeable. For details on port numbers used for communications between a Management Server and Management Client, see section 3.5.1.

Table 3.9 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 when the HDLM version on the management host is 5.8 or later.
24042/tcp#	Management server	Management host	This setting is required when the HDLM version on the management host is 5.8 or later.
23011/tcp#	Management server	Management host	This setting is required when the HDLM version on the management host is earlier than 5.8.
23013/tcp#	Management server	Management host	This setting is required when the HDLM version on the management host is earlier than 5.8.
162/udp#	Management host	Management server	This setting is required when 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, if the HDLM version on the management host is 5.8 or later, see section A.2, if the HDLM version of the management host is earlier than 5.8, see the manual *HiCommand® Device Manager Agent Installation Guide*. For details on the port number required for receiving SNMP traps, see the part that describes the `server.snmp.trap_port_num` property in section 3.3.1.

3.7.2 Settings for Windows Firewalls

If you enable Windows Firewall after installing HGLAM, you must register HiCommand® Suite Common Component and a port number that receives SNMP traps as an exception in the Windows Firewall exceptions list.

To register HiCommand® Suite Common Component and a port number as an exception:

1. Execute the following command to register HiCommand® Suite Common Component as an exception:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsfwcancel.bat
   ```

2. Register a port number that receives SNMP traps as an exception in the Windows Firewall exceptions list.

   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.

3.8 Security Settings for User Accounts

To prevent users' passwords from being guessed by a third party, HGLAM 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 HGLAM GUI to specify the security settings. However, when the system is operating in a cluster environment, the settings from the HGLAM 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 operate the HGLAM GUI, see Help.

Caution:

- When installing version 5.1 or later of HiCommand® Suite Common Component, the user account log function and password complexity check function will be usable. These functions are enabled for users of all HiCommand® Suite products, so the following problems might occur in operations of HiCommand® 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 is unchangeable, or a user account is not addable.

  The specified password might not follow the password-entry rules. Specify an appropriate password, following the output message.

The password conditions and settings related to account locking are implemented from the `security.conf` file.

In a Windows system, the `security.conf` file is stored in the following folder:

installation-folder-for-HiCommand-Suite-Common-Component\conf\sec

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.

When you change a setting in the `security.conf` file, the change takes effect immediately.

The following table lists and describes the items specified in the `security.conf` file.

Table 3.10 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)

No.	Property Name	Description
6	password.check.userID	Specifies whether the password can be the same as the user ID. When true is specified, 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	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. Note, however, that the built-in account (user ID: System) cannot be locked. If you specify 0, any number of unsuccessful login attempts is allowed.# Specifiable value: 0 to 10 Default: 0

#:

When the single sign-on feature is used

Unsuccessful login attempts by a user for other HiCommand® 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. For example, if you change the value for the number of unsuccessful login attempts from 5 to 2, the user account of a user who has already failed to log in three times is still valid. However, if the user again fails to log in, the user account is locked.

If the user account of a logged-in user is automatically locked, the user can continue operation until he or she logs out. However, that account cannot be used to log in again.

Unlocking a user account

Use the HGLAM GUI to unlock a user account. For details on how to unlock the user account, see Help.

3.9 Setting a Warning Banner

In HiCommand® Suite Common Component version 5.1 or later, 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.

The message displayable on the Login panel must be no more than 1,000 characters. 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 HGLAM GUI to specify the warning banner. However, when the system is operating in a cluster environment, the settings from the HGLAM 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 operate the HGLAM GUI, see Help.

3.9.1 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 show an example of message editing, and the results (the warning banner) after the message has been registered.

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.
```

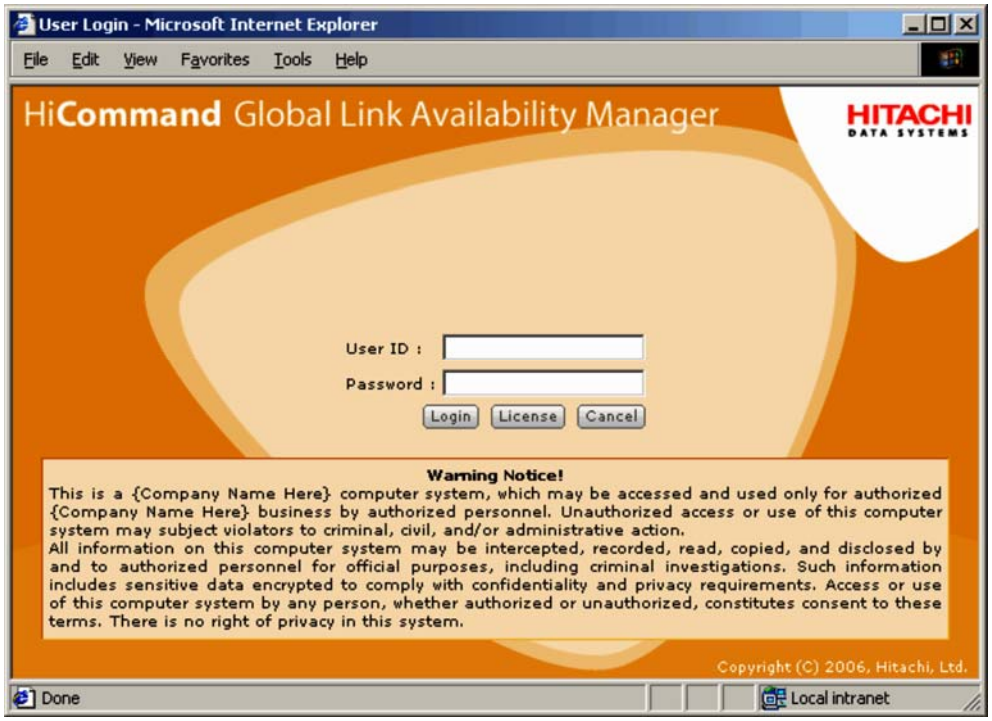

Figure 3.3 Displayed Results After Registering the Message

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-HiCommand-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.

3.9.2 Registering Message

To register an edited message, execute the following command:

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsbanner /add /file
file-name [/locale locale-name]
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsbanner /add /file C:\W_Banner\wbfile1 /locale en
```

If you executed the command without specifying `/locale` *`locale-name`*, you can also use the HGLAM GUI to edit the registered contents. However, if you use the HGLAM GUI to edit the contents, the HTML tags that can be used are limited.

If you operate the HGLAM 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 HGLAM GUI is set, according to the priority of the language set for the Web browser on the HGLAM client.

Caution: If a message for the specified locale is already registered, it will be updated by being overwritten.

3.9.3 Deleting Message

To delete an edited message, execute the following command:

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsbanner /delete [/locale
locale-name]
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsbanner /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.

3.10 Generating Audit Logs

You can generate audit logs for HGLAM and other Hitachi storage-related products in order 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 3.11 Types of Audit Logs

Log Type	Description
`StartStop`	Events indicating starting or stopping of hardware or software ▪ Starting or stopping an OS ▪ Starting or stopping a hardware component (including a microprogram) ▪ Starting or stopping software on a Lightning/Thunder series machine, software on the SVP, or a HiCommand® product
`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 (LUN Security of IP/FC) ▪ 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
`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

Log Type	Description
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
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 HGLAM. For details on the audit logs of other products, see the documentation for those products.

3.10.1 Categories of Information Output to Audit Logs in HGLAM, and Audit Events

The following table lists the categories of information output to audit logs in HGLAM and the audit events. A severity level is set for each audit event.

Table 3.12 Categories of Information Output to Audit Logs, and Audit Events

Category	Description	Audit Event	Severity
Authentication	Administrator or end user authentication	Login succeeded.	6
		Login failed (the specified user ID or password is invalid).	4
		Login failed (login was attempted by a locked user).	4
		Login failed (login was attempted by a nonexistent user).	4
		Login failed (no permissions).	3
		Login failed (authentication failed).	4
		Logout succeeded.	6
	Automatic locking of an account	Account was locked automatically (successive authentication attempts failed, or the account has expired).	4
ConfigurationAccess	User registration	User registration succeeded.	6
		User registration failed.	3
	User deletion	A single user was deleted successfully.	6
		Deletion of a single user failed.	3
		Multiple users were deleted successfully.	6
		Deletion of multiple users failed.	3
	Changing the password (from the administrator window)	The administrator changed the password successfully.	6
		The administrator could not change the password.	3
	Changing the password (from a local user window)	Authentication to determine whether the old password is correct failed.	3
		The password of the login user was changed successfully from the local user window.	6
		The password of the login user could not be changed from the local user window.	3
	Changing a profile	The profile was changed successfully.	6

3.10.1 Categories of Information Output to Audit Logs in HGLAM, and Audit Events

The following table lists the categories of information output to audit logs in HGLAM and the audit events. A severity level is set for each audit event.

Table 3.12 Categories of Information Output to Audit Logs, and Audit Events

Category	Description	Audit Event	Severity
Authentication	Administrator or end user authentication	Login succeeded.	6
		Login failed (the specified user ID or password is invalid).	4
		Login failed (login was attempted by a locked user).	4
		Login failed (login was attempted by a nonexistent user).	4
		Login failed (no permissions).	3
		Login failed (authentication failed).	4
		Logout succeeded.	6
	Automatic locking of an account	Account was locked automatically (successive authentication attempts failed, or the account has expired).	4
ConfigurationAccess	User registration	User registration succeeded.	6
		User registration failed.	3
	User deletion	A single user was deleted successfully.	6
		Deletion of a single user failed.	3
		Multiple users were deleted successfully.	6
		Deletion of multiple users failed.	3
	Changing the password (from the administrator window)	The administrator changed the password successfully.	6
		The administrator could not change the password.	3
	Changing the password (from a local user window)	Authentication to determine whether the old password is correct failed.	3
		The password of the login user was changed successfully from the local user window.	6
		The password of the login user could not be changed from the local user window.	3
	Changing a profile	The profile was changed successfully.	6

Category	Description	Audit Event	Severity
	Input and output of authentication data	Data output by the `hcmdsauthmove` command succeeded.	6
		Data output by the `hcmdsauthmove` command failed.	3
		Data input by the `hcmdsauthmove` command succeeded.	6
		Data input by the `hcmdsauthmove` command failed.	3
	Placing paths online or offline	All paths were successfully placed online or offline.	6
		Some paths could not be placed online or offline.	4
		No paths could be placed online or offline.	3
	Setting up a multipath LU	The multipath LU was set up successfully.	6
		Part of the multipath LU was not set up successfully.	4
		The multipath LU could not be set up.	3
	Setting up HDLM	HDLM was set up successfully.	6
		HDLM setup partially failed.	4
		HDLM could not be set up.	3
	Setting up alerts	The alerts were set up successfully	6
		Some alerts could not be set up	4
		The alerts could not be set up	3
`StartStop`	Starting and stopping software	The SSO server was started successfully.	6
		The SSO server could not be started.	3
		The SSO server stopped.	6

3.10.2 Editing the Environment Settings File for Audit Logs

To generate HGLAM 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 section 7.4.1.

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 the generated logs.

The location of the `auditlog.conf` file is as follows:

```
HiCommand-Suite-Common-Component-installation-folder\conf\sec
```

The following table lists and describes the items specified in the `auditlog.conf` file.

Table 3.13 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. By default, this item 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 Table 3.12.
`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 HGLAM, see Table 3.12. 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 `6` (Severity) Default: `6`

```
Log.Facility  1
Log.Event.Category  Authentication,ConfigurationAccess
Log.Level 6
```

Figure 3.4 Example of the auditlog.conf File

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.

3.10.3 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 3.14 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	HBase Storage Mgmt Log is always output here.
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 "Description"* below, and Table 3.15

Output format of "Description"

```
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 3.15 Information Output to "Description" 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.
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 HGLAM 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 ID and message text, see the manual *HiCommand® Global Link Availability Manager Messages*.

Example of an Audit Event for Login

```
UserManagement [00000E6C]:
CELFSS,1.1,0,KAPM01124-I,2006-05-15T14:08:23.1+09:00,HBase-SSO,management-host,Authenticati
on,Success,uid=system,,,,,,,,,,,BasicLog,,,"The login process has completed properly."
```

3.11 Setting Up Alert Transfer

Alert information reported by the host by means of SNMP traps can be transferred from the HGLAM server to the SNMP transfer destination server. You can use any application to manage the alert information.

To transfer alerts, you must register either of two MIB files (in some cases, both) on the SNMP transfer destination server in advance.

The MIB file to be registered (hglam.mib) is stored in the following folder:

```
HGLAM-installation-CD-drive:\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 section 3.3.

Chapter 4 Installing HGLAM Clusters

This chapter describes how to set up HGLAM running in a cluster environment.

- HGLAM Cluster System Configuration (section 4.1)
- Type of HGLAM Cluster Installations (section 4.2)

4.1 HGLAM Cluster System Configuration

The management server for HiCommand® 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.

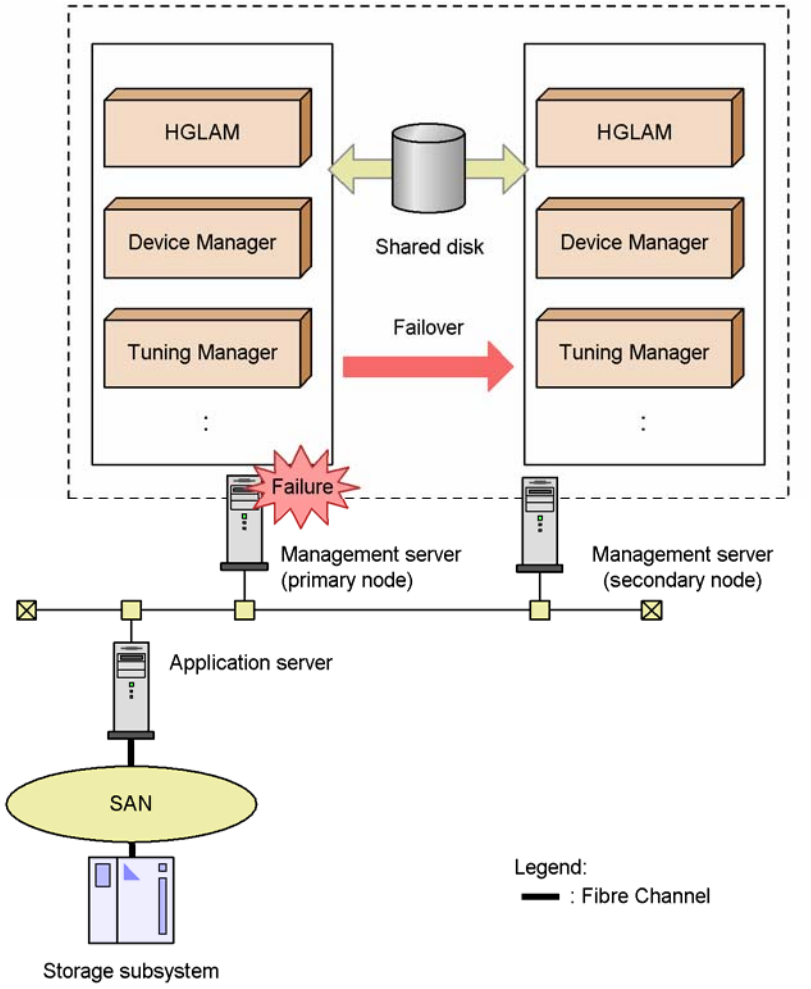

Figure 4.1 Concept of Cluster Configuration

The software programs controlling the entire cluster system are called *cluster software*. Cluster software monitors the system to check whether the system is operating properly, and performs a failover to prevent an interruption to operations if the software detects an abnormal condition.

4.2 Type of HGLAM Cluster Installations

This section describes the types of HGLAM installations in a cluster environment.

There are five types of HGLAM installations in a cluster environment:

- Setting up an HGLAM cluster for a new installation
- Setting up an HGLAM cluster for a reinstallation or version upgrade installation
- Setting up an HGLAM cluster for an existing installation
- Setting up an HGLAM cluster for a new installation in an environment where other HiCommand® products are running in a cluster configuration
- Setting up an HGLAM cluster for uninstallation

  Note:

  – On all nodes that make up a cluster, the disk configuration must be the same, and the installation folder for HGLAM must have the same name (including the drive letter and path name).

  – When you change the HGLAM server settings after the installation in a cluster environment, specify the same settings on all nodes.

4.2.1 Installing HGLAM Clusters for New Installations

Caution: While performing a cluster configuration, do not access HGLAM.

4.2.1.1 Installing HGLAM on the Primary Node

Caution:

- 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 steps 1 to 5 in section 4.2.1.3 to place the resources of the cluster management IP address and shared disk online.
- Make sure that the structure of the HGLAM installation folder is the same for the primary and secondary nodes.

1. On the primary node, perform a new installation of HGLAM.

   For details about the HGLAM new installation procedure, see section 2.1.2. Requirements for installation are as follows:

   – For the folder in which HGLAM is to be installed, specify a folder on the local disk. For the folder for storing the database, specify a folder under the installation folder.

   – For the IP address or host name of the HGLAM server, specify the logical IP address or logical host name of the cluster.

   – For the SNMP trap destination IP address, specify the logical IP address of the cluster.

2. Enter the license key from the HGLAM GUI.

   Use the logical IP address or logical host name of the cluster to access HGLAM. For details on how to specify the license, see section 2.2.

3. Use a text editor to create a cluster-configuration file.

   The items to be specified in the cluster-configuration file are as follows:

   `mode`: Specify `online`.

   `virtualhost`: Specify the logical host name.

   `onlinehost`: Specify the host name of the primary node.

   `standbyhost`: Specify the host name of the secondary node.

   An IP address cannot be specified for `virtualhost`, `onlinehost`, or `standbyhost`. Make sure that the IP address can be resolved from the host name.

   The following shows a coding example in the cluster-configuration file:

```
mode = online
virtualhost = hicommand_cluster
onlinehost = hicommand_1
standbyhost = hicommand_2
```

   Save the created file as `cluster.conf` in *HiCommand-Suite-Common-Component-installation-folder*`\conf`.

4. Stop HiCommand® Suite Common Component.

   Execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
```

5. Start HiRDB.

   Execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbsrv /start
```

6. Back up the database.

   For details about how to back up the database, see section 3.2.1.

7. Migrate the database to the shared disk.

   Execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbclustersetup
/createcluster /databasepath target-folder-for-re-creating-the-database /exportpath
target-folder-for-storing-data
```

   Before executing the command, either delete *target-folder-for-re-creating-the-database* and *target-folder-for-storing-data* or make sure that the two folders are empty.

On the shared disk, deploy the folder in which the database is to be re-created. On the local disk, deploy the folder that stores data.

Specify an absolute path (maximum of 63 bytes) for *target-folder-for-re-creating-the-database* and *target-folder-for-storing-data*.

You can use the following characters for *target-folder-for-re-creating-the-database* and *target-folder-for-storing-data*:

`A` to `Z`, `a` to `z`, `0` - `9`, and `.` and `_`. You can use `\`, `:`, and `/` as the path delimiter.

When this command is executed, the default (23032) is set to the port number that HiRDB uses. If operations are performed by using a port number other than the default port number, you must reset the port number after the command is executed.

8. Stop HiCommand® Suite Common Component.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

9. 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:

   ```
   HGLAM-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
   ```

10. In the Services panel, open the properties for the following services, and if **Startup Type** is **Automatic**, change it to **Manual**:

    - HBase Storage Mgmt Common Service
    - HBase Storage Mgmt Web Service
    - HiRDB/ClusterService _HD0

4.2.1.2 Installing HGLAM on the Secondary Node

1. On the secondary node, perform a new installation of HGLAM.

   For details about the HGLAM new installation procedure, see section 2.1.2. Requirements for installation are as follows:

   - Specify the same installation folder as the one specified on the primary node.
   - Specify the same folders as those specified on the primary node, for the folders for storing the databases of HiCommand® Suite Common Component and the HGLAM server.
   - For the IP address or host name of the HGLAM server, specify the logical IP address or logical host name of the cluster.
   - For the SNMP trap destination IP address, specify the logical IP address of the cluster.

2. Enter the license key from the HGLAM GUI.

   Use the IP address or host name of the secondary node to access HGLAM. For details on how to specify the license, see section 2.2.

3. Use a text editor to create a cluster-configuration file.

   The items to be specified in the cluster-configuration file are as follows:

   `mode`: Specify `standby`.

   `virtualhost`: Specify the logical host name.

   `onlinehost`: Specify the host name of the primary node.

   `standbyhost`: Specify the host name of the secondary node.

   An IP address cannot be specified for `virtualhost`, `onlinehost`, or `standbyhost`. Make sure that the IP address can be resolved from the host name.

   The following shows a coding example in the cluster-configuration file:

   ```
   mode = standby
   virtualhost = hicommand_cluster
   onlinehost = hicommand_1
   standbyhost = hicommand_2
   ```

   Save the created file as `cluster.conf` in *HiCommand-Suite-Common-Component-installation-folder*`\conf`.

4. Stop HiCommand® Suite Common Component.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

5. Change the setting so that the database on the shared disk is to be used.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbremake /cluster
   /databasepath target-folder-for-re-creating-database
   ```

   For *target-folder-for-re-creating-the-database*, specify the same folder as the one specified on the primary node.

When this command is executed, the default (23032) is set to the port that HiRDB uses. If operations are performed by using a port other than the default, you must reset the port after the command is executed.

6. 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:

   HGLAM-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.

7. In the Services panel, open the properties for the following services, and if **Startup Type** is **Automatic**, change it to **Manual**:
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiRDB/ClusterService _HD0

4.2.1.3 Configuring Microsoft Cluster Service for a New Installation

If neither the cluster management IP address nor the shared disk is enabled, perform steps 1 to 5. After installing HGLAM, perform steps 6 to 7.

1. Display Cluster Administrator.

   Select **Start**, **Settings**, **Control Panel**, **Administrative Tools**, and then **Cluster Administrator**.

2. Create a group in which to register the services used by HGLAM.

   Use only resources related to HiCommand® products to configure the group. HGLAM uses the following three services:
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiRDB/ClusterService _HD0

3. Select **IP address** in **Resource type** to register the cluster management IP address to the group.
4. Select **Network name** in **Resource type** to register the logical host name to the group.
5. Select **Physical disk** in **Resource type** to register the shared disk to the group.
6. Register HiRDB, HBase Storage Mgmt Common Service, and HBase Storage Mgmt Web Service as resources.

   Select **New**, and then **Resource**. In each dialog box, specify the settings as shown in Table 4.1 to Table 4.3, and then select **Finish**.

Table 4.1 Settings to Register HiRDB as a Resource

Dialog Box Name	Setting
New Resource	Name: `HiRDB` (optional) Resource type: Generic Service.
Possible Owners	Make sure that the primary and secondary nodes have been added.
Dependencies	Register the drive of the shared disk drive and network name.
Generic Service Parameters	Service Name: `HiRDBClusterService_HD0` Start parameters: None
Registry Replication	Specify nothing.

Table 4.2 Settings to Register the HBase Storage Mgmt Common Service as a Resource

Dialog Box Name	Setting
New Resource	Name: `HBase Storage Mgmt Common Service` (optional) Resource type: Generic Service.
Possible Owners	Make sure that the primary and secondary nodes have been added.
Dependencies	Register the resource in which `HiRDBClusterService_HD0` has been registered.
Generic Service Parameters	Service Name: `HBaseStgMgmtComService` Start parameters: None
Registry Replication	Specify nothing.

Table 4.3 Settings to Register the HBase Storage Mgmt Web Service as a Resource

Dialog Box Name	Setting
New Resource	Name: `HBase Storage Mgmt Web Service` (optional) Resource type: Generic Service.
Possible Owners	Make sure that the primary and secondary nodes have been added.
Dependencies	Register the resource in which `HBaseStgMgmtComService` has been registered.
Generic Service Parameters	Service Name: `HBaseStgMgmtWebService` Start parameters: None
Registry Replication	Specify nothing.

7. In Cluster Administrator, place online the group created in step 2.

4.2.2 Reinstallation or Version Upgrade Installation of HGLAM in a Cluster Environment

This section describes how to perform the following installations when the system has been configured in a cluster environment:

- Re-installing (overwriting) the same version of HGLAM
- Upgrading HGLAM 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.

4.2.2.1 Reinstallation or Version Upgrade Installation of HGLAM on the Primary Node

1. Display Cluster Administrator.

   Select **Start**, **Settings**, **Control Panel**, **Administrative Tools**, and then **Cluster Administrator**.

2. Switch the group (the group to which the services used by HGLAM have been registered) to the executing system.

   HGLAM uses the following three services:

   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiRDB/ClusterService _HD0

   In Cluster Administrator, right-click the group (the group to which the services used by HGLAM have been registered), and then choose **Move Group**.

3. Back up the database.

   For details about how to back up the database, see section 3.2.1.

4. Place the following services offline:

   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service

5. Stop HiCommand® Suite Common Component.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

6. In Cluster Administrator, place the following service offline:

   - HiRDB/ClusterService _HD0

7. In Cluster Administrator, right-click the following services, select **Properties**, select the **Advanced** tab, select **Do not restart**, and then click **OK**.

   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiRDB/ClusterService _HD0

8. Perform a reinstallation or version upgrade installation of HGLAM.

For details about the HGLAM reinstallation procedure, see section 2.1.3. For details about the HGLAM version upgrade installation procedure, see section 2.1.4.

9. Stop HiCommand® Suite Common Component.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

10. When you performed a version upgrade installation and 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:

    HGLAM-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
    ```

11. In the Services panel, open the properties for the following services, and if **Startup Type** is **Automatic**, change it to **Manual:**

    - HBase Storage Mgmt Common Service
    - HBase Storage Mgmt Web Service
    - HiRDB/ClusterService _HD0

12. Switch the group to which the services used by HGLAM have been registered to the standby system.

    HGLAM uses the following three services:

    - HBase Storage Mgmt Common Service
    - HBase Storage Mgmt Web Service
    - HiRDB/ClusterService _HD0

    In Cluster Administrator, right-click the group to which the services used by HGLAM have been registered, and then choose **Move Group**.

4.2.2.2 Reinstallation or Version Upgrade Installation of HGLAM on the Secondary Node

1. Stop HiCommand® Suite Common Component.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

2. Perform a reinstallation or version upgrade installation of HGLAM.

   For details about the HGLAM reinstallation procedure, see section 2.1.3. For details about the HGLAM version upgrade installation procedure, see section 2.1.4.

3. Stop HiCommand® Suite Common Component.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

4. When you performed a version upgrade installation and 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:

   HGLAM-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
   ```

5. In the Services panel, open the properties for the following services, and if **Startup Type** is **Automatic**, change it to **Manual**:

   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service

6. Switch the group to which the services used by HGLAM have been registered to the executing system.

   HGLAM uses the following three services:

   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiRDB/ClusterService _HD0

   In Cluster Administrator, right-click the group to which the services used by HGLAM have been registered, and then choose **Move Group**.

7. In Cluster Administrator, right-click the following services, select **Properties**, select the **Advanced** tab, select **Restart**, and then click **OK**.

   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service

– HiRDB/ClusterService _HD0

8. In Cluster Administrator, place online the group to which the services used by HGLAM have been registered.

4.2.3 Installing an HGLAM Cluster for an Existing Installation

- When you want to change to a cluster configuration after the HGLAM system operations have started in a non-cluster configuration, carry out the following procedure. In this example, the HGLAM whose operations are already running is treated as the primary node.

Caution:

- 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 steps 1 to 5 in section 4.2.1.3 to place the resources of the cluster management IP address and shared disk online.
- Make sure that the structure of the HGLAM installation folder is the same for the primary and secondary nodes.

4.2.3.1 Installing an HGLAM Cluster on the Primary Node

1. Change the HGLAM IP address or host name that was specified during installation to the logical IP address or logical host name for a cluster:

   Check the URL that is currently set. Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdschgurl /print
   ```

   Change the URL. Specify the current URL in *old-URL*, and then execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdschgurl /change old-URL
   new-URL
   ```

   The following shows the URL format:

   ```
   http://ip-address-or-host-name:port-number
   ```

   The following shows an example of executing the command:

   ```
   hcmdschgurl /change http://10.208.116.41:23015 http://10.208.116.45:23015
   ```

   To check the new URL, execute `hcmdschgurl /print`.

2. Use a text editor to edit the SNMP trap destination IP address specified in the property file (`server.properties`).

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

   ```
   HGLAM-installation-folder\conf
   ```

   Change the SNMP Trap destination IP address to the logical IP address of the cluster.

   For `server.snmp.trap_ip_address`, specify the logical IP address of the cluster.

3. Stop HiCommand® Suite Common Component.

   Execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
```

4. Start HiRDB.

   Execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbsrv /start
```

5. Back up the database.

   For details about how to back up the database, see section 3.2.1.

6. Use a text editor to create a cluster-configuration file.

   The items to be specified in the cluster-configuration file are as follows:

   `mode`: Specify `online`.

   `virtualhost`: Specify the logical host name.

   `onlinehost`: Specify the host name of the primary node.

   `standbyhost`: Specify the host name of the secondary node.

   An IP address cannot be specified for `virtualhost`, `onlinehost`, or `standbyhost`. Make sure that the IP address can be resolved from the host name.

   The following shows a coding example in the cluster-configuration file:

```
mode = online
virtualhost = hicommand_cluster
onlinehost = hicommand_1
standbyhost = hicommand_2
```

   Save the created file as `cluster.conf` in *HiCommand-Suite-Common-Component-installation-folder*`\conf`.

7. Migrate the database to the shared disk.

   Execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbclustersetup
/createcluster /databasepath target-folder-for-re-creating-the-database /exportpath
target-folder-for-storing-data
```

   Before executing the command, either delete *target-folder-for-re-creating-the-database* and *target-folder-for-storing-data* or make sure that the two folders are empty.

   On the shared disk, deploy the folder in which the database is to be re-created. On the local disk, deploy the folder that stores data.

   Specify an absolute path (maximum of 63 bytes) for *target-folder-for-re-creating-the-database* and *target-folder-for-storing-data*.

   You can use the following characters for *target-folder-for-re-creating-the-database* and *target-folder-for-storing-data*:

   `A` to `Z`, `a` to `z`, `0` - `9`, and `.` and `_`. You can use `\`, `:`, and `/` as the path delimiter.

   When this command is executed, the default (23032) is set to the port that HiRDB uses. If operations are performed by using a port other than the default, you must reset the port after the command is executed.

8. Stop HiCommand® Suite Common Component.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

9. 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. If you have not used the function, steps 9 to 13 are not necessary. Go to step 14.

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

   Execute the following command:

   ```
   HGLAM-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"
   ```

10. Edit the property file (server.properties).

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

    ```
    HGLAM-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
    ```

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

    Execute the following command:

    ```
    HGLAM-installation-folder\bin\hglamimport /report export-destination-folder-name
    ```

    Before executing the command, you must either delete the folder that you specified in step 10 or make sure that the folder is empty.

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

    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.

12. In the Services panel, open the properties for the following services, and if **Startup Type** is **Automatic**, change it to **Manual**:

    - HBase Storage Mgmt Common Service
    - HBase Storage Mgmt Web Service
    - HiRDB/ClusterService _HD0

4.2.3.2 Installing an HGLAM Cluster on the Secondary Node

1. On the secondary node, perform a new installation of HGLAM.

   For details about the HGLAM new installation procedure, see section 2.1.2. Requirements for installation are as follows:

   - Specify the same installation path as the one specified on the primary node.
   - Specify the same folders as those specified on the primary node, for the folders for storing the databases of HiCommand® Suite Common Component and the HGLAM server.
   - For the IP address or host name of the HGLAM server, specify the logical IP address or logical host name of the cluster.
   - For the SNMP trap destination IP address, specify the logical IP address of the cluster.

2. Enter the license key from the HGLAM GUI.

   Use the IP address or host name of the secondary node to access HGLAM. For details on how to specify the license, see section 2.2.

3. Stop HiCommand® Suite Common Component.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

4. Use a text editor to create a cluster-configuration file.

   The items to be specified in the cluster-configuration file are as follows:

   `mode`: Specify `standby`.

   `virtualhost`: Specify the logical host name.

   `onlinehost`: Specify the host name of the primary node.

   `standbyhost`: Specify the host name of the secondary node.

   An IP address cannot be specified for `virtualhost`, `onlinehost`, or `standbyhost`. Make sure that the IP address can be resolved from the host name.

   The following shows a coding example in the cluster-configuration file:

   ```
   mode = standby
   virtualhost = hicommand_cluster
   onlinehost = hicommand_1
   standbyhost = hicommand_2
   ```

   Save the created file as `cluster.conf` in *HiCommand-Suite-Common-Component-installation-folder*`\conf`.

5. Change the settings so that the database on the shared disk is used.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbremake /cluster
   /databasepath target-folder-for-re-creating-database
   ```

   For *target-folder-for-re-creating-database*, specify the same folder as the one specified on the primary node.

When this command is executed, the default (23032) is set to the port that HiRDB uses. If operations are performed by using a port other than the default, you must reset the port after the command is executed.

6. 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:

   ```
   HGLAM-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.

7. In the Services panel, open the properties for the following services, and if **Startup Type** is **Automatic**, change it to **Manual**:
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiRDB/ClusterService _HD0

8. Configure Microsoft Cluster Service.

   For details about how to configure Microsoft Cluster Service, see section 4.2.1.3.

4.2.4 Installing an HGLAM Cluster with other HiCommand® Clusters Installed

In this procedure, application of the cluster configuration for HiCommand® products is temporarily cancelled. For more information about the settings for a cluster environment for a HiCommand® product, see the corresponding manual for that product.

1. Remove the services for HiCommand® products and cluster groups from the targets of cluster management.
   - In Cluster Administrator, place the target services offline.
   - In Cluster Administrator, right-click the target service, select **Properties**, the **Advanced** tab, **Do not restart**, and then click **OK**. To perform this operation for multiple services, repeat this step as necessary.

2. Stop all HiCommand® products in both the primary and secondary nodes.

   For more information about how to stop a HiCommand® product, see the corresponding manual for that product.

3. Stop HiCommand® Suite Common Component in both the primary and secondary nodes.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

4. Start HiRDB on the primary node.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbsrv /start
   ```

5. Back up the database.

   For details about how to back up the database, see section 3.2.1.

6. On the primary node, back up the database.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbmove /export /datapath
   target-folder-for-outputting-data
   ```

   Before executing the command, delete or empty *target-folder-for-outputting-data*.

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

   You can use the following characters for this folder:

   A to Z, a to z, 0 - 9, ., and _. You can use \, :, and / as the path delimiter.

7. On the primary node, re-create the database system in the local disk.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbremake /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 - 9, ., and _. You can use \, :, and / as the path delimiter.

   When this command is executed, the port designated for HiRDB to use returns to the default (23032). If operations are performed by using a port other than the default, you must reset the port after the command is executed.

8. Register the database that was backed up in step 6 to the re-created database system.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbmove /import /datapath
   target-folder-for-inputting-data
   ```

   For target-folder-for-inputting-data, specify an absolute path for *target-folder-for-outputting-data* specified in step 6

9. Copy *target-folder-for-outputting-data* specified in step 6 to the local disk on the secondary node.

10. In Cluster Administrator, switch each group in which the HiCommand® product service has been registered to the standby system.

11. On the secondary node, re-create the database system on the local disk.

    Execute the following command:

    ```
    HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbremake /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 *target-folder-for-re-creating-the-database*:

`A` to `Z`, `a` to `z`, `0` - `9`, `.`, and `_`. You can use `\`, `:`, and `/` as the path delimiter.

When this command is executed, the port designated for HiRDB to use returns to the default (23032). If operations are performed by using a port other than the default, you must reset the port after the command is executed.

12. Register the database that was copied in step 9.

    Execute the following command:

    ```
    HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbmove /import /datapath
    target-folder-for-inputting-data
    ```

    For *target-folder-for-inputting-data*, specify an absolute path for the folder copied in step 9.

13. Install HGLAM on both the primary and secondary nodes.

    First install HGLAM on the primary node, and then on the secondary node. For details about the HGLAM installation procedure, see sections 4.2.1.1 and 4.2.1.2.

14. Display Cluster Administrator.

    Select **Start**, **Settings**, **Control Panel**, **Administrative Tools**, and then **Cluster Administrator**.

15. Register HiRDB, HBase Storage Mgmt Common Service, and HBase Storage Mgmt Web Service as resources.

    Select **New**, and then **Resource**. In each dialog box, specify the settings as shown in Table 4.4 to Table, and then select **Finish**.

Table 4.4 Settings to Register HiRDB as a Resource

Dialog Box Name	Setting
New Resource	Name: `HiRDB` (optional) Resource type: Generic Service.
Possible Owners	Make sure that the primary and secondary nodes have been added.
Dependencies	Register the drive of the shared disk drive and network name.
Generic Service Parameters	Service Name: `HiRDBClusterService_HD0` Start parameters: None
Registry Replication	Specify nothing.

Table 4.5 Settings to Register the HBase Storage Mgmt Common Service as a Resource

Dialog Box Name	Setting
New Resource	Name: `HBase Storage Mgmt Common Service` (optional) Resource type: Generic Service.
Possible Owners	Make sure that the primary and secondary nodes have been added.
Dependencies	Register the resource in which `HiRDBClusterService_HD0` has been registered.
Generic Service Parameters	Service Name: `HBaseStgMgmtComService` Start parameters: None
Registry Replication	Specify nothing.

Table 4.6 Settings to Register the HBase Storage Mgmt Web Service as a Resource

Dialog Box Name	Setting
New Resource	Name: `HBase Storage Mgmt Web Service` (optional) Resource type: Generic Service.
Possible Owners	Make sure that the primary and secondary nodes have been added.
Dependencies	Register the resource in which `HiRDBClusterService_HD0` has been registered.
Generic Service Parameters	Service Name: `HBaseStgMgmtWebService` Start parameters: None
Registry Replication	Specify nothing.

16. If the installed Device Manager version is earlier than 05-00, change the dependencies for HiCommand® Server.

    Change the resource dependencies from the resource in which `HiCommand®WebService` has been registered to the resource in which `HBaseStgMgmtWebService` has been registered.

17. If the following resources are registered, delete them.
    - A resource in which `HiCommand®Base` has been registered.
    - A resource in which `HiCommand®WebService` has been registered.

18. Return the service that was set to **Do not restart** in step 1 to **Restart**, and then place the service online.

4.2.5 Uninstalling an HGLAM Cluster

To uninstall HGLAM in a cluster environment, perform the following operations on both the primary and secondary nodes.

If the service is not online on the primary node, first place it online, and then perform uninstallation.

To uninstall HGLAM in a cluster environment:

1. Display Cluster Administrator.

   Select **Start**, **Settings**, **Control Panel**, **Administrative Tools**, and then **Cluster Administrator**.

2. Switch the group (the group to which the services used by HGLAM have been registered) to the executing system.

   HGLAM uses the following three services:

   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiRDB/ClusterService _HD0

   In Cluster Administrator, right-click the group (the group to which the services used by HGLAM have been registered), and then choose **Move Group**.

3. Place the following services offline:

   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service

4. On the primary node, stop HiCommand® Suite Common Component.

   Execute the following command:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

5. Place the following service offline:

   - HiRDB/ClusterService _HD0

6. If the following resources are not in use by another application, delete them:

   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiRDB/ClusterService _HD0

7. Among the services listed in step 6, perform the following operation on the services you do not want to delete:

   In Cluster Administrator, right-click the service, select **Properties**, select the **Advanced** tab, select **Do not restart**, and then click **OK**.

8. On the primary node, uninstall HGLAM by selecting **Start**, **Programs**, **Global Link Availability Manager**, and then **Uninstall Global Link Availability Manager**.

9. On the secondary node, stop HiCommand® Suite Common Component.

Execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
```

10. On the secondary node, uninstall the HGLAM by selecting **Start**, **Programs**, **HiCommand®**, **Global Link Availability Manager**, and then **Uninstall Global Link Availability Manager**.
11. If the following resources are not being used by another application, first place the corresponding resource offline, and then delete it:
    - Cluster management IP address
    - Shared disk
12. If the group where the HGLAM resources are registered is no longer necessary, delete that as well.
13. If other HiCommand® products have already been installed and the group was not deleted in step 12, stop the services of other HiCommand® products, and then stop HiCommand® Suite Common Component.

    For details about how to stop other HiCommand® Suite Common Component services, see the manual for each product. To stop HiCommand® Suite Common Component, execute the following command:

    ```
    HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
    ```
14. Return the service that was set to **Do not restart** in step 7 to **Restart**.
15. Place online the service that was set to **Restart** in step 14.

Chapter 5 SSL Setup

This chapter provides an overview of using SSL for communication between a server and clients. This chapter also explains the tasks for SSL setup.

- Introduction to SSL Setup (section 5.1)
- Configuring HBase Storage Mgmt Web Service for SSL Communication (section 5.2)

5.1 Introduction to SSL Setup

When you use the HGLAM GUI to access an HGLAM server remotely via the Internet or 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 HGLAM server, set up SSL for HBase Storage Mgmt Web Service.
2. In the HGLAM GUI, specify a URL that begins with `https://` as the URL used to log in to the HGLAM.

HBase Storage Mgmt Web Service supports SSL versions 3, and TLS version 1.

5.2 Configuring HBase Storage Mgmt Web Service for SSL Communication

HBase Storage Mgmt Web Service uses a public key cryptosystem. Set up SSL on the server.

To set up SSL:

1. Generate a private key.
2. Create a Certificate Signing Request (CSR).
3. Send the CSR to the certificate authority (CA).
4. Obtain a certificate from the CA.
5. Edit the property file.
6. Restart HiCommand® Suite Common Component.

5.2.1 Generating a Private Key

To create a private key, use the `sslc` utility. The private key is used to create a Certificate Signing Request. The location of the `sslc` utility is as follows:

```
HiCommand-Suite-Common-Component-installation-folder\httpsd\sslc\bin
```

The `sslc` utility has the following format:

```
sslc genrsa -out key-file [ 512 | 1024 | 2048 ]
```

- `-out key-file` specifies the file that will contain the private key.
- `[ 512 | 1024 | 2048 ]` specifies the bit length of the private key.

For example, to output a 1024-bit private key to the `httpsdkey.pem` file, execute the command as shown below. This example assumes that you have already moved to the directory storing the sslc utility before executing the command.

```
sslc genrsa -out demoCA\httpsdkey.pem 1024
```

This would generate the following output:

```
Loading 'entropy' into random state - unable to load 'random state'
warning, not much extra random data, consider using the -rand option
Generating 2 prime RSA private key, 1024 bit long modulus
..+++++.............................+++++

e is 65537 (0x10001)
```

5.2.2 Creating a Certificate Signing Request (CSR)

Use the `sslc req` utility to create a Certificate Signing Request (CSR), which you send to a Certificate Authority (CA). When you send the CSR to the CA, the CA will send you a signed certificate. The exact format of the CSR will vary depending on which CA you use.

The `sslc.cnf` file to be specified by the `sslc req` utility is in the following location:

```
HiCommand-Suite-Common-Component-installation-folder\httpsd\sslc\bin\demoCA
```

The `sslc req` utility has the following format:

```
sslc req -config configuration-file -new -key key-file -out CSR-file
```

- `-config` *configuration-file* specifies the `sslc.cnf` file that contains the information you want the utility to access. When you define information in the `sslc.cnf` file in advance, you do not need to enter information such as Country Name and Locality Name on the command line. If you want to use information that is different than that previously defined, you must specify the information when prompted.
- `-new` indicates a new CSR (required)
- `-key` *key-file* indicates the file containing the private key
- `-out` *CSR-file* indicates the file that will contain the Certificate Signing Request (CSR).

For example, to output a CSR when the configuration file is `demoCA\sslc.cnf`, the key file is `demoCA\httpsdkey.pem`, and the name of the CSR file is `demoCA\httpsd.csr`, execute the command as shown below. This example assumes that you have already moved to the directory storing the sslc utility before executing the command.

```
sslc req -config demoCA\sslc.cnf -new -key demoCA\httpsdkey.pem -out demoCA\httpsd.csr
```

The utility will prompt you to enter certain information, including the country name and locality. If you want to leave a field blank, enter a period (.). If you want to select the default, select **Enter**.

Note: For `Common Name`, specify the host name that is actually set in the Web browser. For a cluster environment, specify the same logical host name that is specified for `virtualhost` in the `cluster.conf` file. The prompts generally appear as follows:

```
Using configuration from demoCA/sslc.cnf
You will be prompted to enter information to incorporate
into the certificate request.
This information is called a Distinguished Name or a DN.
There are many fields however some can remain blank.
Some fields have default values.
Enter '.', to leave the field blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:Washington
Locality Name (eg, city) []:New York
Organization Name (eg, company) []:HITACHI
Organizational Unit Name (eg, section) []:WebSite
Common Name (eg, YOUR name) []:www.example.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

5.2.3 Editing the Property File

To enable or disable SSL, or to change the port for SSL, you must edit the property file (`httpsd.conf`). The location of this file is as follows:

```
HiCommand-Suite-Common-Component-installation-folder\httpsd\conf
```

For a non-cluster environment, make sure that the host name specified for `ServerName` at the beginning of the `httpsd.conf` file is entered for `VirtualHost` and `ServerName` in the `httpsd.conf` file. 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 following table shows the editing format of the `httpsd.conf` file.

```
Listen 23016
#<VirtualHost host-name:port-number>
#  ServerName host-name
#  SSLEnable
#  SSLRequireSSL
#  SSLCertificateFile signed-certificate-file
#  SSLCertificateKeyFile private-key-file-for-the-Web-server
#  SSLCACertificateFile certificate-file-of-chained-authorized-body
#  SSLSessionCacheTimeout 3600
#</VirtualHost>
```

Figure 5.1 Editing Format for the httpsd.conf File

5.2.3.1 Enabling SSL

To enable SSL:

1. If services of other HiCommand® products are running, stop them.

   For details about how to check statuses and stop services of other products, see the documentation for those products.

2. Execute the following command to stop HiCommand® Suite Common Component:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

3. Copy the private key file and the signed certificate file returned by the CA to the appropriate directory.

   We recommend that you copy them to the following directory:

   `C:\Program Files\HiCommand\Base\httpsd\conf\ssl\server`

4. Open the `httpsd.conf` file.
5. Make the directives for the SSL port and host name effective, by deleting the hash mark (#) at the beginning of the corresponding lines.
6. In `SSLCertificateFile`, specify the absolute path name of the certificate file returned by the CA.
7. In `SSLCertificateKeyFile`, specify the absolute path name of the private key file for the Web server.
8. To use a certificate issued by a chained CA, in `SSLCACertificateFile`, specify the absolute path name of the certificate file of the chained CA.
9. Execute the following command to start HiCommand® Suite Common Component:

   HiCommand-Suite-Common-Component-installation-folder`\bin\hcmdssrv /start`

The following table shows an example of enabling SSL, where the signed certificate (`httpsd.pem`) received from a CA and the private key (`httpsdkey.pem`) are placed in the `C:\Program Files\HiCommand\Base\httpsd\conf\ssl\server` folder.

Note: A line that begins with a hash mark (#) is a comment line.

```
:
Listen 23015
SSLDisable

SSLSessionCacheSize 0
Listen 23016
<VirtualHost www.example.com:23016>
  ServerName www.example.com
  SSLEnable
  SSLProtocol SSLv3 TLSv1
  SSLRequireSSL
  SSLCertificateFile C:/Program Files/HiCommand/Base/httpsd/conf/ssl/server/httpsd.pem
  SSLCertificateKeyFile C:/Program Files/HiCommand/Base/httpsd/conf/ssl/server/httpsdkey.pem
#  SSLCACertificateFile C:/Program Files/HiCommand/Base/httpsd/conf/ssl/cacert/anycert.pem
  SSLSessionCacheTimeout 3600
</VirtualHost>
:
```

Figure 5.2 Enabling SSL

5.2.3.2 Disabling SSL

To disable SSL, comment out the directives for the SSL port and host in the `httpsd.conf` file. Before editing the `httpsd.conf` file, stop other HiCommand® product services and HiCommand® Suite Common Component. After the editing is complete, restart HiCommand® 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.

```
:
Listen 23015
SSLDisable

SSLSessionCacheSize 0
#Listen 23016
#<VirtualHost www.example.com:23016>
#  ServerName www.example.com
#  SSLEnable
#  SSLProtocol SSLv3 TLSv1
#  SSLRequireSSL
#  SSLCertificateFile C:/Program Files/HiCommand/Base/httpsd/conf/ssl/server/httpsd.pem
# SSLCertificateKeyFile C:/Program Files/HiCommand/Base/httpsd/conf/ssl/server/httpsdkey.pem
#  SSLCACertificateFile C:/Program Files/HiCommand/Base/httpsd/conf/ssl/cacert/anycert.pem
#  SSLSessionCacheTimeout 3600
#</VirtualHost>
:
```

Figure 5.3 Disabling SSL

5.2.3.3 Changing a Port Number Assigned to SSL

The default port of SSL for HBase Storage Mgmt Web Service is 23016. To change the port, change the `Listen` directive and the port number of the host in the `httpsd.conf` file. Before editing the `httpsd.conf` file, stop other HiCommand® product services and HiCommand® Suite Common Component. After the editing is complete, restart HiCommand® Suite Common Component.

Chapter 6 Using HGLAM with Other HiCommand® Products

This chapter describes the HGLAM settings for linking with other HiCommand® products. These settings are required to use single sign-on functionality and to implement integrated user management.

- Overview of HiCommand® Suite Single Sign-On and User Integration Management (section 6.1)
- Settings for Starting HSSM from the Dashboard Menu (section 6.2)

6.1 Overview of HiCommand® Suite Single Sign-On and User Integration Management

Single sign-on functionality and integrated user management are available when linkage with other HiCommand® 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 HiCommand® products from the **Dashboard** menu in the HGLAM GUI. For details about the **Dashboard** menu, see Help.

When the HiCommand® 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 HGLAM links with another HiCommand® product.

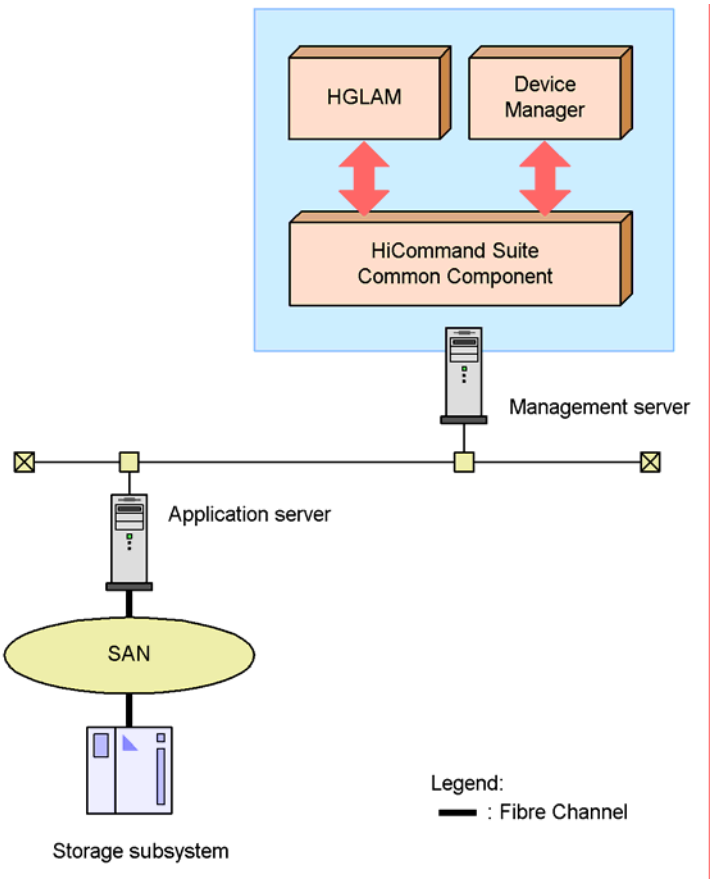

Figure 6.1 Sample Configuration Where HGLAM Links with Another HiCommand® Product

When you install HGLAM 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 HGLAM, 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 HiCommand® products of version 5.0 or later (excluding Tuning Manager 5.0) that are installed on the same server. They are not available for HiCommand® products whose version is earlier than version 5.0, or for HiCommand® products that are installed on other servers.

6.2 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:

HiCommand-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*

Chapter 7 Troubleshooting HGLAM

This chapter explains how to troubleshoot problems that might occur during HGLAM operation.

- Procedure for Troubleshooting HGLAM (section 7.1)
- HGLAM Troubleshooting Examples (section 7.2)
- Procedure for Collecting HGLAM Diagnostic Information (section 7.3)
- Managing HGLAM Log Files (section 7.4)

7.1 Procedure for Troubleshooting HGLAM

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 section 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 section 7.3.

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 section 7.4.

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.

7.2 HGLAM Troubleshooting Examples

This section provides examples of problems that might occur during HGLAM installation, environmental settings, and during GUI operation. This section also describes the causes of such problems and the corrective actions you should take for them.

7.2.1 Installing HGLAM

Table 7.1 Troubleshooting Examples (During HGLAM Installation)

Problem	Cause	Action
Installation fails.	A user without administrator privileges attempted to perform installation.	Log on as a user with administrator privileges, and perform 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.

7.2.2 Setting Up HGLAM

Table 7.2 Troubleshooting Examples (During HGLAM Environment Setup)

Problem	Cause	Action
The specified settings were not applied to the property file.	HGLAM was not restarted after the property file was updated.	Restart HGLAM.
	Default values were used because incorrect values were set in the property file.	Refer to 3.3 and make sure the values set in the property file are correct.

7.2.3 Using the HGLAM GUI

Table 7.3 Troubleshooting Examples (During HGLAM GUI Operation)

Problem	Cause	Action
The HGLAM pages cannot be displayed with a Web browser.	HiCommand® Suite Common Component is not running.	Start HiCommand® Suite Common Component. For details on how to do this, see section 3.1.1.
	An attempt to start HiCommand® Suite Common Component has failed because there is insufficient disk space on the HGLAM server.	Ensure that there is enough disk space on the HGLAM server, and then start HiCommand® Suite Common Component. For details on how to start HiCommand® Suite Common Component, see section 3.1.1.
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 about changing the configuration of the HDLM operating environment, see the manual *HiCommand® Dynamic Link Manager User's Guide*.
	The settings for the Device Manger agent installed on the host are incorrect.	Execute the `hdvmagt_account` command of the Device Manager agent to set up the Device Manager server information or host information. For details on how to do this, see Help.
	HiCommand® Suite Common Agent Component is not running.	Start HiCommand® Suite Common Agent Component. For details on how to do this, see section A.3.1.
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 manual *HiCommand® Dynamic Link Manager User's Guide*.
	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 manual *HiCommand® Dynamic Link Manager User's Guide*.
	The HDLM version installed on the host is not supported by HGLAM.	Install a version of HDLM that is supported by HGLAM. For details on the HDLM versions supported by HGLAM, see section 1.3.3.

Problem	Cause	Action
	Any of the following errors might have occurred during communication between the HGLAM server and HDLM. ▪ The network cable is damaged or not connected properly. ▪ The router or hub is broken. ▪ The network interface card is broken. ▪ 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.	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. ▪ Review the routing settings. ▪ Reconfigure packet filtering so that packets for HDLM and HGLAM 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 the Device Manager agent on the host, the port number for the port specified in one of the following properties has been changed: ▪ `server.agent.port` property (agent service port) ▪ `server.http.port` property (remote port)	Temporarily delete the host, and then add it again. For details on how to add and delete hosts, see Help.
	In the `server.properties` file of HiCommand® 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 Help.
	The settings for the Device Manager agent are incorrect because the version of HDLM on the host has been updated to a version earlier than 5.8.	Restart the Device Manager agent service (or daemon process). For details on how to do this, see the manual *HiCommand® Device Manager Agent Installation Guide*.
	The settings for the Device Manger agent installed on the host are incorrect.	Execute the `hdvmagt_account` command of the Device Manager agent to set up the Device Manager server information or host information. For details on how to do this, see Help.
	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 about changing the configuration of the HDLM operating environment, see the manual *HiCommand® Dynamic Link Manager User's Guide*.

Problem	Cause	Action
	HiCommand® Suite Common Agent Component is not running.	Start HiCommand® Suite Common Agent Component. For details on how to do this, see section A.3.1.
In message KAIF22102-E, `The header information is invalid.` is displayed as the detailed information.	The Device Manager agent is currently stopping its service (or daemon process), or is executing other application processing.	Check the status of the Device Manager agent service (or daemon process). If it is stopped, start it. If it is running, wait a while, and then retry the operation. For details on how to start the service (or daemon process), see the manual *HiCommand® Device Manager Agent Installation Guide*.
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 subsystem.	Change the access permissions for the logged-in user.

7.3 Collecting HGLAM 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 section 7.2, you must collect diagnostic information about the HGLAM 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.

7.3.1 Diagnostic Batch Collection about the HGLAM Server

To collect diagnostic information about HGLAM, use the `hcmdsgetlogs` command.

Note that you can use the `hcmdsgetlogs` command only when an error has occurred.

7.3.1.1 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 hcmdsgetlogs Command

No.	File Type	Archive File Name (Default)
1	Event log	`HiCommand_log.jar`
2	Message log	
3	Installer trace log	
4	Uninstaller trace log	
5	Integrated trace log	
6	Trace log	
7	Property file	
8	InstallShield log	
9	Version file	
10	Database error analysis log	
11	Path availability information (path status log)	
12	Database detailed log	`HiCommand_log.hdb.jar`
13	Database file	`HiCommand_log.db.jar`
14	Database table data	`HiCommand_log.csv.jar`

If you cannot determine the cause of the error after referring to log files No.1 to 4 in the above list, send the archive file that contains files No.1 to No.11 to the Support Center for analysis. At this time, ask the Support Center whether you need to send the archive files for files No.12 to 14 as well. Note that HiCommand® Suite Common Component must be running to obtain the archive file for file No.13.

For details on how to check log files No.1 to 4, see section 7.4.

7.3.1.2 When Acquiring the Path Availability Information (Path Status Log)

When an error occurs during a host discovery, host refresh, or report acquisition, and you need diagnostic information, acquire the path availability information (path status log) listed in No.11 of Table 7.4. 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 HGLAM.

- `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 section 3.3.

7.3.1.3 Format of the hcmdsgetlogs Command

Command format

`hcmdsgetlogs /dir` ***folder-name*** `[/type HGLAM /arc` ***archive-file-name***`]`

Options

Table 7.5 Options and Arguments of the hcmdsgetlogs Command

Options and arguments	Description
`/dir` *folder-name*	Specifies the name of the folder for storing collected diagnostic information.

`/type HGLAM`
or
`GlobalLinkAvailabilityManager`
	Specifies that only HGLAM diagnostic information be collected. If this option is not specified, the command also collects diagnostic information about the other HiCommand® 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 command creates the archive files with the default names shown in Table 7.4.

7.3.2 Diagnostic Batch Collection about the Host

If the output error is caused by a host, you need to collect and check diagnostic information about the host. The collection procedure for the host diagnostic information differs depending on the version of HDLM installed on the host.

- When the version of HDLM is 5.8 or later:

  Use the `DLMgetras` utility to collect diagnostic information. For details on the `DLMgetras` utility, see the manual *HiCommand® Dynamic Link Manager User's Guide*.

- When the version of HDLM is earlier than 5.8:

  Use the `DLMgetras` utility or the TIC command of the Device Manager agent to collect diagnostic information. For details on the `DLMgetras` utility, see the manual *HiCommand® Dynamic Link Manager User's Guide*. For details on the TIC command, see the manual *HiCommand® Device Manager Agent Installation Guide*.

7.3.3 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 HGLAM, but the User Login window did not appear.
- A logon to HGLAM was successful, but the main window did not appear.
- An attempt was made to start HGLAM from another HiCommand® 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:
   HiCommand-Suite-Common-Component-installation-folder`\CC\web\containers\HiCommand`
2. In Control Panel in Windows, double-click **Administrative Tools**, and then **Services**. From the displayed Services window, stop **HBase Storage Mgmt Common Service**.

   The `javacore`*xxx*`.`*xxxx*`.txt` file is created in the following folder:
   HiCommand-Suite-Common-Component-installation-folder`\CC\web\containers\HiCommand`
3. From the Services window, start **HBase Storage Mgmt Common Service**.

7.4 Managing HGLAM Log Files

After you collect diagnostic information as described in section 7.3.1, 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 (`AppEvent.EVT`)	Stores important messages that are output to the message log. When other HiCommand® 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 HGLAM as audit logs. This log file should be checked to audit accesses to HGLAM and operations performed by the user.
Message log (`HGLAM_Message`*n*`.log`)	Stores the messages output while HGLAM is starting, stopping, and being operated. This log file should be checked if an error occurs while HGLAM is starting, stopping, or being operated.
Installer trace log or uninstaller trace log (`HGLAM_TL_Install_`*yyyy-mm-dd_hh-mm-ss*`.log` or `HGLAM_TL_Uninstall_`*yyyy-mm-dd_hh-mm-ss*`.log`)	Stores the messages output during HGLAM installation or uninstallation. This log file should be checked if an error occurs during installation or uninstallation.

7.4.1 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	`HBase Storage Mgmt Log` 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 *HiCommand® Global Link Availability Manager Messages*. A message beginning with *program-name* [*process-ID*]: `CELFSS` is an audit log message. For details on the audit logs, see section 3.10.

7.4.2 Output Format of the Message Log Files

This section shows the format of entries output to the HGLAM message log, 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 HGLAM Message Log

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 HGLAM 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 *HiCommand® Global Link Availability Manager Messages*.

7.4.3 Output Format of the Installer and Uninstaller Log Files

Output format:

```
*** begin HiCommand® Global Link Availability Manager (Windows) setup process Trace Log
date-and-time : (level) trace-information [ supplementary-information ]
*** end HiCommand® Global Link Availability Manager (Windows) setup process Trace Log
```

Table 7.9 Information Output to the Installer Trace Log and the Uninstaller Trace Log

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.

Appendix A Notes on Using HDLM Version 5.8 or Later

This appendix describes the notes on operating HGLAM and the items that have to be configured in advance when the version of HDLM installed on the host is 5.8 or later, and it explains how to start HiCommand® Suite Common Agent Component.

HiCommand® Suite Common Agent Component is included in HDLM version 5.8 or later.

The notes on using HDLM version 5.8 or later are as follows:

When the host OS is Windows:

The installation folder for HiCommand® 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 HiCommand® Suite Common Agent Component. Check the latest version key name.
- Name: Path00

When the host OS is Windows Server 2003 (IPF) or Windows Server 2003 (x64):

When other HiCommand® products installed on the host frequently access the HiCommand® Suite Common Agent Component, JavaVM might finish abnormally. In this case, edit the following file:

installation-folder-for-HiCommand-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%
```

A.1 Changing Firewall Settings for HDLM for Windows

When the OS of the host where HDLM version 5.8 or later is installed is Windows Server 2003 SP1 and Windows Firewall is active, you need to add HiCommand® Suite Common Agent Component to the Windows Firewall exceptions list to run HGLAM.

Registering an exception

To register HiCommand® Suite Common Agent Component as an exception:

1. Execute the following commands to register the exception:

```
netsh firewall add allowedprogram
program="installation-folder-for-HiCommand-Suite-Common-Agent-Component\agent\bin\hbsa_
service.exe" name="HBase Agent" mode=ENABLE

netsh firewall add allowedprogram
program="installation-folder-for-HiCommand-Suite-Common-Agent-Component\agent\JRE1.4\bi
n\java.exe" name="HBase Agent" mode=ENABLE
```

2. Execute the following command to check the registered contents:

```
netsh firewall show all
```

   Make sure of the following from the command execution results:

   - That `HBase Agent` is displayed.
   - That `Mode` is `Enable`.
   - That the paths to `hbsa_service.exe` and `java.exe` are correct.

Deactivating the setting for an exception

If you uninstalled HDLM from the host, deactivate the above setting. Execute the following commands to deactivate the setting.

```
netsh firewall delete allowedprogram
"installation-folder-for-HiCommand-Suite-Common-Agent-Component\agent\bin\hbsa_service.exe"

netsh firewall delete allowedprogram
"installation-folder-for-HiCommand-Suite-Common-Agent-Component\agent\JRE1.4\bin\java.exe"
```

A.2 Changing the Settings of HiCommand® Suite Common Agent Component

In HiCommand® Suite Common Agent Component, by default, 24041 to 24043 are set for the port numbers that are used to communicate with HGLAM. If other products are using these port numbers, change the port numbers of HiCommand® 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 HGLAM.

To change the settings, edit the property files of each host.

***Note**:* If HDLM version 5.8 or later and a Device Manager agent 5.0 or later are installed on the same host, the two products share the property file and use common properties. Therefore, the specified value used by HiCommand® Suite Common Agent Component of HDLM and a Device Manager agent is the same.

Location of property files:

In Windows:

```
installation-folder-for-HiCommand-Suite-Common-Agent-Component\agent\config\
server.properties
```

In Solaris,HP-UX, or Linux:

```
/opt/HDVM/HBaseAgent/agent/config/server.properties
```

In AIX:

```
/usr/HDVM/HBaseAgent/agent/config/server.properties
```

Contents of property files:

The following tables list the properties that are used for changing the settings of HiCommand® Suite Common Agent Component.

Table A.1 Properties for Changing the Settings of HiCommand® 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 HiCommand® Suite Common Agent Component's service (or daemon process). When you add a host as an HGLAM management-target in the HGLAM GUI, specify the **Agent Service Port** to this port number. Default: 24041
2	server.http.port#	Specifies the port number that HiCommand® Suite Common Agent Component's WebServer uses. Default: 24042
3	server.http.localPort#	Specifies the port number for communication between HiCommand® Suite Common Agent Component's service (or daemon process) and the WebServer process. Default: 24043
Settings for the host name, IP address, and network interface cards that are used by the Web server function		
4	server.http.host	Specifies the host name. If you do not specify a host name or specify the default, HiCommand® Suite Common Agent Component automatically acquires the host name. If the host name cannot be acquired, you must set it manually so that HGLAM can access HiCommand® Suite Common Agent Component. Default: localhost
5	server.http.socket.agentAddress	Specifies the IP address of the host. If you do not specify an IP address, HiCommand® Suite Common Agent Component automatically acquires the IP address. If the IP address cannot be acquired, you must set it manually so that HGLAM can access HiCommand® Suite Common Agent Component. Default: Not specified
6	server.http.socket.bindAddress	When multiple network interface cards are installed on a host on which HDLM version 5.8 or later is installed, connect to the same network by specifying the IP address used to communicate with HGLAM. 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. To avoid registering a single host redundantly, specify the IP address used by HGLAM in dotted-decimal IP address form. Default: Not specified
Settings for the basic operations of the Web server function		
7	server.agent.maxMemorySize	Specifies the maximum memory heap size for the process for the Web server function of the HiCommand® Suite Common Agent Component, in MB. If processing stops because the memory heap size is too small, you can correct the problem by increasing this value. Range is 32 to 4096. Default: Not specified (the process runs with a maximum memory heap size of 64 MB)

No.	Property Name	Description
8	server.agent.shutDownTime	Specifies the period (in milliseconds) to shutdown the HiCommand® Suite Common Agent Component's WebServer 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 HiCommand® Suite Common Agent Component to HGLAM, but also increases the resources used by HiCommand® Suite Common Agent Component. Default: 600000[msec]
Security settings for the Web server function		
9	server.http.security.clientIP	Specifies the IP address for which access is permitted. Specify the IP address of the HGLAM server, or do not specify the IP address so that the HiCommand® Suite Common Agent Component can accept connections from all IP addresses. Note that when the HGLAM 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 Manager agent, in addition to the IP address of the HGLAM server. This setting limits the IP addresses permitted for connection, thus preventing denial-of-service attacks or other attacks that intend to overflow buffers. In the following example, the specification to permits 191.0.0.2 and 192.168.0.0 to 192.168.255.255 to connect to the HiCommand® Suite Common Agent Component: server.http.security.clientIP=191.0.0.2, 192.168.*.*. You can use an asterisk (*) as a wildcard character to specify multiple connections from a single IP address. To specify multiple IP addresses, separate them by commas (,). Invalid specifications for dotted decimal IP addresses and spaces are ignored, and do not cause an error. Default: Not specified (the HiCommand® Suite Common Agent Component accepts access from *.*.*.* (any server can access the HiCommand® Suite Common Agent Component))
10	server.http.entity.maxLength	Specifies the maximum length (in bytes) of an XML file that the HGLAM server sends to HiCommand® 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

#: 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 HiCommand® Suite Common Agent Component Log File (logger.properties)

No	Property Name	Description
1	`logger.loglevel`	Specifies the log level for data that the HiCommand® Suite Common Agent Component outputs to the files `error.log` and `trace.log`. Log levels: DEBUG, INFO, WARN, ERROR and FATAL. Default: `INFO`
2	`logger.MaxBackupIndex`	Specifies the maximum number of log file backups. If more log files are generated than specified, the HiCommand® 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 HiCommand® 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: from `512KB` to `32MB` 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 HiCommand® Suite Common Agent Component.

   Caution: Do not change the specified value for any properties other than the properties shown in Table A.1 and Table A.2.

2. Restart HiCommand® Suite Common Agent Component.

   Stop HiCommand® Suite Common Agent Component, and then start the component again. For details on how to start and stop HiCommand® Suite Common Agent Component, see section A.3.

A.3 Starting and Stopping HiCommand® Suite Common Agent Component

When you add a host, on which HDLM version 5.8 or later is installed, as a resource of HGLAM, and place the host under HGLAM management, HiCommand ®Suite Common Agent Component must be running together with the HDLM manager.

This section describes how to start and stop HiCommand® Suite Common Agent Component, and check the operating status.

Although HiCommand® Suite Common Agent Component starts automatically during HDLM installation, in the following cases, you have to manually restart (start and stop) the component:

- When you changed the IP address of the host where HDLM was installed
- When you modified the property file of HiCommand® Suite Common Agent Component

Note: The HiCommand® Suite Common Agent Component runs on WOW64 when the host is Windows Server 2003 (IPF) or Windows Server 2003 (x64). Execute the commands provided by the HiCommand® 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
```

A.3.1 Starting HiCommand® Suite Common Agent Component

To start HiCommand® 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-HiCommand-Suite-Common-Agent-Component\bin\hbsasrv.exe start
```

In Solaris, HP-UX, or Linux:

```
/opt/HDVM/HBaseAgent/bin/hbsasrv start
```

In AIX:

```
/usr/HDVM/HBaseAgent/bin/hbsasrv start
```

A.3.2 Stopping HiCommand® Suite Common Agent Component

To stop HiCommand® 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-HiCommand-Suite-Common-Agent-Component\bin\hbsasrv.exe stop
```

In Solaris, HP-UX, or Linux:

```
/opt/HDVM/HBaseAgent/bin/hbsasrv stop
```

In AIX:

```
/usr/HDVM/HBaseAgent/bin/hbsasrv stop
```

A.3.3 Checking HiCommand® Suite Common Agent Component Operating Status

To check the HiCommand® 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-HiCommand-Suite-Common-Agent-Component\bin\hbsasrv.exe status
```

In Solaris, HP-UX, 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 HiCommand® Suite Common Agent Component service (or daemon process) is operating. If the result displays `Status` as `Stop`, the service (or daemon process) has stopped.

A.3.4 hbsasrv Command Syntax

This section describes the syntax of the `hbsasrv` command used when starting and stopping HiCommand® Suite Common Agent Component, and checking the component's operating status.

The following table shows the `hbsasrv` command syntax.

Table A.3 hbsasrv Command Syntax

Item	Description
Synopsis	`hbsasrv [start | stop [-f] | status]`
Description	Starts or stops the service (or daemon process) of the HiCommand® 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 HiCommand® products are installed on the host, you may not be able to stop HiCommand® 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 HiCommand® Suite Common Agent Component, you can force the HiCommand® 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.

A.4 HiCommand® Suite Common Agent Component Messages

A message output by the HiCommand® Suite Common Agent Component consists of a message ID and message text (error message text). The format is as follows:

KAIE*nnnnn*-Z *message-text*

The message ID consists of the following elements:

KAIE

Indicates the message is generated by the HiCommand® Suite Common Agent Component.

nnnnn

Indicates the error code.

Z

Indicates the error level, which means the severity of the error. The following table explains the meaning of each error level.

Table A.4 Error Levels and Meanings

Error Level	Description
I (Information)	A message reporting that processing finished normally.
W (Warning)	A message reporting that processing will continue under restriction.
E (Error)	A message reporting that a fatal error has occurred, which means that the processing cannot continue.

The following table shows the messages of HiCommand® Suite Common Agent Component.

Table A.5 HiCommand® Suite Common Agent Component Messages

Message ID	Description	Solution
KAIE10401-E	A serious error was detected during one of the following processes: ▪ Installation or uninstallation ▪ Addon-module loading ▪ Request reception There might be a resource shortage or an internal error.	Make sure that there are no resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE10403-E	An error occurred when loading a module. There might be a resource shortage or an internal error.	Make sure that there are no resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.

Message ID	Description	Solution
KAIE10404-E	An I/O error occurred. An attempt to access the following files has failed:· ▪ *HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/mod/* ▪ *HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/mod/*/var The service might not have permission to access these files or directories.	Make sure that the user who is executing the service has permission to access these files or directories. If the user does not have permission, grant permission, or change to a user who has permission.
KAIE10502-E	The environment is invalid. An attempt to read the product information file (*HiCommand-Suite-Common-Agent-Component-installation-directory*/etc/amc_iid) has failed. The installation might not have finished correctly.	Re-install HDLM. If this does not resolve the problem collect maintenance information and contact the support center.
KAIE10602-E	The environment is invalid.	For appropriate action, see the past operating log message containing details about the problem.
KAIE10606-E	An I/O error occurred. An attempt to generate the product information file (*HiCommand-Suite-Common-Agent-Component-installation-directory*/etc/amc_iid) has failed. The installation might not have finished correctly.	Re-install HDLM. If this does not resolve the problem collect maintenance information and contact the support center.
KAIE16002-I	The detail of the error information is output.	For appropriate action, see the content of exception information.
KAIE20001-E	A serious error was detected during one of the following processes: ▪ Installation or uninstallation ▪ Addon-module loading ▪ Request reception There might be a resource shortage or an internal error.	Make sure that there are no resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE20002-E	A serious error was detected during service execution. There might be a resource shortage or an internal error.	Make sure that there are no resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE20101-E	An unexpected error occurred during processing of the request. There might be a resource shortage or an internal error.	Make sure that there are no resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE20102-E	A serious error was detected during service execution. There might be a resource shortage or an internal error.	Make sure that there are no resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE20303-E	A serious error was detected during service execution. There might be a network error or a resource shortage.	Make sure that there are no network errors or resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.

Message ID	Description	Solution
KAIE20402-E	An unexpected error occurred during HTTP connection processing. There might be a network error or a resource shortage.	Make sure that there are no network errors or resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE20403-E	An I/O error occurred while communicating with the remote host. The remote host might have severed the connection, or there might be a network error or resource shortage.	If it was not a normal disconnection by the remote host, make sure that there are no network errors or resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE20601-E	An unexpected error occurred during processing of the service request. There might be a resource shortage or an internal error.	Make sure that there are no resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE20701-E	An error occurred while creating the log output destination directory. The service might not have write permissions for the following directory: ▪ *HiCommand-Suite-Common-Agent-Component-installation-directory*/agent	Make sure that the user who is executing the service has permission to access these files or directories. If the user does not have permission, grant permission, or change to a user who has permission.
KAIE20702-E	An error occurred while creating the log output destination directory. A file which has the same name (*HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/logs) already exists.	Delete the file which has the same name as the directory.
KAIE20703-E	The log output destination directory (*HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/logs) is read-only.	Make the log output destination directory writable.
KAIE20704-E	An attempt to access the log property file (*HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/config/logger.properties) has failed. Possible causes are: ▪ The file does not exist. ▪ The user has the file open. ▪ The user lacks access permissions. ▪ The settings are invalid.	▪ Make sure that the logger.properties file exists. ▪ If the logger.properties file is open, close it. ▪ Grant access permissions for the logger.properties file, or change to a user who has access permissions and restart the service. ▪ Check the settings of the logger.properties file. If they are invalid, correct them.

Message ID	Description	Solution
KAIE20705-E	The log output file cannot be created. A directory which has the same name as a log output file (below) exists in the log output destination directory. ▪ *HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/logs/trace.log ▪ *HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/logs/access.log ▪ *HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/logs/error.log ▪ *HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/logs/service.log	Delete the directory which has the same name as the log output file.
KAIE20706-E	One of the following log output files is not writable because the user who is executing the service does not have write permissions for that file: ▪ *HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/logs/trace.log ▪ *HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/logs/access.log ▪ *HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/logs/error.log ▪ *HiCommand-Suite-Common-Agent-Component-installation-directory*/agent/logs/service.log	Grant write permissions for the log output file, or change to a user who has write permissions and restart the service.
KAIE20707-E	There is an error in the settings of the property file (server.properties).	Check each value of the server.properties property and correct them if necessary.

KAIE20901-E	An unrecoverable error occurred in the service execution process. There might be a resource shortage or an internal error.	▪ If the following properties are specified in the properties file, revise the specification:
		`server.http.socket.agentAddress`
		`server.http.socket.bindAddress`
		▪ Make sure that there are no resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.

KAIE20902-E	A network error occurred while waiting for a connection. There might be a network error or a resource shortage.	Make sure that there are no network errors or resource shortages. If the problem occurs frequently, collect maintenance information and contact the support center.
KAIE20903-E	An unexpected error occurred in the service execution process. There might be a resource shortage or an internal error.	Make sure that there are no network errors or resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.

Message ID	Description	Solution
KAIE20904-E	An error occurred during shutdown of the service execution process.	Make sure that there are no network errors or resource shortages. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE21703-W	There is an error in the settings of the property file (server.properties).	Check each value of the server.properties property and correct them if necessary.
KAIE30101-E	A serious error was detected during service execution. There might be a resource shortage or an internal error.	Make sure that there are no resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE30201-E	A serious error was detected during service execution. There might be a resource shortage or an internal error.	Make sure that there are no resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE30504-E	An unexpected error occurred during execution of the service control process stop command. There might be a resource shortage or an internal error.	Make sure that there are no resource shortages, and then retry a forced termination of the service. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE30505-E	The service execution process could not start because the environment is invalid.	For details on the appropriate action, see the preceding message that gives details about the problem.
KAIE30506-E	The service execution process detected an unexpected error. There might be a resource shortage or an internal error.	Make sure that there are no resource shortages, and then restart the service. If this does not resolve the problem, collect maintenance information and contact the support center.
KAIE30507-E	A communication error occurred during the execution of "hbsasrv stop". Possible causes are: ▪ The service control process cannot receive commands because of a problem such as a system resource shortage. ▪ The service control process is not working correctly.	Re-execute "hbsasrv stop". If the above actions do not resolve the problem, collect maintenance information and contact the support center.
KAIE62001-I	HBsA Service is already running.	Only one instance of HBsA Service can run on a system at any given time.
KAIE62601-E	Permission of HBsA Service was denied.	A user without Administrator permissions executed the command. Execute this command as a user with Administrator permissions.
KAIE62602-E	The directory structure is invalid.	HDLM was not installed correctly. Make sure that installation of HDLM was performed correctly.
KAIE62604-E	Unable to stop HBsA Service because Add-On module is currently running.	Wait until other products installed on the host complete their processing, and then retry the operation. For details on how to stop the service, see the explanation of the hbsasrv command.

Message ID	Description	Solution
KAIE62605-E	The connection error of HBsA Service has occurred.	Make sure that the TCP/IP environment on the host is normal. To do this, use the standard OS commands for network monitoring (such as netstat or ping.). If there is no problem, restart the system and then re-install HDLM. If the problem persists, collect the maintenance information and contact the Support Center.
KAIE62606-E	An error occurred while starting HBsA Service.	Re-install HDLM. If the problem persists, collect the maintenance information and contact the Support Center.
KAIE62607-E	The HBsA service could not start normally.	Make sure that the prerequisite patches have been applied, and then re-install HDLM.
KAIE62638-E	The value specified for server.agent.maxMemorySize in the server.properties file is not numeric.	Correct the value for server.agent.maxMemorySize, and then restart the HBsA service.
KAIE62639-E	The value specified for server.agent.maxMemorySize in the server.properties file is outside the valid range.	Correct the value for server.agent.maxMemorySize, and then restart the HBsA service.

For details on how to collect maintenance information, see the manual *HiCommand® Dynamic Link Manager User's Guide*.

Acronyms and Abbreviations

AJP	Apache JServ Protocol
ASCII	American standard code for information interchange
CA	certificate authority
CLI	Command Line Interface
CPU	central processing unit
CSR	certificate signing request
DEP	data execution prevention
DHCP	dynamic host configuration protocol
EM64T	extended memory 64 technology
FC-SP	fibre channel security protocol
GUI	graphical user interface
HBA	host bus adapter
HDLM	A generic term for HiCommand® Dynamic Link Manager, and Hitachi Dynamic Link Manager
HDLM 5.2	Hitachi Dynamic Link Manager 05-02
HGLAM	HiCommand® Global Link Availability Manager
HSSM	HiCommand® Storage Services Manager
HTTP	hypertext transfer protocol
IP	internet protocol
IPF	Itanium Processor Family
LDAP	lightweight directory access protocol
LU	logical unit
NAS	network attached storage
NTP	network time protocol
OS	operating system
RADIUS	remote authentication dial in user service
SAN	storage area network
SNMP	simple network management protocol
SP	Service Pack
SSL	secure socket layer
SSO	single sign-on
TLS	transport layer security
URL	uniform resource locator
XML	extensible markup language

Index