HITACHI
Inspire the Next

Hitachi Command Suite

8.7

Installation and Configuration Guide

MK-90HC173-27
October 2019

Contents

Preface

This guide provides information about installing and configuring Hitachi Command Suite (HCS).

Intended audience

This document provides instructions for storage administrators.

Product version

This document revision applies to HCS v8.7.0 or later.

Release notes

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

Related documents

Product user documentation is available on Hitachi Vantara Support Connect: https://support.hds.com/en_us/documents.html. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

- *Hitachi Command Suite User Guide*, MK-90HC172
- *Hitachi Command Suite Administrator Guide*, MK-90HC175
- *Hitachi Command Suite CLI Reference Guide*, MK-90HC176
- *Hitachi Command Suite Tiered Storage Manager CLI Reference Guide*, MK-90HC177
- *Hitachi Command Suite Messages*, MK-90HC178
- *Hitachi Command Suite Mainframe Agent Installation and Configuration Guide*, MK-96HC130
- *Hitachi Command Suite System Requirements*, MK-92HC209

- *Hitachi Command Suite Replication Manager Configuration Guide*, MK-98HC151
- *Hitachi Command Suite Replication Manager User Guide*, MK-99HC166
- *Hitachi Command Suite Replication Manager Application Agent CLI Reference Guide*, MK-90HC181
- *Hitachi Command Suite Replication Manager Application Agent CLI User Guide*, MK-90HC189
- *Hitachi Command Suite Tuning Manager User Guide*, MK-92HC022
- *Hitachi Command Suite Tuning Manager Installation Guide*, MK-96HC120
- *Hitachi Ops Center Automator User Guide*, MK-92HC205
- *Hitachi Ops Center Automator Installation and Configuration Guide*, MK-92HC204
- *Hitachi Ops Center Automator Messages*, MK-92HC221
- *Hitachi Command Suite Virtual Appliance Installation Guide*, MK-92HC236

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. ▪ Indicates emphasized words in list items.
Italic	▪ Indicates a document title or emphasized words in text. ▪ Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g group` (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`

Convention	Description
< > angle brackets	Indicates variables in the following scenarios: ▪ Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<report-name><file-version>.csv` ▪ Variables in headings.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.

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

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

Conventions for storage capacity values

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

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1{,}000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1{,}000^3$ bytes
1 terabyte (TB)	1,000 GB or $1{,}000^4$ bytes
1 petabyte (PB)	1,000 TB or $1{,}000^5$ bytes
1 exabyte (EB)	1,000 PB or $1{,}000^6$ bytes

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

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

Accessing product documentation

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

Getting help

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

Hitachi Vantara Community is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

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

Thank you!

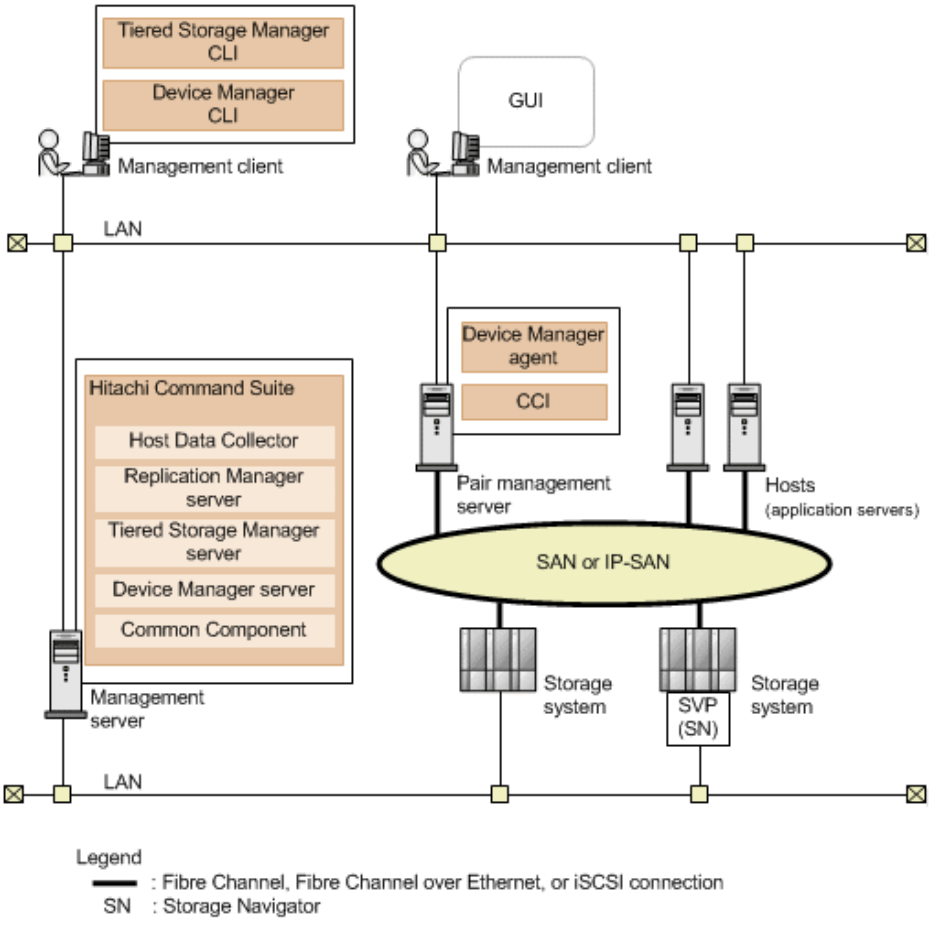
Chapter 1: Overview

This chapter provides basic system configuration information for Hitachi Command Suite.

About basic system configurations

Hitachi Command Suite (HCS) can manage different storage systems. A basic configuration must include a management server and appropriate components.

The following figure shows a basic system configuration for Hitachi Command Suite.



In this example, note the following:

- **Enterprise-class storage system**

  General term for the following enterprise-class storage systems: Hitachi Virtual Storage Platform 5000 series (VSP 5000 series), Hitachi Virtual Storage Platform G1000 (VSP G1000), Hitachi Virtual Storage Platform G1500 (VSP G1500), Hitachi Virtual Storage Platform F1500 (VSP F1500), Hitachi Virtual Storage Platform (VSP), and Hitachi Universal Storage Platform V/VM (USP V/VM).

  - SVP

    The computer used to manage the following storage systems: Enterprise-class storage systems, VSP 5000 series, VSP G1000, VSP G1500, VSP F1500, VSP F350, F370, F700, F900, VSP F400, F600, F800, VSP G200, G400, G600, G800, VSP G350, G370, G700, G900, VSP N400, N600, N800 or Hitachi Unified Storage VM (HUS VM). For enterprise-class storage systems or HUS VM, the SVP is built into the storage system as a component. For VSP Gx00 models, VSP Fx00 models, or VSP Nx00 models servers that provide the storage system management functionality can be installed as the SVP.

  - Hitachi Storage Navigator

    A Device Manager component. Using Storage Navigator you can configure storage systems, set up resources, and perform advanced tasks for managing and optimizing the storage systems.

    The name of the storage system management tool differs depending on the storage system:

    For Hitachi Virtual Storage Platform 5000 series, Hitachi Virtual Storage Platform G1000, Hitachi Virtual Storage Platform G1500, Hitachi Virtual Storage Platform F1500, VSP F350, F370, F700, F900, VSP F400, F600, F800, VSP G200, G400, G600, G800, Hitachi Virtual Storage Platform G350, G370, G700, G900, VSP N400, N600, N800: Hitachi Device Manager - Storage Navigator

    For VSP, USP V/VM, and HUS VM: Storage Navigator

    This tool is referred to as "Storage Navigator" unless there is a need to distinguish Device Manager - Storage Navigator and Storage Navigator.

- **Midrange storage system**

  A general term for the following storage systems: HUS100, Hitachi AMS 2000, Hitachi SMS, and Hitachi AMS/WMS.

You use HCS through a management client (either the web client GUI or the Device Manager and Tiered Storage Manager CLI) from which you can operate HCS, Tiered Storage Manager, and Replication Manager.

The management server (where HCS is installed) centrally manages the storage systems and hosts. The management server supports an active-standby type clustering configuration consisting of two servers.

The management client accesses the servers and storage systems over a TCP/IP network. Hosts (application servers) access the volumes in storage systems that are managed by HCS over a storage area network (SAN) or an IP-SAN.

HCS consists of the following components, which are always installed or removed together on the management server:

- Hitachi Command Suite Common Component

  Provides user account management, security monitoring, and other functions common to all HCS products.

- Device Manager server

  The component used by HCS to manage storage system volumes.

- Tiered Storage Manager server

  The component used by Tiered Storage Manager to manage storage system volume migration.

- Replication Manager server

  The component used by Replication Manager to manage storage system volume replication.

- Host Data Collector

  The component used to collect information about hosts (normal hosts, virtual machines, and virtualization servers), and information about the volumes used by the hosts.

  Note:

  The Host Data Collector component can be installed on other servers and accessed remotely by HCS.

The pair management server collects management information, such as copy pair status and configuration. The following components are installed on the pair management server:

- Device Manager agent

  Collects hosts and storage system information.

- Command Control Interface (CCI)

  Controls storage system copy pairs.

Tip:

Device Manager, Tiered Storage Manager, and Replication Manager support configurations other than those discussed here. For details about the system configurations for each program, see the *Hitachi Command Suite Administrator Guide* and the *Hitachi Command Suite Replication Manager Configuration Guide*.

Prerequisites for basic configurations

Hitachi Command Suite can manage different types of storage systems.

The information in this guide assumes the following system configuration:

- HCS (and Common Component) are used to manage user accounts.
- The system is not linked to an external authentication server.
- For the management server:
  - Only one management server is configured.
  - The management server is not part of a cluster configuration.
  - The management server and management client communicate with each other using non-SSL protocol.
- For copy pair management:
  - HCS is configured for open-volume copy pair management at a single site.
  - Copy pairs are centrally managed from a pair management server.
- For collecting information about managed hosts:
  - The Device Manager agent is installed only on the pair management server used to centrally manage copy pairs.
  - The Host Data Collector component is installed on the management server (from a silent installation initiated by the integrated installer).

Note: Other configurations are possible. For more information, see the *Hitachi Command Suite Administrator Guide* and the *Hitachi Command Suite Replication Manager Configuration Guide*.

Media installations

The installation media includes the HCS product installers and the programs that must be installed by storage and server administrators.

If your media is for Windows, it also includes the following files:

- Index file: *DVD-drive*:\Index.htm
- Readme file: *DVD-drive*:\Readme.txt

Server products

- All-in-One Installer (Windows only)
  - Device Manager
  - Tiered Storage Manager
  - Replication Manager
  - Tuning Manager
  - Compute Systems Manager
  - Ops Center Automator
- Hitachi Command Suite (base product)
  - Device Manager
  - Replication Manager
  - Tiered Storage Manager
- Tuning Manager
- Compute Systems Manager
- Ops Center Automator

Agent products

- Host Data Collector
- Device Manager Agent
- Replication Manager add-on
- Replication Manager Application Agent
- Device Manager Mainframe Agent

Other products

- Hitachi Storage Navigator Modular 2 (integrated installation for Windows only)

Agent software for storage administrators

- Tuning Manager Agent for RAID
- Tuning Manager Agent for Server System
- Tuning Manager Agent for SAN Switch
- Tuning Manager Agent for Network Attached Storage
- Tuning Manager Agent for Oracle
- Tuning Manager Agent for Microsoft SQL Server
- Tuning Manager Agent for DB2
- Tuning Manager Agent for Enterprise Applications
- RAID Agent Extension

Regarding upgrade installation

The following software versions support an upgrade installation from the installation media.

v6.0.0 or later:

- Device Manager server
- Tiered Storage Manager server
- Replication Manager server

Note:

- To upgrade the Replication Manager server when it is connected to Business Continuity Manager, see the *Hitachi Command Suite Replication Manager Configuration Guide*.
- When upgrading from v7.6.1 or earlier, you cannot migrate data from the Tiered Storage Manager GUI in legacy mode. To migrate data by using migration groups, use the Tiered Storage Manager CLI.

About installing Hitachi Command Suite by using a virtual appliance

When VMware ESXi is used, you can create a virtual machine on which Hitachi Command Suite (HCS) is installed by using a virtual appliance.

The virtual machine that is created by using the virtual appliance for HCS has the following products already installed:

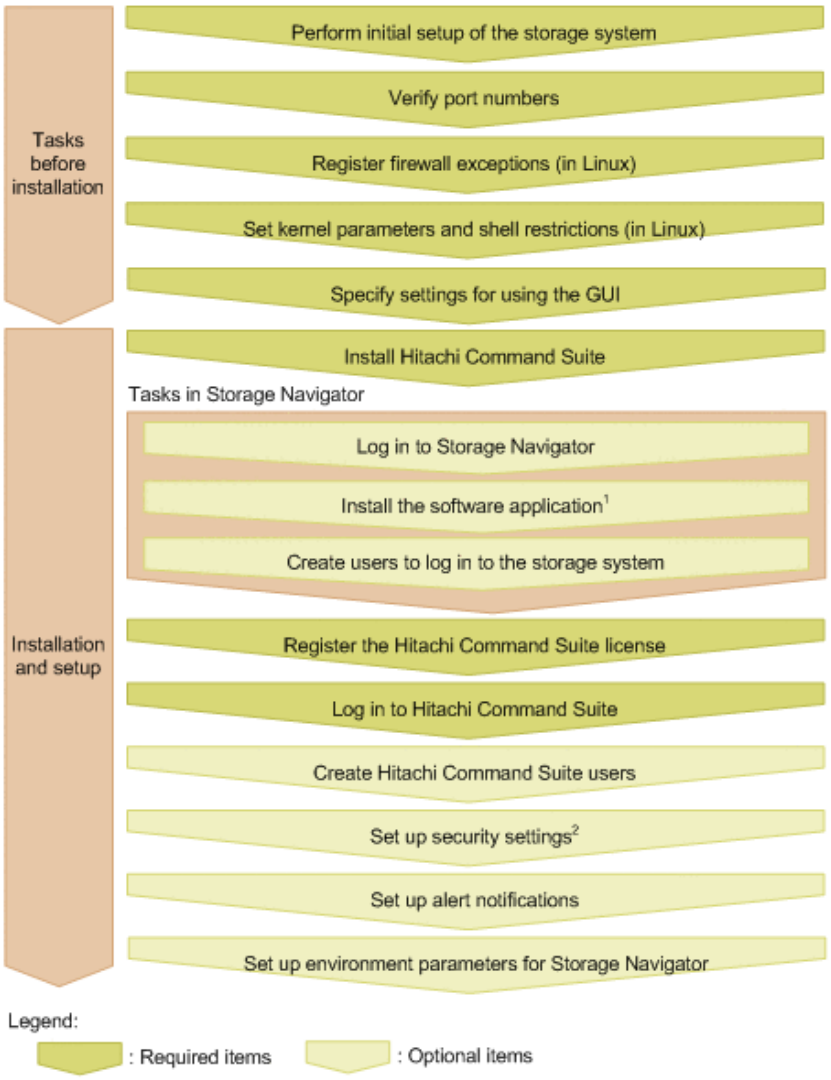
- Device Manager server
- Tiered Storage Manager server
- Replication Manager server
- Tuning Manager server
- Compute Systems Manager server
- Host Data Collector
- Device Manager agent
- CCI

When installing other HCS products other than above, use the integrated installation media.

For more details on installing HCS by using a virtual appliance, see the *Hitachi Command Suite Virtual Appliance Installation Guide*.

Workflow for installing and setting up Hitachi Command Suite

The following figure shows the workflow to install and set up Hitachi Command Suite.



Notes:

1. To register a storage system in Hitachi Command Suite, the license key for the software application of the storage system must be installed. If the license key is not installed, install it before logging into Hitachi Command Suite.

2. Installing Hitachi Command Suite enables secure communication, and enables user account authentication to be linked between Hitachi Command Suite and VSP G series or VSP F series. Note that you need to specify the secure communication settings again in the following cases:
   - If a certificate other than the default certificate is used to enhance security
   - If secure communication is used between the Device Manager server and a component other than
   - VSP 5000 series, VSP G series, VSP F series, or VSP N series

For information about the following tasks, see the documentation listed:

- Completing the Storage Navigator tasks listed in the workflow: *System Administrator Guide* or *System Administrator Guide*.
- Initial setup of the storage system: Documentation for your storage system.
- Registering the storage system, specifying settings for using the GUI, and configuring alert notifications and the environment parameters of Storage Navigator: *Hitachi Command Suite User Guide*.
- Configuring alert notifications and the environment parameters of Storage Navigator: *Hitachi Command Suite Administrator Guide*.

Chapter 2: Hitachi Command Suite server installation

This module describes how to install and set up servers.

Hitachi Command Suite installers

The installation media includes different product installers. The following table lists the products that are installed by each installer:

Installer	Installer contents
All-in-One Installer	▪ Hitachi Command Suite (includes Device Manager, Tiered Storage Manager, and Replication Manager) ▪ Tuning Manager ▪ Compute Systems Manager ▪ Ops Center Automator
Integrated installer	▪ Hitachi Command Suite (includes Device Manager, Tiered Storage Manager, and Replication Manager)
Individual product installers	▪ Tuning Manager ▪ Compute Systems Manager ▪ Ops Center Automator ▪ Storage Navigator Module 2 ▪ Host Data Collector ▪ Device Manager Agent ▪ Replication Manager add-on

Installer	Installer contents
	▪ Replication Manager Application Agent ▪ Mainframe Agent

- All-in-One Installer

  This installer installs products in batch with minimal input or tasks. Then, if necessary, you use the individual product installers to install other products you want.

  The installer installs products on management servers that run the following operating systems:

  - Windows Server 2008 R2 (Server Core is not supported)
  - Windows Server 2012 or Windows Server 2012 R2 (Server Core and Minimal Server Interface environments are not supported)
- Integrated installer

  Use the integrated installer in the following situations:

  - The management server information or memory heap size is changed from the default settings.
  - To install Hitachi Command Suite in a cluster environment.
  - To install Hitachi Command Suite, Tuning Manager, Compute Systems Manager, or Ops Center Automator individually.
- Individual product installers

  You use the individual product installers with one of the other two installers after the installation is complete. Then, if necessary, use the individual product installers to install other products you want.

Planning for server installation

Before installing the Hitachi Command Suite software on the server, verify the conditions and gather the information you need to perform the installation.

Server installation conditions using the All-in-One Installer

The All-in-One Installer allows you to perform a batch installation of Hitachi Command Suite products with minimal input or tasks.

The following items can be installed using the All-in-One Installer:

- Products to install
  - Hitachi Command Suite (Device Manager, Tiered Storage Manager, and Replication Manager)
  - Tuning Manager
  - Compute Systems Manager
  - Ops Center Automator
- Installation destination path (new installation only)

  Select this setting to change the installation destination path.

  If a product is selected that is already installed, that product is overwritten, or an upgrade installation is performed in the same folder as the existing installation.
- Database file storage destination (new installation only)

  Specify the storage destination for database files.

  Default: *installation-destination-path*\database
- Database file backup destination (if a Hitachi Command Suite product is already installed on the management server)

  To back up database files, select the check box, and specify the destination for database file backup.

  Default: *installation-destination-path-for-Hitachi-Command-Suite*\Base64\HCS_backup
- Items to specify when setting up a cluster in Windows. For new installations, default values do not exist for any of these items.
  - Name of the resource group for the cluster management application to which the Hitachi Command Suite product services are to be registered. [1, 2]
  - Logical host name (network name of a cluster management IP address that is registered as a client access point) [1]
  - Host name of an active node [1]
  - Host name of a standby node [1]
  - Database storage path [1]

  Note:

  1. You do not need to specify this item when the cluster configuration is already set up by another Hitachi Command Suite product.
  2. If you changed the name of the resource group to which the Hitachi Command Suite product services are registered, enter the new resource group name.

Server installation conditions using the integrated installer

Before using the integrated installer for the HCS server, determine the required information.

Each item specified during installation has default values (such as the installation destination path and management server information).

Note:

Hitachi recommends accepting default values when available.

- The All-in-One Installer allows you to perform a batch installation of Hitachi Command Suite products with only a few user operations.
- Use the individual product installer when you are not using the default values.
- The items in the table below can be changed in the integrated installer.

New installations

The following table lists default values that are required for new installations only:

Platform	Installation destination path	Storage destination path for database files	Management server information
Windows	`%ProgramFiles%\HiCommand`	*installation-destination-path*`\database`	Host name set for the OS or IP address
Linux	`/opt/HiCommand`	`/var/`*installation-destination-path*`/database`	

All installations

The following information is required for all installations:

- Destination for database file backup (if HCS products are already installed on the management server):

  Windows: *installation-destination-path*\backup

  Linux: /var/*installation-destination-path*/backup

- Memory heap size
  - Default: Large
  - Expected LDEV count: 6,001 or more
  - Number of file servers or NAS modules: 2 or more
- Items to specify when setting up a cluster in Windows. For new installations, default values do not exist for any of these items.
  - Name of the resource group for the cluster management application to which the Hitachi Command Suite product services are to be registered. [1, 2]
  - Logical host name (network name of a cluster management IP address that is registered as a client access point) [1]
  - Host name of an active node [1]
  - Host name of a standby node [1]
  - Database storage path [1]

Note:

1. You do not need to specify this item when the cluster configuration is already set up by another Hitachi Command Suite product.
2. If you changed the name of the resource group to which the Hitachi Command Suite product services are registered, enter the new resource group name.

Notes about upgrading installations from v7.6.1 or earlier

When upgrading an installation from v7.6.1 or earlier to v8.0.0 or later, use the All-in-One Installer.

When upgrading an installation from v7.6.1 or earlier to v8.0.0 or later:

- Upgrade all Hitachi Command Suite products to v8.0.0 or later.

  In an environment where v7.6.1 or earlier products are used with v8.0.0 or later Hitachi Command Suite products, you might not be able to register user accounts and Hitachi Command Suite products might not operate correctly.
- Hitachi Command Suite product databases for v7.6.1 and earlier are backed up. After installation is complete, you can delete these backed up databases. To delete backed up databases, open the following file:

  Windows:

  `%ProgramFiles%\HiCommand\backup\exportpath.txt`

  Linux:

  `/opt/HiCommand/backup/exportpath.txt`

  Delete the file indicated in the `file` line, delete the directory indicated in the `exportdir` line, and then delete the `exportpath.txt` file.
- If a remote connection with the Tuning Manager server is enabled, upgrade both the Device Manager server and Tuning Manager server to v8.0.0 or later.
- When upgrading an installation to a version that is earlier than 6.0.0, or to version 8.0.0 or later, upgrade to v6.x or v7.x, and then upgrade to v8.0.0 or later.

Note: When upgrading to v8.0.0 or later, the installation destination, port numbers, and command names are changed. You need to reset the port numbers and the secure communication settings.

Changes in v8.0.0 and later

Installation destination and database file storage destinations

Installation locations and default values that changed in v8.0.0 and later.

The default installation destination for Hitachi Command Suite and the default database file storage destination are changed.

Table 1 Installation location and database file storage location (default)

Item	v7.6.1 and earlier	v8.0.0 and later
Installation location	Windows: `%ProgramFiles(x86)%\HiCommand`	Windows: `%ProgramFiles%\HiCommand`
Database storage location	Windows: `%ProgramFiles(x86)%\HiCommand\database`	Windows: `%ProgramFiles%\HiCommand\database`

When upgrading to v8.0.0 or later, if v7.6.1 or earlier is installed in one of the following folders, the installation destination is changed.

Table 2 Installation location change (Windows)

v7.6.1 and earlier	v8.0.0 and later
%ProgramFiles(x86)%	*%ProgramFiles%*
%SystemRoot%\SysWOW64	
%CommonProgramFiles(x86)%	*%CommonProgramFiles%*

When upgrading to v8.0.0 or later, if the database files of the installed products are stored in different locations, the database files for the products are stored together in the following folder:

Device-Manager-database-file-storage-destination\x64

Installation destination for Common Component

The installation destination for Common Component is changed.

Upgrading from v7.6.1 or earlier:

In Windows:

installation-destination-path\Base

In Linux:

installation-destination-path/Base

Upgrading to v8.0.0 or later:

In Windows:

installation-destination-path-for-Hitachi-Command-Suite\Base64

In Linux:

installation-destination-path-for-Hitachi-Command-Suite/Base64

Port numbers and command names

The default values for port numbers used by Common Component and port numbers used for remote connections with the Tuning Manager server are changed.

For details about port numbers used by Hitachi Command Suite products, see the *Hitachi Command Suite Administrator Guide*.

Command names changed from `hcmdsxxxx` to `hcmds64xxxx`.

Hitachi Command Suite installation path name restrictions

The following tables list the default installation paths for Hitachi Command Suite and the installation path requirements.

Table 3 HCS default installation path

Platform	Default installation path
Windows	`%ProgramFiles%\HiCommand`
Linux	`/opt/HiCommand`

Each Hitachi Command Suite product is installed in a directory of Hitachi Command Suite.

Table 4 HCS installation destination path references (Windows)

Product	Installation destination path (Windows)
Device Manager	Default: `%ProgramFiles%\HiCommand\DeviceManager` Non-default: *`installation-destination-path-for-Hitachi-Command-Suite`*`\DeviceManager`
Replication Manager	Default: `%ProgramFiles%\HiCommand\ReplicationManager` Non-default: *`installation-destination-path-for-Hitachi-Command-Suite`*`\ReplicationManager`
Tiered Storage Manager	Default: `%ProgramFiles%\HiCommand\TieredStorageManager` Non-default: *`installation-destination-path-for-Hitachi-Command-Suite`*`\TieredStorageManager`
Common Component	Default: `%ProgramFiles%\HiCommand\Base64` Non-default: *`installation-destination-path-for-Hitachi-Command-Suite`*`\Base64`
Host Data Collector	Default: `%ProgramFiles%\HiCommand\HDC` Non-default: *`installation-destination-path-for-Hitachi-Command-Suite`*`\HDC`

Table 5 HCS installation destination path references (Linux)

Product	Installation destination path (Linux)
Device Manager	Default: `/opt/HiCommand`

Product	Installation destination path (Linux)
	Non-default: *installation-destination-path-for-Hitachi-Command-Suite*
Replication Manager	Default: `/opt/HiCommand/ReplicationManager` Non-default: *installation-destination-path-for-Hitachi-Command-Suite*`/ReplicationManager`
Tiered Storage Manager	Default: `/opt/HiCommand/TieredStorageManager` Non-default: *installation-destination-path-for-Hitachi-Command-Suite*`/TieredStorageManager`
Common Component	Default: `/opt/HiCommand/Base64` Non-default: *installation-destination-path-for-Hitachi-Command-Suite*`/Base64`
Host Data Collector	Default: `/opt/HiCommand/HDC` Non-default: *installation-destination-path-for-Hitachi-Command-Suite*`/HDC`

For a new installation of HCS, the default HCS installation location can be changed. If you change the location, ensure that the path name adheres to the following requirements.

Table 6 Installation path name requirements

Description	Requirements
Absolute path name length	64 bytes maximum
Allowed path name characters	Windows: A to Z, a to z, 0 to 9, periods (.), underscores (_), left parentheses (( ), right parentheses ( )), single-byte spaces, backslashes (\), and colons (:) Linux: A to Z, a to z, 0 to 9, underscores (_), and forward slashes (/)
Path name restrictions	Windows: ▪ Do not include consecutive spaces. ▪ Do not include a period or space at the end of a folder name.

Description	Requirements
	▪ Do not use parentheses, except for the character string `(x86)`. ▪ If `(x86)` is included in the installation path, also include a space somewhere in the installation path. ▪ Do not include a symbolic link and junction for the installation folder. ▪ Do not specify the root of a drive as the destination. ▪ Do not specify a network drive. Linux: ▪ Do not include a path delimiter (/) at the end of the directory path. ▪ If Common Component has not been installed, ensure that the installation directory you specify does not contain any files or subdirectories.

Database file storage path name restrictions (new installations only)

You can change the default database file storage location. If you change the location, ensure that the path name adheres to the restrictions in the following table.

Table 7 Database file storage path and location requirements

Description	Requirements
Absolute path name length	90 bytes maximum
Allowed path name characters	Windows: A to Z, a to z, 0 to 9, periods (.), underscores (_), left parentheses (( ), right parentheses ( )), single-byte spaces, backslashes (\), and colons (:) Linux: A to Z, a to z, 0 to 9, periods (.), underscores (_), and forward slashes (/)
Path name restrictions	Windows: ▪ Do not include consecutive spaces. ▪ Do not include a period or space at the end of a folder name.

Description	Requirements
	▪ Do not use parentheses, except for the character string `(x86)`. ▪ Do not include a symbolic link and junction for the installation folder. ▪ Do not specify the root of a drive as the destination. ▪ Do not specify a network drive. Linux: Do not include a path delimiter (/) at the end of the directory path.

Management server information

Install HCS on the management server. To access the management server from the web client, include the host name or IP address in the URL.

- When specifying the host name, verify that the management server host name is 128 bytes maximum.
- When using an IP address to access a management server with multiple NICs, use the IP address for the system connected to the management client.

Memory heap size for Device Manager server

The value that is set for the memory heap size depends on the number of LDEVs, and the number of file servers or NAS modules managed by Hitachi Command Suite products.

Calculate the memory heap size by determining the following values and using the larger of the two:

- The number of managed LDEVs
- The number of managed file servers or NAS modules

Calculation based on the number of managed LDEVs

Table 8 Appropriate memory heap size for the Device Manager server

Managed Resource	Memory Heap Size		
	Small	Medium	Large
Number of LDEVs per storage system	2,000 or less	6,000 or less	6,001 or more

Calculation based on number of managed file servers

When managing file servers, set a memory heap size according to the number of file server clusters and the number of file servers as follows:

- When managing one file server or NAS module, set the memory heap size to `Medium`.
- When managing two or more file servers or NAS modules, set the memory heap size to `Large`.

Database file backup locations

If you change the database backup location, ensure that the path adheres to the restrictions in the following table.

Table 9 Database path and location requirements

Condition	Requirements
Absolute path length	Maximum 150 bytes
Allowed characters	Windows: A to Z, a to z, 0 to 9, periods (.), underscores (_), left parentheses ((), right parentheses ()), single-byte spaces, backslashes (\), and colons (:) Linux: A to Z, a to z, 0 to 9, underscores (_), and forward slashes (/)
Other conditions	Windows: ▪ Do not include consecutive spaces. ▪ Do not include a period or space at the end of a folder name. ▪ Do not use parentheses, except for the character string `(x86)`. ▪ Do not include a symbolic link and junction. ▪ Do not specify the root of a drive as the destination. ▪ Do not specify a network drive. Linux: Do not specify a path delimiter (/) at the end of the directory path.

Resource group name requirements (Windows)

When configuring a cluster environment in Windows and creating a resource group name, ensure that the resource group name adheres to the following requirements.

Table 10 Resource group name requirements

Description	Requirements
Absolute path length	1024 bytes maximum
Allowed resource group name characters	A to Z, a to z, 0 to 9
Resource group name restrictions	The following characters cannot be used: Exclamation mark (!), double quotation mark ("), ampersand (&), closing parenthesis ( )), asterisk (*), caret (^), vertical bar (|), less-than sign (<), or greater-than sign (>).
Other conditions	Register the resource group name in advance to the cluster management application.

Logical host name requirements (Windows)

When configuring a cluster environment in Windows and creating a logical host name, ensure that the logical host name adheres to the following requirements.

Table 11 Logical host name requirements

Description	Requirements
Absolute path length	Integrated installer: 128 bytes maximum All-in-One Installer: 32 bytes maximum
Allowed logical host name characters	Integrated installer: N/A All-in-One Installer: A to Z, a to z, 0 to 9, and hyphen (-). A hyphen cannot be used as the first or last character of a logical host name.
Logical host name restrictions	Register the logical host name (client access point) in advance by using the cluster management application.

Host name requirements for an active node (Windows)

When configuring a cluster environment in Windows and creating a host name for an active node, ensure that the host name adheres to the following requirements.

Table 12 Host name requirements

Description	Requirements
Absolute path length	128 bytes maximum
Allowed host name characters	N/A
Host name restrictions	None

Host name requirements for a standby node (Windows)

When configuring a cluster environment in Windows and creating a host name for a standby node, ensure that the host name adheres to the following requirements.

Table 13 Host name requirements

Description	Requirements
Absolute path length	128 bytes maximum
Allowed host name characters	N/A
Host name restrictions	None

Hitachi Command Suite server installation preparations

Before installing Hitachi Command Suite, review the prerequisite tasks that are common to all operating systems and those that apply to specific environments.

- If you are going to upgrade the operating system, do so before you install the Hitachi Command Suite server.
- When installing Hitachi Command Suite on the same server where Hitachi File Services Manager resides due to server migration, migrate the Hitachi File Services Manager database.
- Review the information about avoiding port conflicts.
- Check your browser and Java settings. For more information about these settings, see the *Hitachi Command Suite User Guide*.
- To set up a cluster environment, create a resource group to which the Hitachi Command Suite product services are to be registered by using the cluster management application (Windows).

- For Linux, review the prerequisites about verifying that the host environment satisfies installation conditions and information about kernel parameter values and shell restrictions. For information about registering firewall exceptions, see the *Hitachi Command Suite Administrator Guide*.
- When installing Hitachi Command Suite v8.2.1 or later and Hitachi Command Suite products on the same server, the Hitachi Command Suite products must be v8.0.1 or later.

Caution: When upgrading to v7.0 or later, storage tiers (custom tiers) created from search conditions that included any of these items are removed but the volumes remain:

- Logical group
- Average array group usage
- Maximum array group usage
- SYSPLEXID/DEVN
- VOLSER
- P-VOL migration group
- P-VOL MU number

Avoiding port conflicts

If any of the HCS products use a port number that is also used by another product on the management server, the affected products may not operate correctly.

To avoid port conflicts, run the **`netstat`** command and check the output for conflicts.

Migrate the Hitachi File Services Manager database

When installing Hitachi Command Suite on the same server where Hitachi File Services Manager resides due to server migration, migrate the Hitachi File Services Manager database.

Depending on the environment of the migration source server, the procedure for importing the Hitachi File Services Manager database to the migration target server differs.

If a Hitachi Command Suite version earlier than 8.0.0 and Hitachi File Services Manager are installed on the same server:

1. Export the Hitachi File Services Manager and the Hitachi Command Suite databases from the migration source server.
2. Install Hitachi File Services Manager on the migration target server.
3. Import the Hitachi File Services Manager database to the migration target server.
4. Install Hitachi Command Suite on the migration target server.
5. Import the Hitachi Command Suite database to the migration target server.

If Hitachi Command Suite v8.0.0 or later and Hitachi File Services Manager are installed on the same server, or Hitachi Command Suite and Hitachi File Services Manager are installed on separate servers:

1. Export the Hitachi File Services Manager and the Hitachi Command Suite databases from the migration source server.
2. Install Hitachi File Services Manager on the migration target server.
3. Install Hitachi Command Suite on the migration target server.
4. Import the Hitachi Command Suite database to the migration target server.
5. Import the Hitachi File Services Manager database to the migration target server.

For more information about how to install Hitachi File Services Manager and how to export or import databases, see the Hitachi File Services Manager documentation.

Prerequisites for the management server (Linux)

Before installing HCS in a Linux environment, verify that the host environment satisfies installation conditions.

To do this, write **`localhost`** and the server host name to the `/etc/hosts` file.

Note: In the `/etc/hosts` file, do not specify any host name other than `localhost` as the host name that corresponds to the local loopback address (such as `127.0.0.1` or `::1`). If a management server name is specified to correspond with the local loopback address, a communication error might occur between Tiered Storage Manager CLI and the management server.

You must manually register exceptions for port numbers and exceptions for Linux firewalls. To register port numbers as exceptions, see the information about server ports. To register firewall exceptions for Linux, see the *Hitachi Command Suite Administrator Guide*.

About setting kernel parameters and shell restrictions (Linux)

Before installing HCS on Linux, set the kernel parameters and shell restrictions.

- Red Hat Enterprise Linux 5:

  Set the kernel parameters in the `/etc/sysctl.conf` and the shell restrictions in the `/etc/security/limits.conf` files.

- Red Hat Enterprise Linux 6:

  Set the kernel parameters in the `/etc/sysctl.conf` and the shell restrictions in the `/etc/security/limits.conf`

  and `/etc/security/limits.d/90-nproc.conf` files.

- Red Hat Enterprise Linux 7 or Oracle Linux 7:

  Set the kernel parameters in the `/etc/sysctl.conf` file. Set the shell restrictions in the `/etc/security/limits.conf` and the `/etc/security/limits.d/20-nproc.conf` files.

Note: Verify that the maximum value set for a kernel parameter does not exceed the maximum value specified by the operating system.

Recommended Red Hat Enterprise Linux 5 or Red Hat Enterprise Linux 6 /etc/sysctl.conf values

Before installing HCS on a Red Hat Enterprise Linux system, set the kernel parameters for the `/etc/sysctl.conf` file.

These settings depend on which HCS products you are installing:

- Common Component
- Device Manager
- Tiered Storage Manager
- Replication Manager
- Tuning Manager
- Compute Systems Manager
- Ops Center Automator

The following tables show the kernel parameter values you need to set. The formulas for calculating these values follow the tables.

Table 14 Kernel parameter values for Red Hat Enterprise Linux 5 or Red Hat Enterprise Linux 6 /etc/sysctl.conf (1/2)

Kernel Parameter	Installer Check value	Operating System Initial Value	HiRDB	Common Component	Device Manager
`fs.file-max`	297944	99483	42276	42276	155161
`kernel.threads-max`	16748	16384	576	142	162
`kernel.msgmni`	2066	1978	44	44	44
4th parameter of `kernel.sem`	1024	128	1024	9	10
2nd parameter of `kernel.sem`	32308	32000	7200	80	128

Kernel Parameter	Installer Check value	Operating System Initial Value	HiRDB	Common Component	Device Manager
`kernel.shmmax`	888509824	4294967295	200000000	24372224	613392384
`kernel.shmmni`	5091	4096	2000	0	995
`kernel.shmall`	1091000704	268435456	24372224	23793664	745348096

Table 15 Kernel parameter values for Red Hat Enterprise Linux 5 or Red Hat Enterprise Linux 6 /etc/sysctl.conf (2/2)

Kernel Parameter	Tiered Storage Manager Software	Replication Manager Software	Tuning Manager	Compute Systems Manager	Automation Director
`fs.file-max`	512	512	41354	162478	133384
`kernel.threads-max`	30	30	32	453	615
`kernel.msgmni`	0	0	12	44	53
4th parameter of `kernel.sem`	1	1	12	10	1235
2nd parameter of `kernel.sem`	50	50	0	144	8646
`kernel.shmmax`	100745216	150000000	966656000	421699584	238248346
`kernel.shmmni`	0	0	0	995	2400
`kernel.shmall`	147486720	150000000	966656000	458306560	175963623

These formulas are for calculating kernel parameter values:

- For `kernel.shmmax`:

```
kernel-parameter-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    ,
    value-for-Common-Component
    + value-for-Device-Manager
    + value-for-Tiered-Storage-Manager
    + value-for-Replication-Manager
    + value-for-Tuning-Manager
    + value-for-Compute-Systems-Manager
    + value-for-Automation-Director
    ,
    value-for-HiRDB
}
```

- For `kernel.shmall`:

```
kernel-parameter-value-to-be-set =
Max{
    value-that-is-enabled-in-the-system
    ,
     initial-value-of-the-OS
}
+ value-for-Common-Component
+ value-for-Device-Manager
+ value-for-Tiered-Storage-Manager
+ value-for-Replication-Manager
+ value-for-Tuning-Manager
+ value-for-Compute-Systems-Manager
+ value-for-Automation-Director
+ value-for-HiRDB
```

- Other kernel parameters and shell restrictions:

```
kernel-parameter-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    + value-for-Common-Component
    + value-for-Device-Manager
    + value-for-Tiered-Storage-Manager
    + value-for-Replication-Manager
    + value-for-Tuning-Manager
    + value-for-Compute-Systems-Manager
    + value-for-Automation-Director
    ,
    value-for-HiRDB
}
```

Note:

Max{x, y, z} indicates the maximum value among x, y, and z.

Recommended Red Hat Enterprise Linux 7 or Oracle Linux 7 /etc/sysctl.conf values

Before installing HCS on a Red Hat Enterprise Linux system, set the kernel parameters for the `/etc/sysctl.conf` file.

These settings depend on which HCS products you are installing:

- Common Component
- Device Manager
- Tiered Storage Manager
- Replication Manager
- Tuning Manager
- Compute Systems Manager
- Ops Center Automator

The following tables show the kernel parameter values you need to set. The formulas for calculating these values follow the tables.

Table 16 Kernel parameter values for Red Hat Enterprise Linux 7 or Oracle Linux 7 /etc/sysctl.conf (1/2)

Kernel Parameter	Installer Check value	Operating System Initial Value	HiRDB	Common Component	Device Manager
`fs.file-max`	297944	99483	42276	42276	155161
`kernel.threads-max`	16748	16384	576	142	162
`kernel.msgmni`	2066	1978	44	44	44
4th parameter of `kernel.sem`	1024	128	1024	9	10
2nd parameter of `kernel.sem`	32308	32000	7200	80	128
`kernel.shmmax`	888509824	4294967295	200000000	24372224	613392384
`kernel.shmmni`	5091	4096	2000	0	995
`kernel.shmall`	1091000704	268435456	24372224	23793664	745348096

Table 17 Kernel parameter values for Red Hat Enterprise Linux 7 or Oracle Linux 7 /etc/sysctl.conf (2/2)

Kernel Parameter	Tiered Storage Manager Software	Replication Manager Software	Tuning Manager	Compute Systems Manager	Automation Director
`fs.file-max`	512	512	41354	162478	133384
`kernel.threads-max`	30	30	32	453	615
`kernel.msgmni`	0	0	12	44	53
4th parameter of `kernel.sem`	1	1	12	10	1235

Kernel Parameter	Tiered Storage Manager Software	Replication Manager Software	Tuning Manager	Compute Systems Manager	Automation Director
2nd parameter of `kernel.sem`	50	50	0	144	8646
`kernel.shmmax`	100745216	150000000	966656000	421699584	238248346
`kernel.shmmni`	0	0	0	995	2400
`kernel.shmall`	147486720	150000000	966656000	458306560	175963623

These formulas are for calculating kernel parameter values:

- For `kernel.shmmax`:

```
kernel-parameter-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    ,
    value-for-Common-Component
    + value-for-Device-Manager
    + value-for-Tiered-Storage-Manager
    + value-for-Replication-Manager
    + value-for-Tuning-Manager
    + value-for-Compute-Systems-Manager
    + value-for-Automation-Director

    ,
    value-for-HiRDB
}
```

- For `kernel.shmall`:

```
kernel-parameter-value-to-be-set =
Max{
    value-that-is-enabled-in-the-system
    ,
     initial-value-of-the-OS
}
+ value-for-Common-Component
+ value-for-Device-Manager
+ value-for-Tiered-Storage-Manager
+ value-for-Replication-Manager
+ value-for-Tuning-Manager
+ value-for-Compute-Systems-Manager
+ value-for-Automation-Director
+ value-for-HiRDB
```

- Other kernel parameters and shell restrictions:

```
kernel-parameter-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    + value-for-Common-Component
    + value-for-Device-Manager
    + value-for-Tiered-Storage-Manager
    + value-for-Replication-Manager
    + value-for-Tuning-Manager
    + value-for-Compute-Systems-Manager
    + value-for-Automation-Director
    ,
    value-for-HiRDB
}
```

Note:

Max{x, y, z} indicates the maximum value among x, y, and z.

Recommended Red Hat Enterprise Linux 5 /etc/security/limits.conf values

Before installing HCS on a Red Hat Enterprise Linux system, set the shell restriction values for the `/etc/security/limits.conf` file. Set the shell restrictions for soft and hard settings.

Note:

The soft value must be less than or equal to the hard value.

These settings depend on which HCS products you are installing:

- Common Component
- Device Manager
- Tiered Storage Manager
- Replication Manager
- Tuning Manager
- Compute Systems Manager
- Ops Center Automator

The following tables show the shell restriction values you need to set. The formula for calculating these values follow the tables.

Table 18 Shell restriction values for Red Hat Enterprise Linux 5 /etc/security/limits.conf (1/2)

Shell Restriction	Installer Check Value	Operating System Initial Value	HiRDB	Common Component	Device Manager
nofile (soft/hard)	8192	4096	8192	1346	0
nproc (soft/hard)	8391	8192	512	198	1

Table 19 Shell restriction values for Red Hat Enterprise Linux 5 /etc/security/limits.conf (2/2)

Shell Restriction	Tiered Storage Manager Software	Replication Manager Software	Tuning Manager	Compute Systems Manager	Automation Director
nofile (soft/hard)	0	0	1024	-	1104
nproc (soft/hard)	0	0	32	-	1398

The following formula is for calculating the values for the shell restriction:

```
shell-restrictions-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    + value-for-Common-Component
    + value-for-Device-Manager
    + value-for-Tiered-Storage-Manager
    + value-for-Replication-Manager
    + value-for-Tuning-Manager
    + value-for-Compute-Systems-Manager
    + value-for-Automation-Director
    ,
    value-for-HiRDB
}
```

Note:

Max{x, y} indicates the larger value of x or y.

Recommended Red Hat Enterprise Linux 6 /etc/security/limits.conf values

Before installing HCS on a Red Hat Enterprise Linux system, set the shell restriction values for the `/etc/security/limits.conf` file. Set the shell restrictions for soft and hard settings.

Note:

The soft value must be less than or equal to the hard value.

These settings depend on which HCS products you are installing:

- Common Component
- Device Manager
- Tiered Storage Manager
- Replication Manager
- Tuning Manager
- Compute Systems Manager
- Ops Center Automator

The following tables show the shell restriction values you need to set. The formula for calculating these values follow the tables.

Table 20 Shell restriction values for Red Hat Enterprise Linux 6 /etc/security/limits.conf (1/2)

Shell Restriction	Installer Check Value	Operating System Initial Value	HiRDB	Common Component	Device Manager
nofile (soft/hard)	8192	4096	8192	1346	0

Table 21 Shell restriction values for Red Hat Enterprise Linux 6 /etc/security/limits.conf (2/2)

Shell Restriction	Tiered Storage Manager Software	Replication Manager Software	Tuning Manager	Compute Systems Manager	Automation Director
nofile (soft/hard)	0	0	1024	528	1104

The following formula is for calculating the values for the shell restriction:

```
shell-restrictions-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    + value-for-Common-Component
    + value-for-Device-Manager
    + value-for-Tiered-Storage-Manager
    + value-for-Replication-Manager
    + value-for-Tuning-Manager
    + value-for-Compute-Systems-Manager
    + value-for-Automation-Director
    ,
    value-for-HiRDB
}
```

Note:

Max{x, y} indicates the larger value of x or y.

Recommended Red Hat Enterprise Linux 7 or Oracle Linux 7 /etc/security/limits.conf values

Before installing HCS on a Red Hat Enterprise Linux system, set the shell restriction values for the `/etc/security/limits.conf` file. Set the shell restrictions for soft and hard settings.

Note:

The soft value must be less than or equal to the hard value.

These settings depend on which HCS products you are installing:

- Common Component
- Device Manager
- Tiered Storage Manager
- Replication Manager
- Tuning Manager
- Compute Systems Manager
- Ops Center Automator

The following tables show the shell restriction values you need to set. The formula for calculating these values follow the tables.

Table 22 Shell restriction values for Red Hat Enterprise Linux 7 or Oracle Linux 7 /etc/security/limits.conf (1/2)

Shell Restriction	Installer Check Value	Operating System Initial Value	HiRDB	Common Component	Device Manager
nofile (soft/ hard)	8192	4096	8192	1346	0

Table 23 Shell restriction values for Red Hat Enterprise Linux 7 or Oracle Linux 7 /etc/security/limits.conf (2/2)

Shell Restriction	Tiered Storage Manager Software	Replicatio n Manager Software	Tuning Manager	Compute Systems Manager	Automation Director
nofile (soft/ hard)	0	0	1024	528	1104

The following formula is for calculating the values for the shell restriction:

```
shell-restrictions-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    + value-for-Common-Component
    + value-for-Device-Manager
    + value-for-Tiered-Storage-Manager
    + value-for-Replication-Manager
    + value-for-Tuning-Manager
    + value-for-Compute-Systems-Manager
    + value-for-Automation-Director
    ,
    value-for-HiRDB
}
```

Note:

Max{x, y} indicates the larger value of x or y.

Recommended Red Hat Enterprise Linux 6 /etc/security/limits.d/90-nproc.conf values

Before installing HCS on a Red Hat Enterprise Linux system, set the shell restriction values for the **`/etc/security/limits.d/90-nproc.conf`** file.

Note:
The soft value must be less than or equal to the hard value.

These settings depend on which HCS products you are installing:

- Common Component
- Device Manager
- Tiered Storage Manager
- Replication Manager
- Tuning Manager
- Compute Systems Manager
- Ops Center Automator

The following tables show the shell restriction values you need to set. The formula for calculating these values follow the tables.

Table 24 Shell restriction values for Red Hat Enterprise Linux 6 /etc/security/limits.d/90-nproc.conf (1/2)

Shell Restriction	Installer Check Value	Operating System Initial Value	HiRDB	Common Component	Device Manager
nproc (soft/hard)	8391	8192	512	198	1

Table 25 Shell restriction values for Red Hat Enterprise Linux 6 /etc/security/limits.d/90-nproc.conf (2/2)

Shell Restriction	Tiered Storage Manager Software	Replication Manager Software	Tuning Manager	Compute Systems Manager	Automation Director
nproc (soft/hard)	0	0	32	50	1398

The following formula is for calculating the values for the shell restriction:

```
shell-restrictions-value-to-be-set =
```

```
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    + value-for-Common-Component
    + value-for-Device-Manager
    + value-for-Tiered-Storage-Manager
    + value-for-Replication-Manager
    + value-for-Tuning-Manager
    + value-for-Compute-Systems-Manager
    + value-for-Automation-Director
    ,
    value-for-HiRDB
}
```

Note:

Max{x, y} indicates the larger value of x or y.

Recommended Red Hat Enterprise Linux 7 or Oracle Linux 7 /etc/security/limits.d/20-nproc.conf values

Before installing HCS on a Red Hat Enterprise Linux 7 or Oracle Linux 7 system, set the shell restriction values for the **`/etc/security/limits.d/20-nproc.conf`** file.

Note:

The soft value must be less than or equal to the hard value.

These settings depend on which HCS products you are installing:

- Common Component
- Device Manager
- Tiered Storage Manager
- Replication Manager
- Tuning Manager
- Compute Systems Manager
- Ops Center Automator

The following tables show the shell restriction values you need to set. The formula for calculating these values follow the tables.

Table 26 Shell restriction values for Red Hat Enterprise Linux 7 or Oracle Linux 7 /etc/security/limits.d/20-nproc.conf (1/2)

Shell Restriction	Installer Check Value	Operating System Initial Value	HiRDB	Common Component	Device Manager
nproc (soft/ hard)	8391	8192	512	198	1

Table 27 Shell restriction values for Red Hat Enterprise Linux 7 or Oracle Linux 7 /etc/security/limits.d/20-nproc.conf (2/2)

Shell Restriction	Tiered Storage Manager Software	Replication Manager Software	Tuning Manager	Compute Systems Manager	Automation Director
nproc (soft/ hard)	0	0	32	50	1398

The following formula is for calculating the values for the shell restriction:

```
shell-restrictions-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    + value-for-Common-Component
    + value-for-Device-Manager
    + value-for-Tiered-Storage-Manager
    + value-for-Replication-Manager
    + value-for-Tuning-Manager
    + value-for-Compute-Systems-Manager
    + value-for-Automation-Director
    ,
    value-for-HiRDB
}
```

Note:

Max{x, y} indicates the larger value of x or y.

Modifying kernel parameter values and shell restrictions

After you check the current kernel parameter values and shell restrictions against your estimated requirements, you can change the values if necessary.

Procedure

1. Back up the kernel parameter files.
2. Set the value of each parameter according to the estimate.
3. Restart the operating system.

Hitachi Command Suite server installation

When you install HCS on the management server, use the installation procedure that is appropriate for the operating system you are using.

Server installation prerequisites

Before installing HCS, review the information about planning for the installation. Then complete the following tasks.

Check server requirements and prerequisite software:

- For more information about server requirements and prerequisite software, see the *Hitachi Command Suite System Requirements*.

Stop Tuning Manager services (for an overwrite or upgrade installation):

- If a version earlier than 6.3 is installed on the same management server, stop the Tuning Manager Agent for SAN Switch service.
- If Tuning Manager is remotely connected, stop the Tuning Manager server service.

Run Tiered Storage Manager tasks when upgrading from v7.1.0 or earlier:

- If there are incomplete tasks (standby, running, or being canceled), go to the Tasks & Alerts tab and execute or cancel the tasks. After upgrading, register the canceled tasks as new.

Check the user group name when upgrading from v7.1 to v7.5.0:

- When upgrading to v7.6.0 or later, private logical groups are created and within these groups, top folders are created for each user group. The user group name is used as the initial folder name. Users that have Admin permission for user management should check the user group name before performing an upgrade installation.
- For more information about private logical groups, see the *Hitachi Command Suite User Guide*.

Remove the Plug-in for Virtualization Server Provisioning when upgrading from versions 7.1.1 to 7.6.1:

- If you are using Plug-in for Virtualization Server Provisioning, remove it. You cannot use Plug-in for Virtualization Server Provisioning in v8.0 or later.

Stop virus-detection programs.

- If a virus-detection program is running during installation, the installation might be slow, fail, or finish incorrectly.

Determine values that are set during installation:

- The installation destination path
- The database storage destination path
- Management server information (this step is not necessary when using the All-in-One Installer)
- Memory heap size (this step is not necessary when using the All-in-One Installer)
- The database backup destination

Determine values to specify when setting up a cluster in Windows. Default values do not exist for these items.

- Name of the resource group for the cluster management application to which the Hitachi Command Suite product services are to be registered.
- Logical host name (network name of a cluster management IP address that is registered as a client access point)
- Host name of an active node
- Host name of a standby node
- Database storage path (when setting up a cluster environment in Windows)

Prerequisite checker

The prerequisite checker verifies whether the installation destination satisfies the requirements.

- In Windows, use the integrated installation media or run the **`prereqchk.exe`** file in *`DVD-drive`*`:\HCS\`
- In Linux, run the **`prereqchk.sh`** file in *`DVD-ROM-mount-directory`*`/TOOL/PREREQCHK/`

  The results of running the prerequisite checker are output to `/var/opt/HInst/prereqchk_`*`YYYY-MM-DD-hh-mm-ss`*`/reports/report.txt`

  Note:
  - Do not run the prerequisite checker and the installer simultaneously.
  - Install Hitachi Command Suite in the order specified by the prerequisite checker.

For information about checking task status, see the *Hitachi Command Suite User Guide*.

Installing HCS using the All-in-One Installer (Windows)

Use the installation media for installing HCS.

You can use the All-in-One Installer to install Hitachi Command Suite only on a management server whose host name uses the following characters:

A to Z, a to z, 0 to 9, and hyphens (-), and periods (.)

If the host name of the target management server contains a character other than those above, use the individual product installers.

When specifying the management server, enter the IP address.

Procedure

1. Log on to Windows as the administrator.
2. Insert the installation media.
3. In the displayed window, select **All-in-One Installer** in the **Server Products** tree, and click **All-in-One Installer**.

   Note:

   If the installation window does not open, run the following command:

   DVD-drive:\HCS2\setup.exe
4. When you are prompted, enter the required information.

Result

After the installation is complete, perform the necessary setup for each product.

Installing HCS using the integrated installer (Windows)

Install HCS on a Windows host by using the installation media.

Procedure

1. Log on to Windows as the administrator.
2. Insert the installation media.
3. In the displayed window, select **HDvM/HRpM/HTSM** in the **Server Products** tree, and click **Install**.

   Note:

   If the installation window does not open, run the following command:

   DVD-drive:\HCS\setup.exe
4. When you are prompted, enter the required information.
5. In the Installation Completed window, select the **When installation completes, open the Device Manager GUI** check box.
6. Click **Finish**.

The GUI login window appears.

Note:

- If the Remote Desktop Session HOST role service is installed on the Windows host on which you plan on installing HCS products, then make sure to enable **Turn off Windows Installer RDS Compatibility** in the Windows Local Group Policy Editor. If this setting is not configured or disabled, the installation of common component might fail with the KAIB20200-E error.

  To check the current policy, browse the following directory in Windows Local Group Policy Editor.

  Local Computer Policy > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Application Compatibility**

  If the Windows host server is configured as a member server of Windows Active Directory, then check with your domain administrator about the configuration regarding the above policy.

- The GUI login window might not display if you are using SSL communication or if the port number of Common Component has been changed. If this is the case, type the URL for Device Manager in the address bar of the web browser.
- A blank or transitional window might be displayed after logging on to Device Manager if Internet Explorer 11 is set as the default browser. If this is the case, restart the web browser and type the URL for Device Manager in the address bar of the web browser.

When you upgrade to v7.5.0 or later, if v7.4.1 or earlier is installed on a drive other than the system drive, a `temp` folder is created in the `root` folder. You can delete the `temp` folder.

Installing HCS on Linux

Install HCS on a Linux host by using the installation media.

Procedure

1. Log on to Linux as the root user.
2. Insert the installation media.

   If the drive with the installation media is not mounted automatically, mount it manually.
3. Navigate to the installer directory:

   DVD-ROM-mount-directory/HCS/*platform-name*/install.sh
4. Run the command **#./install.sh**
5. When you are prompted, enter the required information.

Result

When the installation is complete, the following message appears:

```
Hitachi Command Suite installation completed successfully.
```

Note: If the integrated installation media is automatically mounted (Red Hat Enterprise Linux only), unmount the media and mount it again without specifying `noexec`.

These characters can be used in the mount path of a DVD-ROM: A to Z, a to z, 0 to 9, underscores (_), forward slashes (/).

Post-installation tasks (new installation)

After a new installation of Device Manager, Tiered Storage Manager, or Replication Manager, there are tasks to complete in Storage Navigator and Hitachi Command Suite.

Product	Tasks to complete
Storage Navigator	The following tasks apply: ▪ Open a browser and log in to Storage Navigator. This log in procedure is for the super-user who logs into Storage Navigator for the first time and sets up the user accounts. The super-user has a built-in ID that includes all permissions and a default password. ▪ Register the licenses for Storage Navigator products. To register a storage system in HCS, the license key for the software products of the storage system must be installed. ▪ Create user accounts for storage system registration. ▪ Create an administrator login user account (required in the event that HCS is not available). ▪ Create user accounts for accessing NAS Manager when using VSP Gx00 models, VSP Fx00 models, or VSP Nx00 models with NAS modules.

Product	Tasks to complete
Hitachi Command Suite	▪ Open a browser and log in to HCS. ▪ Register the license for HCS. ▪ Create a new user who will be the storage administrator and to whom you can assign permissions for all HCS resources.

After you create a storage administrator user account in HCS, the storage administrator can discover and register storage systems and hosts, add accounts for other storage administrators, and begin using HCS.

For VSP 5000 series, VSP G series, VSP F series, and VSP N series, user accounts are authenticated by Hitachi Command Suite during log in to Storage Navigator or CCI, so the user accounts can be centrally managed from HCS. For more information about centralized management of user accounts, see the *Hitachi Command Suite User Guide*.

Note: For version 8.1.3 or later, the default certificate for the Device Manager server is registered to the keystore, and the SSL/TLS communication setting is enabled. This setting is used to link user account authentication, if the storage system is VSP G series, VSP F series, and VSP N series.

Registering Hitachi Command Suite licenses

Before using HCS to manage storage systems and hosts, you must register valid licenses. Each product managed from HCS requires a registered license.

Procedure

1. Start a web browser.
2. In the address bar, specify the URL for HCS in the following format:

   protocol`://`*IP-address-of-the-management-server*`:`*port-number*`/DeviceManager/`

   - *protocol*

     Specify `http` for non-SSL communication and `https` for SSL communication.

   - *IP-address-of-the-management-server*

     Specify the IP address or host name of the management server.

   - *port-number*

     Confirm the port numbers that are used to communicate with the management client (GUI). If a port number other than the default is set, refer to the `user_httpsd.conf` file, and then use the number specified in that file.

     For non-SSL communication, the default port number is 22015. For SSL communication, the default port number is 22016.

The `user_httpsd.conf` file is stored in the following locations:

In Windows:

installation-destination-path-for-Hitachi-Command-Suite
`\Base64\uCPSB\httpsd\conf\user_httpsd.conf`

In Linux:

installation-destination-path-for-Hitachi-Command-Suite`/Base64/uCPSB/httpsd/conf/user_httpsd.conf`

- For non-SSL communication, specify the port number for the Listen line under `ServerName` in the `user_httpsd.conf` file.
- For SSL communication, specify the port number for the Listen line under `SSLDisable` in the `user_httpsd.conf` file.

For information about editing the `user_httpsd.conf` file, see the *Hitachi Command Suite Administrator Guide*.

The login window opens.

3. In the login window, click **Licenses**.
   If you are already logged in, from the **Help** menu, select **About**.
4. Register one or more licenses using one of these methods:
   - Enter the license key manually.
   - Specify the license key file (recommended).
5. Click **Save**.
   License Information by Product is updated with the license information for the associated product. If you registered the license after you logged in, you must log out and then log in again for the license to be enabled.

Logging in to Hitachi Command Suite to change the default password

When Hitachi Command Suite is installed for the first time, change the System account password for security. The System account is a built-in account that has all permissions for both operations and user management for Hitachi Command Suite products.

The initial password for the System account is `manager`.

Before you begin

- This task requires the IP address or host name of the management server that was specified during installation.
- Check your browser and Java settings. For more information about these settings, see the *Hitachi Command Suite User Guide*.

Procedure

1. Log in to HCS.
   - User ID: `system`
   - Password: `manager`

2. On the **Administration** tab, select **Users and Permissions**.
3. From the tree, select **Users**.
4. From the list of users, select the System account, and then click **Change Password**. Enter a new password.

Result

The new password can be used for log in.

Creating user accounts in Hitachi Command Suite

Create accounts for users and assign permissions (roles) to the new accounts, so users can perform tasks.

Note:

After you install a HCS product, you can add permissions (roles) for that product to existing user accounts.

Procedure

1. Log in to HCS using the System account.
2. On the **Administration** tab, click **Users and Permissions**.
3. In the tree view, click **Users** and then **Add User**.
4. Specify the required information, such as user ID and password.
5. On the **Administration** tab, click **User Groups**.
6. From the list of users in the **Users** tab, select a user account and click **Assign User Groups**.
7. Register the account into the group **AdminGroup**.

   AdminGroup is a built-in user group.
8. On the **Administration** tab, click **Users and Permissions**.
9. In the tree view, select the user account and click **Change Permission**.
10. From **All Applications**, select the **Admin**, **Modify**, **View**, and **Execute** check boxes.

    This grants operating permissions for managing users and using HCS products other than Device Manager.

Roles

The operations that a user can perform depend on the roles you assign to that user. You can also assign roles to each resource group.

Role	Capabilities
Admin	▪ Resource groups can be managed when `All Resources` is assigned. ▪ Management resources and tasks can be registered, management resource settings can be modified, and management resource information can be referenced.
Modify	Management resources and tasks can be registered, management resource settings can be modified, and management resource information can be referenced.
View	Management resource and task information can be referenced.
Custom	This role can be selected only when managing VSP 5000 series, VSP G series, VSP F series, or VSP N series. When Custom is selected, you can set roles by combining them to perform detailed operations for VSP 5000 series, VSP G series, VSP F series, or VSP N series.
Peer	Only for Device Manager agents and file server management software. Cannot be assigned to resource groups. This role does not allow a user to log in to HCS or view resource information.

For details about roles in Device Manager and Tiered Storage Manager, see the *Hitachi Command Suite User Guide*.

User permissions

You can assign permissions to HCS user accounts.

User management permissions

- Admin allows the user to manage users and security for all HCS products. This permission can be set in conjunction with assigned roles for each product.

Tiered Storage Manager CLI permissions

These permissions are required when using the Tiered Storage Manager CLI. In addition, All Resources must be assigned and roles must be set.

- Admin: Allows the user to view information about Tiered Storage Manager resources and tasks.
- Modify: Allows the user to perform any operation from Tiers on the Resources tab, and migrate volumes.
- Execute: Allows the user to view information about Tiered Storage Manager Software resources and execute Tiered Storage Manager tasks.
- View: Allows the user to view information about Tiered Storage Manager resources and tasks.

Replication Manager permissions

- Admin: Allows the user to perform any operation within a resource group, with the exception of user management.
- Modify: Allows the user to manage resources within a resource group, as well as resources that have been granted by a user with Admin permissions.
- View: Allows the user to view any resources within a resource group that have been granted by a user with Admin permissions.

For details, see the *Hitachi Command Suite User Guide*.

Built-in user groups

The following table describes the built-in user groups.

Table 28 Built-in user groups

Built-in user group name	Roles and Resource Groups
AdminGroup	The Admin role and All Resources group are assigned.
ModifyGroup	The Modify role and All Resources group are assigned.
ViewGroup	The View role and All Resources group are assigned.
PeerGroup	The Peer role and All Resources group are assigned.

Built-in user group name	Roles and Resource Groups
	This user group applies only to Device Manager agents and file server management software. Users that belong to this group and have no other HCS permissions are not allowed to log in to HCS, nor can they view resource information. The `HaUser` account is assigned to this group after installation completes.

For details about built-in user groups, see the *Hitachi Command Suite User Guide*.

Configuring secure communication settings after a new installation

For v8.1.3 or later, when Hitachi Command Suite is installed as a new installation, the default certificate for the Device Manager server is registered to the keystore, and the SSL/TLS communication is enabled.

The default certificate is a self-signed certificate that is used to encrypt communication when user account authentication is linked between Hitachi Command Suite and VSP G series, VSP F series, or VSP N series.

User account authentication needs to be linked:

- For VSP G1000 or VSP G1500, VSP F1500, if user accounts are authenticated by Hitachi Command Suite during log in to CCI and SVP.
- For VSP 5000 seriesVSP Gx00 models, VSP Fx00 models, or VSP Nx00 model when performing tasks on storage systems.

Use HiKeyTool to view certificate details, and then check if the security requirements are met. To enhance security by using a different self-signed certificate or a certificate that is already signed by certificate authorities, delete the default certificate for the Device Manager server, and then specify the SSL/TLS communication settings again.

To use secure communication between the Device Manager server and a component other than VSP G series, VSP F series, or VSP N series, delete the default certificate for the Device Manager server, and then specify the SSL/TLS communication settings again.

Note: If a KAIB10219-W or KAIB10220-W message was output while Hitachi Command Suite was installed, and SSL/TLS was not enabled, enable the SSL/TLS setting as necessary by using a self-signed certificate or a certificate that has already been signed by certificate authorities.

For more information about procedures and secure communication, see the chapter about security settings for communication in the *Hitachi Command Suite Administrator Guide*.

Preventing virus scanning of the HCS database folders

If a virus-detection program is running during HCS installation and scanning the database folders, the installation might be slow or fail.

Procedure

1. To prevent virus scanning of the database folders during HCS installation, register the following folders or directories in the virus scan program as exempt from the virus scan.
   - Windows:

     installation-destination-path-for-Hitachi-Command-Suite`\Base64\HDB`

     installation-destination-path-for-Hitachi-Command-Suite`\database`

   - Linux:

     installation-destination-path-for-Hitachi-Command-Suite`/Base64/HDB`

     `/var/`*installation-destination-path-for-Hitachi-Command-Suite*`/database`

Result

The registered folders or directories are not included in the virus scanning during installation.

Post-installation tasks (overwrite or upgrade)

After an HCS installation, you need to complete tasks for the installed products. The tasks vary and are dependent on which version of HCS you were using before upgrading. In the following table, tasks are listed that apply when upgrading any version of HCS. In addition, there are tasks listed that apply only when upgrading from a specific version.

Version before upgrade	Tasks to complete
Applies to all versions	▪ If you stopped virus-detection programs prior to the installation, restart the programs. ▪ Back up databases after upgrades. ▪ Refresh storage systems. ▪ If Device Manager manages virtualization servers, refresh the virtualization server information.

Version before upgrade	Tasks to complete
	▪ If Device Manager manages a NAS Platform (firmware version 10.2.3071 or later), refresh the file server information. ▪ If Replication Manager is using the Device Manager server on a secondary site to obtain information, synchronize databases. ▪ If you configured your environment to view volume performance, for example IOPS or response time, with Tuning Manager, link to Tuning Manager.
v8.4.1 or earlier, and when the following storage systems are managed: ▪ VSP Gx00 model and VSP Fx00 model storage systems whose microcode version is `83-04-XX-XX/XX` or later ▪ VSP G1000 storage systems whose microcode version is `80-05-XX-XX/XX` or later	▪ If your site is using the REST API and you are completing an upgrade, then register the destinations for sending notifications about changes that are made to storage system configurations.
v8.1.3 or later	▪ If you use secure communications and upgraded without previously having a Device Manager server certificate, review the secure communications settings.
v8.0.0 or later	▪ If using a version of Oracle Java Development Kit that is not supported in the upgraded HCS products, reset the JDK.
version earlier than 8.0.0	▪ If using Oracle Java Development Kit, reset the JDK.
v7.6.1 or earlier	▪ If you changed the port numbers, reset the port numbers. ▪ If you use scripts with written command names and file paths, and will use scripts in v8.0.0 or later, reset the scripts.

Version before upgrade	Tasks to complete
	▪ If using Oracle Java Development Kit, reset the JDK. ▪ If you use secure communications, review the secure communications settings.
v7.1.1 or earlier	▪ If Device Manager manages SMI-S enabled storage systems, re-register the SMI-S enabled storage systems.
v7.1.0 or earlier	▪ Reset roles and permissions. Existing user accounts are migrated according to the previous environment. ▪ (Optional) Specify Tiered Storage Manager event notifications.
Versions in the range from 7.0 to 7.5.0	▪ Verify logical group statuses.

Refreshing storage systems

To refresh the database, refresh all storage systems registered in HCS.

Procedure

1. Log in to HCS using the System account.
2. On the **Resources** tab, click **Storage Systems**.
3. From the list of storage systems, select the storage system you want to refresh.
4. Click **Refresh Storage Systems**.
   The database of storage systems is updated and the current information is reflected in the **Summary** and **Storage Systems** list.

Backing up databases

To prepare against failures, back up databases after completing the installation.

Note: Backing up the database involves operations that stop Hitachi Command Suite services. Do not attempt to access Hitachi Command Suite during the database back up.

Procedure

1. Log on to the management server as a user with administrator or root permissions.
2. Run the **`hcmds64backups`** command to back up the database.
   For Windows:

```
installation-destination-path-for-Hitachi-Command-Suite
\Base64\bin\hcmds64backups /dir folder-for-storing-backup-files /
auto
```

For Linux:

```
installation-destination-path-for-Hitachi-Command-Suite/
Base64/bin/hcmds64backups -dir directory-for-storing-backup-files
-auto
```

Note:

The `dir` option is used to specify the absolute path of the folder or directory on the local disk where the database backup files are stored. Verify that the folder or directory specified does not already include any files or subdirectories. (For Linux, do not specify a path that includes a space.)

The `auto` option automatically starts or stops Hitachi Command Suite services.

When **`hcmdsbackups`** completes, the backup directory is created in the directory specified by the `dir` option, and database files are combined and stored as `backup.hdb`.

Refreshing virtualization server information

Device Manager virtualization server information must be refreshed to reflect the current configuration.

In configurations where all the virtual servers are managed together by VMware vCenter Server, you can update information for all of the virtualization servers by updating the VMware vCenter Server information.

When managing the virtualization server VMware ESXi by using Device Manager, apply the latest virtualization server configuration to the database by using one of the following options:

- In the **Add Hosts** dialog box, re-register the virtualization server in Device Manager.
- On the Administration tab, click the Hosts tab, and then update the information for each virtualization server.
- On the Administration tab, click the vCenters tab, and then update the VWware vCenter Server information.

For more information about refreshing virtualization server information, see the *Hitachi Command Suite User Guide*.

Refreshing the registered information on the file server

If Device Manager manages a NAS Platform (firmware version: 10.2.3071 or later), the file server information must be refreshed.

To refresh registered information on the file server, perform synchronization from the SMU or from the NAS Platform. For details about how to synchronize, see the NAS Platform guides.

Roles and permissions after upgrades

When upgrading from 7.1.0 or earlier, user roles or permissions can change.

To verify user account status after upgrading, output the following CSV files:

- user information (you can verify the user group for each user account).
- user group information (you can verify the resource group or roles for each user group).

Managing accounts by users

When upgrading, user accounts change according to the version before the upgrade, the user permissions (roles), and the resource groups. The storage administrator must review user account settings for the new environment.

Managing accounts by groups

When linked to external authorization servers, nested groups acquire the permissions (roles) specified for the higher-level groups.

Because permissions (roles) of users who belong to nested groups can change after an upgrade, the storage administrator must review:

- Device Manager roles
- Tiered Storage Manager permissions
- Replication Manager permissions and user roles

The following table contains the necessary information for user account settings after an upgrade.

Table 29 Account settings after upgrading

From version	Before upgrading			After upgrading
	Device Manager permissions (roles)	Tiered Storage Manager permissions	Resource group	
6.x	Y	None	All Resources	Registered in built-in user groups according to Device Manager permissions. Operations can be restarted without performing any additional tasks.
6.x	Y	None	User defined resource groups	Resource groups and permissions are released, but only the accounts remain registered. To restart Device Manager operations, do the following: Register user accounts in user groups. Allocate resource groups to user groups. Set roles to resource groups.
6.x	Y	Y	All Resources	User accounts are registered in built-in user groups according to Device Manager permissions.

From version	Before upgrading			After upgrading
	Device Manager permissions (roles)	Tiered Storage Manager permissions	Resource group	
				Depending on the user responsibilities, ask the storage administrator to review the allocation of user groups and resource groups to which the user belongs.*
6.x	Y	Y	User defined resource groups	Resource groups and permissions are released, and only the accounts remain registered. To restart Device Manager and Tiered Storage Manager operations, verify the following from the GUI*: User accounts must be registered to user groups. Resource groups must be allocated to user groups. Roles must be set to resource groups.
6.x	None	Y	None	Only the accounts remain registered. To restart Tiered Storage Manager operations, verify the following from the GUI*: User accounts must be registered to user groups.

From version	Before upgrading			After upgrading
	Device Manager permissions (roles)	Tiered Storage Manager permissions	Resource group	
				Resource groups must be allocated to user groups. Roles must be set to resource groups.
7.0.0 - 7.0.1	Y	None	All Resources	Registered in built-in user groups according to Device Manager permissions. Operations can be restarted without performing any additional tasks.
7.0.0 - 7.0.1	Y	Y	All Resources	Registered in built-in user groups according to Device Manager permissions. Depending on the user responsibilities, ask the storage administrator to review the allocation of user groups and resource groups to which the user belongs.*
7.1.0	Y	None	All Resources	User groups, resource groups, and roles are inherited. Operations can be restarted without performing any additional tasks.

From version	Before upgrading			After upgrading
	Device Manager permissions (roles)	**Tiered Storage Manager permissions**	**Resource group**	
7.1.0	Y	None	User defined resource groups	User groups, resource groups, and roles are inherited. Operations can be restarted without performing any additional tasks.
7.1.0	Y	Y	All Resources	User groups, resource groups, and roles are inherited. Depending on the user responsibilities, ask the storage administrator to review the allocation of user groups and resource groups to which the user belongs.*
Legend: * : When using the Tiered Storage Manager CLI, allocate All Resources to the user group.				

For more information, see the *Hitachi Command Suite User Guide*.

Logical group statuses after upgrades

When the version before the upgrade is a version from 7.0 to 7.5.0, upgrading the version migrates the existing logical groups to public logical groups. Top folders are created for each user group in the private logical groups.

The top folders that are created in the private logical groups differ according to the user group to which a user belongs.

- When a user belongs to a built-in user group, for example AdminGroup, ModifyGroup, ViewGroup, or PeerGroup, a folder with the same name as the built-in user group is created.
- When the user belongs to a user group other than a built-in user group, a folder with the same name as the user group is created.

Migrate logical groups from the public logical groups to private logical groups, as required.

When a user is using the System account, a top folder named `System` is created in the private logical groups. A system account user cannot reference or edit private logical groups other than the `System` folder. If the user wants to manage private logical groups other than the `System` folder, create another user account and have that account belong to the relevant user group.

For details about public logical groups and private logical groups, see the *Hitachi Command Suite User Guide*.

Configuring event notifications

You can configure event notifications in Tiered Storage Manager after upgrading from v7.1.0 or earlier.

For more information, see the *Hitachi Command Suite Administrator Guide*.

Procedure

1. In the `server.properties` file for Device Manager, set the following:
   - `server.mail.enabled`
   - `server.mail.smtp.host`
   - `server.mail.from`
   - `server.mail.errorsTo`
   - `server.mail.smtp.port`
   - `server.mail.smtp.auth`
   - `server.eventNotification.mail.to`
2. Register SMTP authenticated users to Device Manager.
3. (Optional) Customize the email template.
4. Restart the Hitachi Command Suite product services.

Synchronizing Replication and Device Manager databases

After performing an overwrite installation or upgrade, you must synchronize the Replication and Device Manager databases.

Procedure

1. If Replication Manager Application Agent v7.1 or later is installed on the management server, set the value of the `base.refreshdginfo.exec` property in the Replication Manager `base.properties` file to `0`.

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

   - In Windows:

     `installation-destination-path-for-Hitachi-Command-Suite``\ReplicationManager\conf`

   - In Linux:

     `installation-destination-path-for-Hitachi-Command-Suite/``ReplicationManager/conf`

2. Restart the Hitachi Command Suite product services.
3. Log in to Device Manager using the System account.
4. On the **Actions** menu, select **Manage Replication**.
5. In the Explorer menu, select **Settings** and then select **Refresh Setting**.
6. In the tree view, select **Configuration Setting**.
7. Select the instances to synchronize and click **Refresh Configuration**.

   When upgrading the Replication Manager server at primary sites, do this for Device Manager on secondary sites.

   When upgrading the Device Manager server at secondary sites, do this for Device Manager on the upgrade sites.

Importing report definition files for Tuning Manager

If you are using Performance Reporter in Tuning Manager to view volume performance, verify you have the latest report definition file for the **Analytics** tab. If the file is out of date, you must import the latest report definition file.

Before you begin

Check the latest report definition file (`AnalyticsReportDefV840`) that is stored on the integrated installation media:

`DVD-drive``:\HTNM_SERVER\Definitions\Report_Definitions`

Compare this to the version displayed in the **Performance Reporter Reports** window.

Procedure

1. In the **Performance Reporter Reports** window, delete the previous report definition.
2. Import the latest report definition file from the installation media.

Updating the properties file for Tuning Manager

Update the report definition and properties files if you set up your environment to view volume performance, such as IOPS or response time, with Tuning Manager.

If you upgraded from v7.1.1, update the `config.xml` properties file.

Procedure

1. Change the value of the `logFileSize` parameter in the `config.xml` file to 8 or more.

   In Windows:

   `installation-destination-path-for-Hitachi-Command-Suite``\DeviceManager\HiCommandServer\vsa\conf`

   In Linux:

   `installation-destination-path-for-Hitachi-Command-Suite/``HiCommandServer/vsa/conf`

2. Restart the Hitachi Command Suite product services.

Resetting the Java Development Kit

When using Oracle Java Development Kit (JDK) and upgrading Hitachi Command Suite products, reset the JDK if either of the following conditions apply:

- If you upgraded Hitachi Command Suite from a version earlier than 8.0.0.
- If you upgraded Hitachi Command Suite from version 8.0.0 or later and you are using a version of Oracle JDK that is not supported in the upgraded Hitachi Command Suite products.

Before you begin

Verify that the server meets the minimum requirements and that prerequisite software is installed.

For more information, see *Hitachi Command Suite System Requirements*.

Procedure

1. Install a version of Oracle JDK that is supported in the Hitachi Command Suite products.
2. Register the JDK that you want to use in the Hitachi Command Suite products.

   For more information about registering the JDK, see the *Hitachi Command Suite Administrator Guide*.

Resetting port numbers

When upgrading from v7.6.1 or earlier, some port numbers are reset to the default. If the port numbers were changed using an earlier version, reset the port numbers after the upgrade installation.

Before you begin

Check the following port numbers to determine if they need to be reset:

- Port numbers used to access HBase 64 Storage Mgmt Web Service.
- Port number for the Start menu URL.
- Port numbers used for remote connections with the Tuning Manager server.

For information about changing port numbers, see the *Hitachi Command Suite Administrator Guide*.

Configuring secure communication settings after an upgrade

Depending on the version used before upgrading Hitachi Command Suite, the secure communication settings change after the upgrade.

When upgrading from v7.6.1 or earlier, the secure communication settings are canceled. You need to reconfigure the secure communications settings for Hitachi Command Suite products.

When upgrading to v8.1.3 or later, the communication is encrypted when user account authentication is linked between Hitachi Command Suite and VSP G series or VSP F series. If a Device Manager server certificate does not exist, the default certificate for the Device Manager server is registered to the keystore, and the SSL/TLS communication is enabled. When the SSL/TLS communication is enabled, port number 2443 is used. If you are using Linux, you need to register firewall exceptions. Verify if port number 2443 is registered in the firewall exception list.

For more information about secure communication and how to register firewall exceptions, see the *Hitachi Command Suite Administrator Guide*.

Resetting scripts

When upgrading from v7.6.1 or earlier, command names and file paths are changed.

If you use scripts with written command names and file paths, and will use scripts in v8.0.0 or later, review the command names and file paths that are written in these scripts.

Registering destinations for sending notifications about storage system configuration changes

When using the REST API with certain conditions, the destinations for sending notifications about changes made to storage system configurations need to be registered.

When using the REST API and both of the following conditions are met, register the destinations for sending notifications about changes that are made to storage system configurations:

- An upgrade installation from version 8.4.1 or earlier was performed.
- One of the following storage systems is being managed:
  - A VSP Gx00 model and VSP Fx00 model storage system whose microcode version is `83-04-XX-XX/XX` or later.
  - A VSP G1000 storage system whose microcode version is `80-05-XX-XX/XX` or later.

For details about registering destinations for sending notifications about changes made to storage system configurations, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

Workflow for upgrading the OS on the management server

When upgrading the operating system on the management server where Hitachi Command Suite is installed, you need to remove Hitachi Command Suite.

This process applies to the following:

- All operating systems
- When you upgrade to either a minor or major version. For example, if you upgrade from Windows Server 2012 to Windows Server 2012 R2, you need to remove Hitachi Command Suite.

1. Remove Hitachi Command Suite.
2. After upgrading the operating system, install a Hitachi Command Suite version that supports the upgraded operating system.
3. Migrate the Hitachi Command Suite database.

For more information about migrating the database, see the *Hitachi Command Suite Administrator Guide.*

Chapter 3: Host Data Collector installation

This module describes how to install and set up Host Data Collector on different hosts.

About installing Host Data Collector

When the storage administrator installs Host Data Collector on hosts and registers the hosts on the management server, information about volumes being used by the hosts can be collected.

The instructions for installing Host Data Collector vary depending on your operating system.

Required values for installing Host Data Collector

Best practice is to use the default values during installation of Host Data Collector, such as installation path and port number.

The following table lists values required for Host Data Collector installation.

Value	Condition	Requirements

Installation path	The default path to the folder in which Host Data Collector will be installed.	Windows:
		`%ProgramFiles%Hitachi`
		Linux:
		`/opt/Hitachi`

	If you change the default installation folder, verify that the installation location satisfies the following conditions:	
	Absolute path length	Maximum 64 bytes
	Allowed characters	Windows: A to Z, a to z, 0 to 9, periods (.), underscores (_), left parentheses (( ), right parentheses ( )), single-byte spaces, backslashes (\), and colons (:) Linux:

Value	Condition	Requirements
		A to Z, a to z, 0 to 9, underscores (_), and forward slashes (/)
	Other conditions	Windows: ▪ Do not include consecutive spaces. ▪ Do not include a single byte space at the beginning or end of a folder name. ▪ Do not specify the root of a drive as the installation destination.
Port number	Port number for RMI registry	Specify the non-SSL communication port number of the RMI registry (default: 22098/tcp).
	Port number for RMI server	Specify the non-SSL communication port number of the RMI server (default: 22099/tcp).
	Port number for class loader	Specify the non-SSL communication port number of the class loader (default: 22100/tcp).

Installing Host Data Collector (Windows)

Install Host Data Collector by using the installation media.

Before you begin

- Verify that the server meets the minimum requirements and that prerequisite software is installed. For more information, see *Hitachi Command Suite System Requirements*.
- Verify the versions of the Host Data Collector and Hitachi Command Suite products on the management server:
  - To use Host Data Collector for Device Manager to manage hosts, the version of Host Data Collector must be the same or later than the version of the Device Manager server installed on the management server. For example, if the version of Host Data Collector is 7.5.0 or later, the version of the Device Manager server must be 7.5.0 or later.
- To use Host Data Collector on multiple computers, the same version of Host Data Collector must be installed on all the computers.

Tip: To check the version of Host Data Collector, use the following command: *`installation-destination-path-for-Host-Data-Collector`*`\HDC\Base\bin\hdc_info.exe`.

- Log in with administrator permissions.
- Stop virus-detection programs. If a virus-detection program is running during installation, the installation might be slow, fail, or finish incorrectly.
- Determine the installation path for a new installation.
- This task requires the port number used by Host Data Collector for a new installation.

For information about starting and stopping services, see the *Hitachi Command Suite Administrator Guide*. For information about downloading components, see the *Hitachi Command Suite User Guide*.

Procedure

1. Insert the installation media.
2. In the installation window, select **HDC** in the **Agent Products** tree, and then click **Install**.

   If the window does not automatically open, start the installer `setup.exe` directly. The installer is in the following location:

   DVD-drive`\AGENTS\HHDC\Windows`
3. Specify the necessary information on the installation wizard pages.
   When installation is complete, the **Install Complete** window appears and the Host Data Collector service is registered in the operating system.

   Caution: If you install Host Data Collector in a folder other than the default installation folder, specify a folder protected by Administrator permissions.

   Tip:
   - You can also download the Host Data Collector installer from the Device Manager GUI.
   - If v7.4.1 or earlier of Host Data Collector is installed on a drive other than the system drive, if you upgrade the installation to v7.5.0 or later, a `temp` folder is created in the `root` folder of the drive where Host Data Collector is installed. If you do not need the `temp` folder, delete it.
   - If you upgrade an installation, restart the services of the Hitachi Command Suite products on the management server.

Installing Host Data Collector (Linux)

Install Host Data Collector by using the installation media.

Before you begin

- Verify that the server meets the minimum requirements and that prerequisite software is installed. For more information, see *Hitachi Command Suite System Requirements*.
- Verify the versions of the Host Data Collector and Hitachi Command Suite products on the management server:
  - To use Host Data Collector for Device Manager to manage hosts, the version of Host Data Collector must be the same or later than the version of the Device Manager server installed on the management server. For example, if the version of Host Data Collector is 7.5.0 or later, the version of the Device Manager server must be 7.5.0 or later.
- To use Host Data Collector on multiple computers, the same version of Host Data Collector must be installed on all the computers.

  Tip: To check the version of Host Data Collector, use the following command: *`installation-destination-path-for-Host-Data-Collector`*`\HDC\Base\bin\hdc_info.sh`.
- Log in as the root user.
- Stop virus-detection programs. If a virus-detection program is running during installation, the installation might be slow, fail, or finish incorrectly.
- Determine the installation path for a new installation.
- This task requires the port number used by Host Data Collector for a new installation.

For information about starting and stopping services, see the *Hitachi Command Suite Administrator Guide*. For information about downloading components, see the *Hitachi Command Suite User Guide*.

Procedure

1. Insert the installation media.

   If the media is not mounted automatically, manually mount it on the `/mnt/dvdrom` directory.
2. Locate the installer (`setup.sh`) in the following location:

   `DVD-drive``/AGENTS/HHDC/`*`platform-name/`*
3. Run the following command:

   ```
   # ./setup.sh
   ```
4. Follow the instructions in the displayed prompts.
   When installation is complete, the following message appears:

```
Host Data Collector installation completed successfully.
```

Tip:

- You can also download the Host Data Collector installer from the Device Manager GUI.
- If you upgrade an installation, restart the services of the Hitachi Command Suite product on the management server.

Post-installation tasks for Host Data Collector

After installing Host Data Collector, you must specify settings for your operating environment.

- Register Host Data Collector computer information to the management server.

  If Host Data Collector is installed on a computer other than the management server, add the information for that computer to the properties in the `hostdatacollectors.properties` file on the Device Manager server.

  When Host Data Collector computer information is registered on the management server, you can register hosts and check the volume usage for each host.
- Reset the execution environment for Java. This task is required when the person using Oracle JDK installs an upgrade for Host Data Collector.
- Reset secure communication (Windows).

  Required when upgrading from v7.6.1 or earlier and using SSL communication between the Device Manager server and Host Data Collector.
- Update host information

  When Host Data Collector is upgraded to v8.0.1 or later and an IPv6 address is configured on a host that was registered by using Host Data Collector prior to the upgrade, update the host information if needed.

  Host Data Collector acquires the host IPv6 addresses in the priority order of (1) global address, (2) link local address, and (3) site local address. The scope ID, which is the string of characters starting with a percent sign (%), is omitted from the displayed IPv6 addresses.
- Change the settings of the antivirus software

  To use antivirus software with Host Data Collector, you need to exclude the installation directory of Host Data Collector from scans that are performed by the antivirus software.

Registering a Host Data Collector computer on the management server

Register information about the computer on which Host Data Collector is installed in the properties of the `hdcbase.properties` file on the Device Manager server.

Before you begin

- Log in with administrator permissions (Windows) or as the root user (Linux).
- Install Hitachi Command Suite on the management server.
- Install Host Data Collector on a host.
- If the operating system of the Host Data Collector computer is Linux, set up name resolution (setting up the DNS server or hosts file) for the Host Data Collector computer.
- Collect the following information for the computer where Host Data Collector is installed:
  - IP address or host name.
  - Port number of the RMI registry.

    You can get this value from the `hdc.common.rmi.registryPort` or `hdc.common.rmi.ssl.registryPort` property in the `hdcbase.properties` file.
  - Port number of the RMI server.

    You can get this value from the `hdc.common.rmi.serverPort` or `hdc.common.rmi.ssl.serverPort` property in the `hdcbase.properties` file.
  - Port number of the class loader.

    You can get this value from the `hdc.common.http.serverPort` or `hdc.common.http.serverPort` property in the `hdcbase.properties` file.

For information about starting and stopping services, network configuration, or Host Data Collector properties, see the *Hitachi Command Suite Administrator Guide*.

Procedure

1. Stop Hitachi Command Suite services.
2. Add the information about the computer where Host Data Collector is installed to the following properties in the `hostdatacollectors.properties` file on the Device Manager server:
   - `hdc.rmiregistry`
   - `hdc.rmiserver`
   - `hdc.classloader`
3. Start Hitachi Command Suite services.

Resetting the Java execution environment for Host Data Collector

When upgrading Host Data Collector and using Oracle Java Development Kit (JDK), the system defaults to the Java execution environment that was used before the upgrade. If you are using a version of Oracle JDK that is not supported in the upgraded Host Data Collector, you need to reset the Java execution environment.

Also, when upgrading Host Data Collector from v7.6.1 or earlier in a Windows environment, the system defaults to the Java execution environment included with Host Data Collector. If you are using Oracle JDK, you need to reset the Java execution environment.

For information about starting and stopping services, and Host Data Collector properties, see the *Hitachi Command Suite Administrator Guide*.

Before you begin

- Check the Java execution environment prerequisite for Host Data Collector. For more information, see the *Hitachi Command Suite System Requirements*.
- Log in with administrator permissions.

Procedure

1. Stop the Host Data Collector service.
2. Use the absolute path to configure the installation path of the Java execution environment to the `javapathlocation` property in the `javaconfig.properties` file for Host Data Collector.
3. Start the Host Data Collector service.

Result

The Java execution environment used by Host Data Collector is changed to the Java execution environment in the `bin` folder in the specified path.

Resetting secure communication (Windows)

When upgrading from v7.6.1 or earlier and using SSL communication between Host Data Collector and the Device Manager server, you must reset secure communication.

For information about secure communication between Host Data Collector and the Device Manager server, see the *Hitachi Command Suite Administrator Guide*.

Preventing virus scanning of the Host Data Collector installation folders

If antivirus software accesses files that Host Data Collector uses, failures caused by delays in I/O or file exclusions might occur.

Procedure

1. To prevent failures, exclude the following directory from scans performed by antivirus software while Host Data Collector is operating: *`installation-destination-of-Host-Data-Collector`*

Workflow for upgrading the OS on the Host Data Collector host

When upgrading the operating system on the management server or host where Host Data Collector is installed, you need to remove Host Data Collector.

This process applies to the following:

- All operating systems
- When you upgrade to either a minor or major version. For example, if you upgrade from Windows Server 2012 to Windows Server 2012 R2, you need to remove Host Data Collector.

1. Remove Host Data Collector.
2. After upgrading the operating system, install a Host Data Collector version that supports the upgraded operating system.

Chapter 4: Device Manager agent installation

This module describes how to install and set up Device Manager agent.

Planning for Device Manager agent installation

Before you install the Device Manager agent, verify the prerequisites and gather the information you need to perform the installation.

Prerequisites for agent installation

Before a new installation, gather the appropriate information for the installation wizard, including the installation folder.

Note:

When updating a system or performing a recovery, the Device Manager server information and **`HiScan`** command execution periods are imported.

For Windows:

- Installation folder. Default: *`program-files-folder`*`\HITACHI\HDVM\HBaseAgent`

  `program-files-folder` indicates the following location:

  - For Windows (x86): The folder specified in the Windows system environment variable `%ProgramFiles%`.
  - For Windows (x64 or IPF): The folder specified in the Windows system environment variable `%ProgramFiles(x86)%`.

  You can change the agent installation folder location on Windows as long as the following software is not installed:

  - Dynamic Link Manager
  - Replication Manager application agent
  - Tuning Manager Agent for SAN switch
  - Global Link Manager Agent
- Whether to set up agent services account information. To set up account information for agent services, you must specify a Windows account with Administrator permissions (default is Yes).

For Solaris, AIX, or HP-UX:

- The UNIX installation folder cannot be changed.

For Linux:

- Installation folder. Default: `/opt/HDVM/HBaseAgent`

You can change the agent installation folder location on Linux as long as the following software is not installed:

- Dynamic Link Manager
- Tuning Manager Agent for SAN switch

For Windows, UNIX, and Linux :

- Device Manager server IP address or host name. Default: `255.255.255.255`
- SSL communications settings.
  - Directory to store the Device Manager server certificate: Setting `None`
  - All certificate files in the specified directory will be imported but subdirectories will not be imported.
  - If SSL communication is used between the Device Manager server and Device Manager agent, do not use the default Device Manager server certificate. Before installing Device Manager agent, create a Device Manager server certificate on the management server and then import the created server certificate to the truststore.
- Device Manager port.
  - Default for non-SSL communications: `2001/tcp`
  - Default for SSL communications: `2443/tcp`
- User ID (user account that belongs to `PeerGroup`): `HaUser`

  Password: `haset`
- **`HiScan`** command execution schedule. Default: Daily at 2:30 AM.

For CCI:

- Installation location.
  - Default on Windows: Device Manager agent installation drive.
  - Default on UNIX: `/HORCM`
- By default, copy pairs are not batch managed by the agent host. Default: `disable`.

Note:

The host name of the machine where the Device Manager agent is installed must be no longer than 50 bytes.

Prerequisites for agent installations with add-ons

If you use Replication Manager on Windows to monitor or perform copy pair operations, you can use an add-on function to install and configure the Device Manager agent.

When using either of the following configurations, you can use the add-on function to install and configure the Device Manager agent with suitable settings:

- Configurations in which SVPs are used for virtual command devices to manage copy pairs
- Configurations in which copy pairs are defined as device groups

The following items are automatically set when using the add-on function:

- Installation destination: Automatically set by the installer.
- Agent service accounts: By default, agent service accounts are set up on your local system. You do not need to change this setting.
- Device Manager server:
  - IP address or host name: `localhost`
  - Default Device Manager server port: `2001/tcp`

    Note:

    If the port set for the `server.http.port` property in the Device Manager server `server.properties` file is different from the default port setting, after the installation, use the **`hdvmagt_setting`** command to change the Device Manager agent setting.

  - User ID (user account that belongs to `PeerGroup`): `HaUser`
  - Password: `haset`
  - **`HiScan`** command schedule: Do not set.
- CCI:
  - The Windows default installation folder: CCI installation drive
  - Enable batch management of copy pairs on the host on which the Device Manager agent is installed. Default: `enable`

For more information, see the *Hitachi Command Suite Administrator Guide*.

Note:

- The host name of the machine where the Device Manager agent is installed must be no longer than 50 bytes.
- The add-on function cannot automatically set the configuration information for SSL communication.

Prerequisites for agent installation locations

Before specifying an installation folder for the Device Manager agent, verify that the required disk space is available.

When creating the installation location for the Device Manager agent, adhere to the naming conventions in the following table.

Table 30 Agent installation folder naming requirements

Condition		Requirements
Maximum length		64 characters
Windows	Allowed characters	A to Z, a to z, 0 to 9, periods (.), underscores (_), left parentheses (( ), right parentheses ( )), and single-byte spaces
	Other conditions	▪ Do not use a space as the first or last character of the installation folder name. ▪ Do not include multi-byte characters in the file name or path. ▪ Do not include consecutive spaces in the file name or path.
Linux	Allowed characters	A to Z, a to z, 0 to 9, underscores (_), and forward slash (/)
	Other conditions	▪ Specify an absolute path. ▪ Specify a path other than the path for the `root` directory. ▪ The directory *specified path*`/HBase/Agent` must be empty or nonexistent. ▪ Do not specify the path of a symbolic link.

Modifying agent services

A user account that is registered in a Device Manager agent service (HBsA Service) and is part of the Administrators group can be used to edit horcm instances run by the Device Manager agent.

To modify horcm instances run by Device Manager agents, specify users in the Windows Administrators group. To use domain user accounts, specify domain users as *`domain-name\user-name`*.

Prerequisites for verifying server information

Before installing a Device Manager agent, determine information about the Device Manager server (where the host information is sent).

- The server IP address or host name. IPv6 addresses can be specified using global addresses.

  Server host name maximum length: 50 bytes.

  Server host name allowed characters: A through Z, a through z, 0 through 9, hyphens (-), underscores (_), periods (.), and at signs (@)

  Other server host name conditions: Do not use a hyphen as the first or last character.

- The server port number. This is used by the agent and the server.

- User ID and password. This is the user account for logging in to the Device Manager server. The user account must belong to `PeerGroup`.

- SSL communication settings. For SSL communication, use the following guidelines when specifying the directory to store the Device Manager server certificate and the password to access the Device Manager agent truststore.

  Absolute path maximum length: 64 bytes

  Allowed characters (Windows): A through Z, a through z, 0 through 9, underscores (_), periods (.), opening parenthesis (( ), closing parenthesis ( )), and a single space.

  Allowed characters (Unix): A through Z, a through z, 0 through 9, underscores (_), and forward slash (/).

  Default password for the Device Manager agent truststore is `changeit`. The password is case-sensitive.

  Using the installation wizard, import the Device Manager server certificate to the Device Manager agent truststore.

  The settings for the Device Manager agent property file are:

  - `server.server.ssl.hdvm: True`
  - `server.server.serverPort: `*`Port-number-for-SSL-communication`*

About HiScan command execution

The **`HiScan`** command configures Device Manager agents to send information to the server on a regular basis. You can schedule **`HiScan`** for hourly, daily, or weekly execution.

Note:

If you specify weekly executions, also specify the day of the week you want the scan to run.

If no **`HiScan`** execution periods are set, agents do not regularly send acquired information to the server.

To reduce HCS server loads when agents are installed on multiple hosts, specify daily or weekly executions and verify that multiple instances of **`HiScan`** do not run simultaneously.

For Windows, the batch file `exeHiScan.bat` with the **`HiScan`** settings is registered as a Windows task.

Prerequisites for identifying CCI

When Device Manager is linked to CCI and used to manage copy pairs, you must determine some information.

- The location of the CCI installation folder:
  - In Windows, the installation drive.
  - In UNIX, the installation directory.
- The method used for managing copy pairs:
  - Batch managed on a Device Manager agent host.
  - Managed for each host on which the Device Manager agent is installed.

Agent installation prerequisites

Before installing the Device Manager agent, review the general prerequisites. Check the host settings and the status of each affected program to confirm that the host system is in the appropriate state.

For more information about system requirements, see the *Hitachi Command Suite System Requirements*.

Host prerequisites

Before installing the Device Manager agent, perform prerequisite tasks as appropriate.

- The Device Manager agent does not support operating systems that allow only IPv6 addresses. To use the agent in an IPv6 operating system, configure it to allow both IPv4 and IPv6 addresses.
- Stop all programs.
- When setting up a firewall provided by an operating system, configure it so socket connections cannot be terminated in the local host.
- If you are running security monitoring or backup software, either temporarily stop them or change the settings so they do not prevent the installation.
- Device Manager agent v5.7.0 and later are compatible with the Daylight Saving Time (DST) rules implemented in the United States and Canada in 2007. When using the Device Manager agent in these time zones, set the host operating system for the new DST rules according to information provided by the operating system vendor.

- When installing or upgrading Device Manager agent, do not run these commands:
  - **hbsasrv**
  - **hdvmagt_setting**
  - **HiScan**
  - **hldutil**
  - **TIC**

  If you run these one of these commands by mistake, restart your system when the installation or upgrade completes.
- Do not perform an overwrite installation of Device Manager agent using a version that is earlier than the one currently installed. To install an earlier version, first remove the Device Manager agent that is currently installed.
- Do not install Replication Monitor agent v5.9.0 or earlier if Device Manager agent v6.0.0 or later is already installed.

  Note: Replication Monitor agent is integrated with Device Manager agent v6.0.0 and later. If you update Device Manager agent to v6.0.0 or later on a system with Replication Monitor v5.9.0 or earlier installed, Replication Monitor agent is automatically removed.

  Replication Monitor program information is no longer displayed in the Windows Add or Remove Programs dialog box.

Host prerequisites for Windows

If these conditions are not satisfied, Device Manager agent installation may fail or the Device Manager agent may not work properly.

Before installing Device Manager agents, perform the following task:

- If the Windows logon account contains multi-byte characters, agents cannot be installed. Specify a folder that does not include multi-byte characters for the `TMP` environment variable.

HCS products for Windows support the Windows remote desktop functionality.

Note:

The Microsoft terms for this functionality differ depending on the Windows operating system. These terms can refer to the same functionality:

- Terminal Services in the Remote Administration mode
- Remote Desktop for Administration
- Remote Desktop Connection

Keep the following in mind when working with Windows remote desktop:

- When using the remote desktop, connect to the console session of the target server in advance and ensure that no one else connects to your session.
- When logging on to Windows from a remote console, use the Terminal Service Client.

Host prerequisites for Solaris

Do not install Device Manager agents on Solaris environments when symbolic links exist for the following directories:

- `/opt`
- `/opt/HDVM` and its subdirectories
- `/var`
- `/var/opt`
- `/var/opt/HBaseAgent` and its subdirectories
- `/var/opt/HDVM` and its subdirectories
- `/var/tmp`

When installing the Device Manager agent in Solaris 10 or 11, do not specify system zone settings.

Removing agents when using Solaris 10

If the Device Manager agent v4.1 through v5.1 was upgraded to v5.5 or later in an environment with the non-global zone specified, it is installed in the global and non-global zones. Because the agent is not required for the non-global zone, you can remove it.

Procedure

1. Log in to the non-global zone.
2. Run the **`# pkgrm HDVMAgent`** command.

Host prerequisites for AIX

Do not install Device Manager agents in AIX environments when symbolic links exist for the following directories:

- `/usr`
- `/usr/HDVM` and its subdirectories
- `/var/HDVM` and its subdirectories
- `/var`
- `/var/HBaseAgent` and its subdirectories
- `/var/tmp`

When IBM XL C/C++ Enterprise Edition V8 for AIX Runtime v8.0.0.3 through v8.0.0.5 is applied, the overwrite installation of the Device Manager agent hangs if either:

- The Hitachi Dynamic Link Manager version that is installed is from 5.8.0 or later, to a version that is earlier than 5.9.0.
- The Device Manager agent version that is installed is 5.0.0 through 5.1.03.

When you use the Device Manager agent, upgrade IBM XL C/C++ Enterprise Edition V8 for AIX Runtime to v8.0.0.6 or later, or apply the APAR IY87291 patch.

Before you install the Device Manager agent in AIX, verify the IBM XL C/C++ Enterprise Edition V8 for AIX Runtime version by running # **`lslpp -L xlC.aix50.rte`**

- AIX includes the Stack Execution Disable (SED) function that protects systems from attacks that use a buffer overflow. If the SED mode is set to **`all`**, change the mode before installing the Device Manager agent by running **`# sedmgr -m {select|off|setidfiles}`**

Note:

To return the SED mode to **`all`** after installing the Device Manager agent, exclude the Java process used by the Device Manager agent from the SED protection targets. For details, see the *Hitachi Command Suite Administrator Guide*.

Removing HDSHiScan packages when using AIX

Remove the HDSHiScan package before installing the Device Manager agent. Hitachi recommends that you remove any agent not being used.

Caution:

HDSHiScan is the name used for versions earlier than 2.2.0. HDVMAgent is the name used for v2.2.0 and later. The HDSHiScan package is installed in the `/usr/HDVM` directory.

Procedure

1. At the prompt, confirm whether a HiScan package is installed by running:
   - **`% su`**
   - **`% lslpp -l HDSHiScan.rte`**
2. If the HDSHiScan package is installed, confirm the execution period of the **`HiScan`** command before removing by running:
   - **`% su`**
   - **`# crontab -l`**
3. To remove HiScan packages, run the following commands.

Device Manager agent v2.4.0 or earlier:

- **`% su`**
- **`% installp -u HDSHiScan.rte`**

Device Manager agent v3.0.0 or later:

`% /usr/HDVM/bin.uninstall.sh`

Host prerequisites for Linux

Do not create a symbolic link for any directories or subdirectories in the *installation-destination-path-for-Device-Manager-agent*.

- `/var`
- `/var/opt`
- `/var/opt/HBaseAgent` and its subdirectories
- `/var/opt/HDVM` and its subdirectories
- `/var/tmp`

If the Device Manager agent installation directory is `/opt/HDVM/Agent`, the following directories are included:

- `/opt`
- `/opt/HDVM`
- `/opt/HDVM/Agent` and its subdirectories

Allowing communication with Linux firewalls

If you are installing on a Linux system that has a firewall, the firewall may prevent communication between the Device Manager agent and the Device Manager server. To open the communication, you can do one of the following:

- Open the port used by Device Manager.
- Prevent the services related to the firewall from automatically running during the Linux startup process.

Procedure

1. Log in to Linux as a root user.
2. Run the **`iptables`** command to open the port used by Device Manager, or skip to step 3.

3. Depending on the version of Linux that you are using, run one of the following commands on the Linux host to prevent services related to the firewall from automatically running during the Linux startup process.
   - If you are using Red Hat Enterprise Linux 5 or Red Hat Enterprise Linux 6:

     Run the **`chkconfig iptables off`** command.
   - If you are using Red Hat Enterprise Linux 7 or Oracle Linux 7:

     Run the **`systemctl disable firewalld.service`** command.
   - If you are using the SUSE Linux Enterprise Server:

     Run the **`YaST`** command.

     Then from the **System Services (Runlevel)** window, disable the following two items:

     `SuSEfirewall_init`

     `SuSEfirewall_setup`

Result

Communication is allowed between the Device Manager agent and the Device Manager server.

Host prerequisites for HP-UX

When installing the Device Manager agent in an HP-UX environment, you must consider the following:

- Verify that the **`swagentd`** daemon is running.

  If necessary, start the daemon process by executing:

  `/usr/sbin/swagentd`
- Verify that the file system mounted on the host matches the one defined in

  `/etc/fstab`.
- Verify that the network settings (such as those in the `hosts` file) are correct.

Note:

Do not try to install the Device Manager agent on an HP-UX workstation. If you do, the installation fails and the following message appears:

```
ERROR: Could not apply the software selection "HDVMAgent"
because there are no product variations that are compatible
with the destination host(s).
```

- Do not create a symbolic link for any of the directories below. If you have already created a symbolic link by using any of the directories below, do not install the Device Manager agent.
  - `/opt`
  - `/opt/HDVM` and its subdirectories
  - `/var`
  - `/var/opt`
  - `/var/opt/HBaseAgent` and its subdirectories
  - `/var/opt/HDVM` and its subdirectories
  - `/var/tmp`

Removing HDSHiScan packages when using HP-UX

Remove the HDSHiScan package before installing the Device Manager agent. Hitachi recommends that you remove any agent not being used.

Caution:

HDSHiScan is the name used for versions earlier than 2.2.0. HDVMAgent is the name used for v2.2.0 and later. The HDSHiScan package is installed in the `/opt/HDVM` directory.

Procedure

1. At the prompt, confirm whether a HiScan package is installed by running:
   - **`% su`**
   - **`# swlist HDSHiScan`**
2. If the HDSHiScan package is installed, confirm the execution period of the **`HiScan`** command before removing by running:
   - **`% su`**
   - **`# crontab -l`**

3. To remove HiScan packages, run the following commands.
   - `% su`
   - `# swremove HDSHiScan`

Installing Device Manager agent

Before you install the Device Manager agent, review the information about planning for the installation. Follow the instructions for installing the Device Manager agent for your operating system.

Installing the Device Manager agent on a Windows host

You can install the Device Manager agent on a Windows host from the product installation media, and add the `agent-commands` folder to the `PATH` variable.

Tip:

You can also download the Device Manager agent installer using the Tools menu in the GUI.

Before you begin

Stop virus-detection or backup software. If virus-detection or backup software is running during installation, the installation might be slow, fail, or finish incorrectly.

Procedure

1. Log in to Windows as the administrator.
2. Insert the product installation media.
3. In the installation window, select **HDvM Agent** in the **Agent Products** tree, and then click **Install**.

   If the installation window does not display automatically, run the following command:

   DVD-drive:\AGENTS\HDVM\Windows\setup.exe

   Note:

   To install the Device Manager agent and automatically configure the appropriate settings for Replication Manager operation, select **HRpM add-on** in the **Agent Products** tree, and then click **Install**.
4. Enter the required information when prompted.

   Caution: If you install Device Manager agent in a folder other than the default installation folder, specify a folder protected by Administrator permissions.
5. Log out.

6. Log in again to add the agent-commands folder to the `PATH` environment variable.
7. If the following temporary folder remains after the installation, delete it:
   system-drive`\_HDVMAgent`*version-number*`_Install_tmp_\`

Installing the Device Manager agent on a UNIX host

You can install the Device Manager agent on a UNIX host by using the product installation media.

Tip:

You can also download the Device Manager agent installer using the Tools menu in the GUI.

Before you begin

Stop virus-detection programs. If a virus-detection program is running during installation, the installation might be slow, fail, or finish incorrectly.

Procedure

1. Log in to UNIX as the root user.
2. Insert the product installation media.

   If the drive with the installation media is not mounted automatically, mount it manually.
3. Navigate to the directory where the installer program (`install.sh`) is located:

   DVD-ROM-mount-point`/AGENTS/HDVM/`*platform-name*

   These characters can be used in the mount path of a DVD-ROM: A to Z, a to z, 0 to 9, underscores (_), forward slashes (/).
4. Enter the following command:
   - In Solaris, AIX, or HP-UX:

     # **`./install.sh`**
   - In Linux:

     # **`./install.sh [-instpath`** *installation-destination-path-for-Device-Manager-agent*`]`
5. Enter the required information when prompted.

   The following message displays when the Device Manager agent setup is complete:

   `The Device Manager agent setup has completed successfully.`
6. Add host names to the `hosts` file:
   a. Open the `/etc/hosts` file.
   b. Confirm that the local host name and agent host name are present. If your host is running on Linux, enter the name of the local host in the line before the `localhost` entry.
   c. Restart the Device Manager agent services.

Device Manager agent post-installation tasks

After the Device Manager agent installation completes, additional tasks might be required depending on the previous version of the agent that was installed. These tasks can include:

- Modifying Device Manager agent properties
- Registering firewall exceptions (only when performing an unattended installation on Windows)

  This task is required when an unattended installation is performed while Windows Firewall is enabled and the registration of firewall exceptions is disabled.
- Resetting the Java execution environment
- Changing the settings of the antivirus software

  To use antivirus software with Device Manager agent, you need to exclude the installation directory of Device Manager agent from scans that are performed by the antivirus software.

Version upgraded to	Changes and tasks to complete
All versions	▪ If you are using Oracle JDK and either of the following occurs, and the system defaults to a Java execution environment that is not supported, then you need to reset the Java execution environment. • An upgrade installation of Device Manager agent • A new installation of Device Manager agent on a host that has Dynamic Link Manager, Global Link Manager, or Replication Manager Application Agent installed.
v8.1.2 or later	▪ If the value of the `server.http.entity.maxLength` property in the Device Manager agent `server.properties` file is smaller than the default value (262144), the modified value is changed to the default value (262144).

Version upgraded to	Changes and tasks to complete
v8.0.1 or later	▪ If an IPv6 address is configured on a host that has Device Manager agent installed, update the host information if needed. ▪ Device Manager agent acquires the host IPv6 addresses in the priority order of (1) global address, (2) link local address, and (3) site local address. The scope ID, which is the string of characters starting with a percent sign (%), is omitted from the displayed IPv6 addresses.
Upgraded from v7.5.0 or earlier to v8.0.0 or later (Windows)	▪ Reset the user that runs the agent service in Windows. This task is required if the Device Manager agent is upgraded in an environment where the user that runs the agent service has been changed to something other than the default (`LocalSystem`).

Modifying Device Manager agent properties

After installing the Device Manager agent, you might have to modify some of agent properties.

1. Stop the agent service.
2. Modify the properties for the appropriate environment (see the categories that follow).
3. Start the agent service.

Internet Protocol v6 (IPv6)

Set the following properties in the agent `server.properties` file.

- `server.http.socket.agentAddress`: Set the property to the IP address used to connect the Device Manager agent to the Device Manager server.
- `server.http.socket.bindAddress`: If the agent host has multiple NICs, specify the IP address of one or more NIC, as needed, to receive requests.

Veritas Volume Manager (VxVM)

Specify the installed VxVM version in the `veritas.volume.manager.version` property of the `programproductinfo.properties` file. Use the format *x.x* to specify a version.

Dynamic Link Manager environments in which the installation version is earlier than 05-80

In the agent `server.properties` file, specify the agent ports for the `server.http.port` and `server.agent.port` properties.

Oracle JDK used in a Solaris, AIX, or HP-UX environment

When Oracle JDK is used in a Solaris, AIX, or HP-UX environment, a Java execution environment that is not supported is inherited when the following occurs:

- Upgrading Device Manager agent
- A new Device Manager agent installation on a host that also has Dynamic Link Manager, Global Link Manager, or Replication Manager Application Agent installed.

If a Java execution environment that is not supported is inherited, you need to reset the Java execution environment. Install a version of Oracle JDK that provides an appropriate Java execution environment, and then configure an installation path for the `server.agent.JRE.location` property in the `server.properties` file.

UNIX environments, when the Device Manager agent is updated from v05-00 through v5.9

If host programs do not require a different Java Runtime Environment (JRE) other than v 1.4, then JRE v1.4 (included in v05-00 through v5.9) is used.

After the update, if a program is installed with a valid JRE, specify that program installation path in the `server.agent.JRE.location` property of the `server.properties` file.

When a host recognizes a copy pair and is a virtual machine that uses VMware ESXi for virtualization software

Set `true` for the `server.agent.rm.ignorePairStatus` property in the Device Manager agent `server.properties` file.

(Optional) Review the following properties when the Device Manager agent is updated from v8.0.1 or earlier

In the `agent.properties` file, review the `agent.rm.horcmInstance` property values for instance numbers.

- If the default value (4094) or a value in the range from 2048 to 4093 is set: The value changes to 2047.
- If a value in the range from 1 to 2047 is set: The set value is inherited.

  Based on the values mentioned above, instance numbers in the range mentioned below are used, depending on the CCI version.

- If the version is 01-32-03/*XX* or later:
  - Upper limit for the instance numbers:

    (value-of-the-agent.rm.horcmInstance-property)
  - Lower limit for the instance numbers:

    (value-of-the-agent.rm.horcmInstance-property)

    -

    (value-of-the-agent.rm.horcmRange-property) + 1
- If the version is earlier than 01-32-03/*XX*:
  - The instance numbers to use are:

    (value-of-the-agent.rm.horcmInstance-property)

    and

    (value-of-the-agent.rm.horcmInstance-property) - 1

In the `agent.properties` file, review the `agent.rm.horcmService` property values for UDP port numbers.

- If the default value (54323) or a value in the range from 49153 to 65535 is set: The set value is inherited.
- If a value in the range from 2 to 49152 is set: The value changes to 54323.

  Based on the values mentioned above, port numbers in the range mentioned below are used, depending on the CCI version.
- If the version is 01-32-03/*XX* or later:
  - Upper limit for the port numbers:

    (value-of-the-agent.rm.horcmService-property)
  - Lower limit for the port numbers:

    (value-of-the-agent.rm.horcmService-property)

    -

    (value-of-the-agent.rm.horcmRange-property) + 1
- If the version is earlier than 01-32-03/*XX*:
  - The port numbers to use are:

    (value-of-the-agent.rm.horcmService-property)

    and

    (value-of-the-agent.rm.horcmService-property) - 1

Resetting the Java execution environment for Device Manager agent

When Oracle JDK is used, a Java execution environment that is not supported in Device Manager agent, is inherited when the following occurs and you need to reset the Java execution environment:

- Upgrading Device Manager agent
- A new Device Manager agent installation on a host that also has Dynamic Link Manager or Replication Manager Application Agent installed.

For information about the Java execution environment, check the `server.agent.JRE.location` property in the `server.properties` file for Device Manager agent.

For information about starting and stopping Hitachi Command Suite services, see the *Hitachi Command Suite Administrator Guide*.

Before you begin

- Check the Java execution environment prerequisite for Device Manager agent. For more information, see the *Hitachi Command Suite System Requirements*.
- Log in as a user with administrator permissions.

Procedure

1. Stop the Device Manager agent service.
2. Change the Java execution environment.

   In Windows or Linux:

   Run the `javapath_setup` command to change the Java execution environment.

   In Solaris, AIX, or HP-UX:

   Modify the Device Manager agent properties settings.
3. Start the Device Manager agent service.

Result

The Java execution environment used by Device Manager agent is changed to the Java execution environment in the `bin` folder in the specified path.

Resetting the user that runs the agent service in Windows

When Device Manager agent is upgraded to v8.0.0 or later on Windows, the user that runs the agent service reverts to the default (`LocalSystem`). If the user account information has been changed to something other than the default (`LocalSystem`), reset this account information after the installation is complete.

Procedure

1. To modify account information, select **Settings** > **Control Panel** > **Windows Computer Management** > **HBsA Service**.
2. Revise the HBsA Service account information.

Registering firewall exceptions (Windows)

When you perform an unattended installation, if you have Windows Firewall enabled and the registration of firewall exceptions disabled, the port numbers used by Device Manager agent must be manually registered in the firewall exceptions list.

- The port number specified for the `server.agent.port` property in the `server.properties` file (Default: `24041/tcp`)
- The port number specified for the `server.http.port` property in the `server.properties` file (Default: `24042/tcp`)
- The port number specified for the `server.http.localPort` property in the `server.properties` file (Default: `24043/tcp`)

Procedure

1. Log in to Windows using a user ID with Administrator permissions.
2. Run the following command to add the port numbers used by the Device Manager agent to the exceptions list:

   installation-destination-path-for-Device-Manager-agent`\bin\firewall_setup.bat -set`

Preventing virus scanning of the Device Manager agent installation folders

If antivirus software accesses files that Device Manager agent uses, failures caused by delays in I/O or file exclusions might occur.

Procedure

1. To prevent failures, exclude the applicable directory from scans performed by antivirus software while Device Manager agent is operating.
   - Windows or Linux:

     installation-destination-path-for-Device-Manager-Agent
   - Solaris or HP-UX:

     `/opt/HDVM/HBaseAgent`
   - AIX:

     `/usr/HDVM/HBaseAgent`

Workflow for upgrading the OS on the Device Manager agent host

When upgrading the operating system on the management server or host where Device Manager agent is installed, you need to remove Device Manager agent.

This process applies to the following:

- All operating systems
- When you upgrade to either a minor or major version. For example, if you upgrade from Windows Server 2012 to Windows Server 2012 R2, you need to remove Device Manager agent.

1. Remove Device Manager agent.
2. After upgrading the operating system, install a Device Manager agent version that supports the upgraded operating system.

Chapter 5: Hitachi Command Suite server installation in a cluster environment

By clustering two Hitachi Command Suite management servers in an active-standby configuration, the availability of Hitachi Command Suite products is improved.

This module explains how to set up Hitachi Command Suite products in a cluster environment.

Prerequisites for a cluster environment

To set up Hitachi Command Suite in a cluster environment, the management server must have sufficient unused capacity to re-create and back up the database.

- Unused capacity required to re-create the database
  - New installation:

    Disk space used by the Common Component database

    + the disk space used by the databases for all Hitachi Command Suite products (including the Device Manager server database) installed on a Device Manager server
  - Upgrading from v7.6.1 or earlier:

    Disk space used by the Common Component database

    + the disk space used by the databases for all Hitachi Command Suite products (including the Device Manager server database) installed on a Device Manager server + 0.7 GB
- Unused capacity required to back up the databases

  (Total size of all Hitachi Command Suite product databases to be backed up + 4.6 GB) x 2

The combined size of the Device Manager, Tiered Storage Manager, Replication Manager, and Common Component databases is equal to the size of the folders (Windows) or directories (Linux) that contain the database files for the corresponding products. For details about the size of other Hitachi Command Suite product databases, see the guides for those products.

Notes about a cluster environment

When you set up a cluster configuration on the management server, the following applies when using Hitachi Command Suite products:

- The disk configuration must be the same on all the nodes that make up a cluster. Additionally, the installation destination for the Hitachi Command Suite products must also be the same, including the drive letter and path.
- If you change some Hitachi Command Suite product settings after you create the cluster, you must specify the same settings on all the nodes.
- The following names are used for a group of clustered services that can be configured for high availability:

  In Windows: resource group

  In Red Hat Enterprise Linux: service group
- If Host Data Collector is installed, the Host Data Collector service (Host Data Collector Base Service) on the standby node must be running, even when the service is running on the active node.
- If the port for HiRDB is a number other than the default (22032/tcp), configure the same port number for both the active and standby nodes.
- You must configure different port numbers for HiRDB for Hitachi Command Suite v7.6.1 or earlier products and Hitachi Command Suite v8.0.0 or later products. Also, you must configure different port numbers for HiRDB for Hitachi Command Suite v8.0.0 or later and Hitachi File Services Manager.

  When you migrate the database to a shared disk, used for storing database information and accessible by either cluster node, the port number used by HiRDB returns to the default value. If Hitachi Command Suite products are already being used and you have changed the port number for HiRDB to a number other than the default, configure the port number so that the port number for v7.6.1 or earlier does not conflict with the port number for v8.0.0 or later.

  To change the port number, edit the Hitachi Command Suite Common Component settings file, located in the following folders:

  For v8.0.0 or later:

  installation-destination-path-for-Hitachi-Command-Suite\Base64

  For v7.6.1 or earlier:

  installation-destination-path-for-Hitachi-Command-Suite\Base

  For more information about changing port numbers used by Common Component, see the *Hitachi Command Suite Administrator Guide*.
- Register as a client access point, the network name and IP address (cluster management IP address) to the resource group for accessing Hitachi Command Suite products. If the IP address is registered to the resource group, reregister it as a client access point. In this guide, the network name of the cluster management IP address that is registered as a client access point, is referred to as "logical host name."

- The following characters cannot be used in a resource group name: exclamation mark (!), double quotation mark ("), ampersand (&), closing parenthesis ( )), asterisk (*), caret (^), vertical bar (|), less-than sign (<), or greater-than sign (>).
- Log in as a domain user with administrator permissions to access the cluster management application.
- Using the All-in-One Installer, you can install all of the Hitachi Command Suite products except Ops Center Automator. For details about the installation and set up procedures for Ops Center Automator, see the *Hitachi Ops Center Automator Installation and Configuration Guide*.

Installing Hitachi Command Suite in a cluster environment (Windows)

This section describes installing Hitachi Command Suite on the management servers in a cluster configuration when the operating system on the Hitachi Command Suite management server is Windows. This is a common procedure for a new, overwrite, or upgrade installation.

Note:

- To set up a cluster environment, select the Installation in a cluster environment check box in the **Specify the Installation Destination and the Cluster Setting** window of the installation wizard.
- During the setup of a cluster environment, Hitachi Command Suite services are stopped. Consequently, do not access Hitachi Command Suite while setup is in progress.
- Do not run the `hcmds64dbclustersetup` command or the Hitachi Ops Center Automator `setupcluster` command until installation of the standby node is complete.

Procedure

1. Move the owner of the resource group to which Hitachi Command Suite product services are registered from the standby node to the active node.
2. Bring the shared disk and IP address online.
3. When performing an overwrite or upgrade installation in an environment where the REST API is used, take the scripts in the REST API server that are registered to the resource group for the cluster management application offline, and then delete them from the resource group.
4. Install Hitachi Command Suite on the active node. You can also install any other Hitachi Command Suite products at this time by using the All-in-One Installer or integrated installer.

Note:

- In the **Cluster Settings** window, for **Cluster mode**, select **Active node**.
- After the installation on the active node is completed, the Hitachi Command Suite product services registered in the resource group are removed temporarily.
- If you specified names for the services registered to the resource group, respecify the names the next time you register the services. The specified service names are invalid if the services are deleted.

5. If you are using the REST API, complete one of the following applicable tasks on the active node.

   For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

   - **To configure a cluster environment for the REST API:**

     a. If you are using notifications about changes made to storage system configurations, run the API request for deleting the notification destinations registered in the storage system.
     b. Stop the services on the REST API server.
     c. Create a shared folder for the REST API on the shared disk.
     d. Copy the database files to the shared folder.
     e. Set up the cluster environment for the REST API server.
     f. Copy the environment settings file on the active node to the shared folder.
     g. Specify a character string to be used in notifications about changes made to storage system configurations.
     h. Start the services on the REST API server.
     i. Run the API request for obtaining version information, and then check whether the request is processed properly.
     j. Stop the services on the REST API server.
     k. Change the settings so that REST API services do not run automatically when the operating system starts on the active node.

   - **To apply settings in a cluster environment where the REST API has been configured:**

     a. Stop the services on the REST API server.
     b. Specify a character string to be used in notifications about changes made to storage system configurations.#
     c. Start the services on the REST API server.#
     d. Run the API request for obtaining version information, and then check whether the request is processed properly.#
     e. Stop the services on the REST API server.#
     f. Change the settings so that REST API services do not run automatically when the operating system starts on the active node.

   #: This operation is required when upgrading from version 8.4.1 or earlier.

6. Move the owner of the resource group to which Hitachi Command Suite product services are registered from the active node to the standby node.
7. Install Hitachi Command Suite on the standby node.

   Note:
   - In the **Cluster Settings** window, for **Cluster mode**, select **Standby node.**
   - When installing multiple Hitachi Command Suite products on a standby node, install the products in the order that they were installed on the active node.

8. If you are using the REST API, complete one of the following applicable tasks on the standby node, based on when you used the REST API.

   For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

   - **To configure a cluster environment for the REST API:**

     a. Stop the services on the REST API server.
     b. Copy the environment settings file in the shared folder to the standby node.
     c. Specify the character string to be used in notifications about changes made to storage system configurations.
     d. Start the services on the REST API server.
     e. Run the API request for obtaining version information, and then check whether the request is processed properly.
     f. Stop the services on the REST API server.
     g. Change the settings so that REST API services do not run automatically when the operating system starts on the standby node.
     h. Register the script for controlling the activation or stopping of the REST API service in the cluster management application.

   - **To apply settings in a cluster environment where the REST API has been configured:**

     a. Stop the services on the REST API server.
     b. Specify the character string to be used in notifications about changes made to storage system configurations.#
     c. Start the services on the REST API server.#
     d. Run the API request for obtaining version information, and then check whether the request is processed properly.#
     e. Stop the services on the REST API server.#
     f. Change the settings so that REST API services do not run automatically when the operating system starts on the standby node.
     g. Register the script for controlling the activation or stopping of the REST API service in the cluster management application.

   #: This operation is required when performing an upgrade installation from version 8.4.1 or earlier.

9. Start operations in the cluster environment.

For details, see the section that describes how to start operations in a cluster environment.

Note:

- After the installation of Ops Center Automator, it is mandatory to set up Ops Center Automator. For information about this post-installation task, see the *Hitachi Ops Center Automator Installation and Configuration Guide*.
- Set up Compute Systems Manager after a new installation of Compute Systems Manager. For information about this post-installation task, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

Changing from a non-cluster to a cluster environment (Windows)

This section describes the procedures for migrating the operating environment of a Hitachi Command Suite product from a non-cluster to a cluster environment after operation has started.

Note:

- If you are using a custom configuration for Hitachi Command Suite, make note of the custom settings before migrating the operating environment to a cluster environment. During the migration process, you will uninstall Hitachi Command Suite temporarily. You need to specify the custom settings after the operating environment is migrated to a cluster environment.
- During cluster configuration, Hitachi Command Suite services are stopped. Consequently, do not access Hitachi Command Suite while configuration is in progress.
- Uninstall Tuning Manager or Ops Center Automator before migrating the operating environment to a cluster environment.Tuning Manager or Ops Center Automator cannot be migrated by using the following procedure. For information about remote connection to the Tuning Manager server, see the *Hitachi Command Suite Administrator Guide*. For information about starting or stopping the Tuning Manager service, see the documentation for the version that corresponds to the installed Tuning Manager.
- For SSL communication between the REST API client and the REST API server, if you are using a certificate signed by a certificate authority (or a self-signed certificate that you created separately) and you want to continue using SSL communication after migrating to a cluster environment, check the IP address or host name that was specified for Common Name in the request for the issuance of a certificate. If this IP address or host name is not the cluster management IP address or a logical host name, then complete the following tasks after migration:
  - Resubmit an application for a server certificate to the certificate authority.
  - Set up SSL communication on each active and standby node.

  For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide.*

For this procedure, the Device Manager, Tiered Storage Manager, or Replication Manager server operating in a non-cluster configuration is used for the active node in the cluster.

Procedure

1. Run the `hcmds64dbtrans` command to export the Hitachi Command Suite databases.

```
installation-destination-path-for-Hitachi-Command-Suite
\Base64\bin\hcmds64dbtrans /export /workpath work-folder /file
archive-file /auto
```

- `workpath`

  Specify the absolute path to the working folder where you want to temporarily store database data. Specify a folder on your local disk. Verify that no files or subfolders are in the folder specified for the `workpath` option.

- `file`

  Using an absolute path, specify the name of the archive file to be output.

- `auto`

  Automatically starts or stops Hitachi Command Suite services.

2. When using the REST API, complete the following steps.

   For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

   a. If you are using notifications about changes made to storage system configurations, run the API request for deleting the notification destinations registered in the storage system.
   b. Back up the database and the environment settings file.

3. If HiRDB is currently using a different port number than the default (22032/tcp) in a non-cluster environment, make a note of the current port number that is being used.
4. Uninstall Hitachi Command Suite. If other v8.0.0 or later Hitachi Command Suite products are installed, uninstall them also.
5. Install Hitachi Command Suite on the active node. If you are installing other v8.0.0 or later Hitachi Command Suite products, install them also.
6. Run the `hcmds64dbtrans` command to import the Hitachi Command Suite databases.

```
installation-destination-path-for-Hitachi-Command-Suite
\Base64\bin\hcmds64dbtrans /import /workpath work-folder [/file
archive-file] /type ALL /auto
```

- `workpath`

  When using the *archive-file* for the import:

  Specify the absolute path to the folder used to extract the *archive-file*. Specify a folder on your local disk. If you want to use the *archive-file*, the `file` option must be specified. Verify that no files or subfolders are in the folder specified for the `workpath` option.

  When not using the *archive-file* for the import:

  Specify the folder that stores the database data files transferred from the migration source server. Do not change the structure of those files in the transferred folder. Also, do not specify the `file` option.

- `file`

  Specify the absolute path to the *archive-file* of the databases transferred from the migration source server. If the database data files transferred from the migration source server are stored in the directory specified by `workpath`, you do not need to specify the `file` option.

- `type`

  As a rule, specify `ALL`. If you specify `ALL`, the databases for all installed Hitachi Command Suite products that are installed on the migration destination server are automatically selected and migrated. When migrating the database of a specific Hitachi Command Suite product because of different management server configurations, specify the product name to be migrated, as listed in the following table. To specify multiple product names, use a comma to separate the names.

  You can use the `type` option to migrate databases only if the database data of all the specified products is contained in the *archive-file* or in the folder specified by the `workpath` option. and all of the specified products exist on the migration destination server. If any of the products do not meet these conditions, data cannot be migrated.

  The following table shows the values to use for the `type` option when migrating databases.

Table 31 Type option values to specify when migrating databases

Product	Value
Device Manager[1, 2]	DeviceManager
Tiered Storage Manager[1]	TieredStorageManager
Replication Manager[2]	ReplicationManager
Other products	Refer to the guide for each product.
Notes:	

Product	Value
a. When importing databases that were exported from a v7.0.0 or later environment, regardless of whether you have registered a Tiered Storage Manager license, import both the Device Manager and Tiered Storage Manager databases at the same time. **b.** When importing the Replication Manager database, import the Device Manager database at the same time.	

- `auto`

  Automatically starts or stops Hitachi Command Suite services.

7. If you are using the REST API, complete the following steps on the active node.

   For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

   a. Stop the services on the REST API server.
   b. Create a shared folder for the REST API on the shared disk.
   c. Copy the database files to the shared folder.
   d. Set up the cluster environment for the REST API server.
   e. Specify a character string to be used in notifications about changes made to storage system configurations.
   f. Start the services on the REST API server.
   g. Run the API request for obtaining version information, and then check whether the request is processed properly.
   h. Stop the services on the REST API server.
   i. Change the settings so that REST API services do not run automatically when the operating system starts on the active node.

8. Install Hitachi Command Suite on the standby node. If you are installing other v8.0.0 or later Hitachi Command Suite products, install them also.
9. If HiRDB is currently using a different port number than the default (22032/tcp) in a non-cluster environment, set the port number you made note of in step 2 for both the active and standby nodes.
10. If Tuning Manager was remotely connected while Device Manager and Tiered Storage Manager were being used in a non-cluster environment, if necessary, start Tuning Manager and then reconfigure the setting for linking with Tuning Manager.
11. If you are using the REST API, complete the following steps on the standby node.

    For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

    a. Stop the services on the REST API server.
    b. On the standby node, restore the database file and environment settings file that were backed up on the active node.

c. Overwrite the environment settings files on the standby node with the following environment settings files on the active node.
   - `StartupV.properties` file
   - `rabbitmq-env-conf.bat` file
   - `rabbitmq.config` file
   - `.erlang.cookie` file

d. Specify the character string to be used in notifications about changes made to storage system configurations.
e. Start the services on the REST API server.
f. Run the API request for obtaining version information, and then check whether the request is processed properly.
g. Stop the services on the REST API server.
h. Change the settings so that REST API services do not run automatically when the operating system starts on the standby node.
i. Register the script for controlling the activation or stopping of the REST API service in the cluster management application.

12. Start operations in the cluster environment.

For details, see the section that describes how to start operations in a cluster environment.

Starting Hitachi Command Suite server after a new installation or migration in a cluster environment (Windows)

After a new installation of Hitachi Command Suite, or an operating environment is changed from a non-cluster to a cluster environment, configure and start the cluster environment by using a command.

Before you begin

Before starting Automation Director in a cluster environment:

- In the cluster management software, right-click to select the resource script and set its dependence on the [property]-[Dependencies] tab.
- In addition, specify [HAutomation Engine *HCS-clustergroup-name*] to the resources that must be brought online before bringing the script online.

Procedure

1. Verify that the owner of the resource group to which the Hitachi Command Suite product services are registered is a host name of the standby node.
2. Run the following command to bring online the resource group of the cluster management application and the Hitachi Command Suite product services.

```
installation-destination-path-for-Hitachi-Command-Suite
\Base64\ClusterSetup\hcmds64clustersrvstate /son /r resource-
group-name
```

- `son`

  Use this option to enable failover by bringing the resource group set for the cluster management application online.

- `r`

  Specify the resource group name. If a resource group name contains a space, comma (,), semicolon (;), or equal sign (=), enclose the resource group name in double quotation marks ("). The following characters cannot be used in a resource group name: exclamation mark (!), double quotation mark ("), ampersand (&), closing parenthesis ( )), asterisk (*), caret (^), vertical bar (|), less-than sign (<), or greater-than sign (>).

3. To use the REST API, bring online the scripts that are registered to the resource group for the cluster management application, on the REST API server.
4. On the standby node, register the licenses for the products you want to use by using the graphical user interface.
   - Access the logical host name of the standby node.
   - A license key must be entered for each product that is installed.
5. Move the owner of the resource group to which the Hitachi Command Suite product services are registered from the standby node to the active node.
6. On the active node, register the licenses for the products you want to use by using the graphical user interface.
   - Access the logical host name of the active node.
   - A license key must be entered for each product that is installed.
7. Depending on the environment in which the REST API is to be used, you might need to complete the following step.

   For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

   a. Run the API request for registering storage systems by specifying `true` for the `isNotifiable` attribute.

Starting Hitachi Command Suite server after overwriting, upgrading, or removing in a cluster environment (Windows)

This section describes starting the Hitachi Command Suite server when upgrading or overwriting Hitachi Command Suite or after removing a Hitachi Command Suite product in a cluster environment.

Before you begin

Before starting Automation Director in a cluster environment:

- In the cluster management software, right-click to select the resource script and set its dependence on the [property]-[Dependencies] tab.
- In addition, specify [HAutomation Engine *HCS-clustergroup-name*] to the resources that must be brought online before bringing the script online.

Procedure

1. Move the owner of the resource group to which the Hitachi Command Suite product services are registered from the standby node to the active node.
2. Run the following command to bring online the resource group of the cluster management application and the Hitachi Command Suite product services.

   ```
   installation-destination-path-for-Hitachi-Command-Suite
   \Base64\ClusterSetup\hcmds64clustersrvstate /son /r resource-
   group-name
   ```

   - `son`

     Use this option to enable failover by bringing the resource group set for the cluster management application online.

   - `r`

     Specify the resource group name. If a resource group name contains a space, comma (,), semicolon (;), or equal sign (=), enclose the resource group name in double quotation marks ("). The following characters cannot be used in a resource group name: exclamation mark (!), double quotation mark ("), ampersand (&), closing parenthesis ( )), asterisk (*), caret (^), vertical bar (|), less-than sign (<), or greater-than sign (>).

3. In order to use the REST API, bring online the scripts that are registered to the resource group for the cluster management application, on the REST API server.
4. Depending on the environment in which the REST API is to be used, you might need to complete the following steps.

   For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

   a. Run the API request for registering destinations for notifications about changes made to storage system configurations.
   b. Run the API request for registering storage systems by specifying `true` for the `isNotifiable` attribute.

Removing Hitachi Command Suite from a cluster environment (Windows)

This section describes how to remove Hitachi Command Suite from the management servers in a cluster configuration in Windows.

For information about stopping services, see the *Hitachi Command Suite Administrator Guide.*

Before you begin

Preparations for removing Hitachi Command Suite.

Procedure

1. Move the owner of the resource group to which the Hitachi Command Suite product services are registered, from standby node to active node.
2. If you are using the REST API, then on the REST API server, take offline the target script that is registered in the resource group. Afterward, delete it from the resource group.
3. Uninstall Hitachi Command Suite from the active node.

   In the **Cluster Settings** window, for the resource group name, specify the name of the resource group to which the Hitachi Command Suite product services are registered.
4. Move the owner of the resource group to which the Hitachi Command Suite product services are registered, from the active node to the standby node.
5. Uninstall Hitachi Command Suite from the standby node.

   In the **Cluster Settings** window, for the resource group name, specify the name of the resource group to which the Hitachi Command Suite product services are registered.
6. If the following resources are not used by other applications, take the resources offline, and then delete them by using the cluster management application.

   - Cluster management IP address
   - Shared disk

   When the resource group to which the Hitachi Command Suite product services are registered is no longer necessary, delete that resource group.

   Note: If you specified names for the services registered to the resource group, respecify the names the next time you register the services. The specified service names are invalid if the services are deleted.

Performing tasks on Hitachi Command Suite product services by using commands (Windows)

During cluster configuration, commands can be run in the following instances:

- If registration of Hitachi Command Suite product services failed during cluster configuration, you can re-register the product services by using commands.
- If Hitachi Command Suite product services were mistakenly registered or deleted by using the cluster management application, you can delete the services mistakenly registered or re-register services that were deleted.
- If suppressing failover and you want Hitachi Command Suite product services to be offline or online.

Registering Hitachi Command Suite services (Windows)

This section describes registering Hitachi Command Suite services to a cluster management application resource group.

Before you begin

- Provide a resource group, which is a group of services to be clustered (units of service failover).
- Configure a resource group that includes the shared disks and client access points (cluster management IP addresses and network names) that can be inherited by the active and standby nodes.
- Confirm that the cluster management application can successfully control resource allocation, resource removal, and operation monitoring.
- If there is a resource group in which other Hitachi Command Suite products are registered, use that resource group.
- Verify that the resource group consists of only those resources that are related to Hitachi Command Suite products.

Procedure

1. Run the following command to register the Hitachi Command Suite services to a resource group managed by the cluster management application:

   installation-destination-path-for-Hitachi-Command-Suite`\Base64\ClusterSetup\hcmds64clustersrvupdate /sreg /r` *resource-group-name* `/sd` *drive-letter-name* `/ap` *name-of-the-resource-set-as-a-client-access-point*

   - `sreg`

     Use this option to register the Hitachi Command Suite services to a resource group.

   - `r`

     Specify the resource group name. If a resource group name contains a space, comma (,), semicolon (;), or equal sign (=), enclose the resource group name in double quotation marks ("). The following characters cannot be used in a resource group name: exclamation mark (!), double quotation mark ("), ampersand (&), closing parenthesis ( )), asterisk (*), caret (^), vertical bar (|), less-than sign (<), or greater-than sign (>).

- `sd`

  Specify the drive letter of the shared disk drive registered to the resource group. You cannot specify multiple drive letters for this option. If data is stored across multiple shared disk drives, you must run the **`hcmds64clustersrvupdate`** command for each disk.

- `ap`

  Specify the name of the resource set as a client access point.

2. If you are using the REST API, complete the following steps:
   a. Stop the services on the REST API server.
   b. Register, as a generic script, the script for controlling the activation or stopping of the REST API service in the resource group of the cluster management application.

   For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

Deleting Hitachi Command Suite services (Windows)

This section describes deleting Hitachi Command Suite services from a cluster management application resource group.

Procedure

1. Run the following command to delete the Hitachi Command Suite services from a resource group managed by the cluster management application:

   installation-destination-path-for-Hitachi-Command-Suite`\Base64\ClusterSetup\hcmds64clustersrvupdate /sdel /r` *resource-group-name*

   - `sdel`

     Use this option to delete the Hitachi Command Suite services from the specified resource group. The Hitachi Command Suite services for v7.x.x and 8.x.x will be deleted.

   - `r`

     Specify the resource group name. If a resource group name contains a space, comma (,), semicolon (;), or equal sign (=), enclose the resource group name in double quotation marks ("). The following characters cannot be used in a resource group name: exclamation mark (!), double quotation mark ("), ampersand (&), closing parenthesis ( )), asterisk (*), caret (^), vertical bar (|), less-than sign (<), or greater-than sign (>).

   Note:
   - Manually delete Hitachi File Services Manager services.
   - If you specified names for the services registered to the resource group, respecify the names the next time you register the services. The specified service names are invalid if the services are deleted.

2. If you are using the REST API, complete the following steps:
   a. Take offline the REST API server scripts that are registered to the resource group for the cluster management application.
   b. Delete the REST API server scripts from the resource group.

Bringing Hitachi Command Suite services online (Windows)

This section describes bringing online a resource group of the cluster management application to which the Hitachi Command Suite product services are registered.

Procedure

1. Run the following command to bring online a resource group of the cluster management application to which the Hitachi Command Suite product services are registered.

   installation-destination-path-for-Hitachi-Command-Suite`\Base64\ClusterSetup\hcmds64clustersrvstate /son /r` *resource-group-name*

   - `son`

     Use this option to enable failover by bringing the resource group that is set for the cluster management application online.

   - `r`

     Specify the resource group name. If a resource group name contains a space, comma (,), semicolon (;), or equal sign (=), enclose the resource group name in double quotation marks ("). The following characters cannot be used in a resource group name: exclamation mark (!), double quotation mark ("), ampersand (&), closing parenthesis ( )), asterisk (*), caret (^), vertical bar (|), less-than sign (<), or greater-than sign (>).

2. In order to use the REST API, bring online the scripts on the REST API server that are registered to the resource group for the cluster management application.

Taking Hitachi Command Suite services offline (Windows)

This section describes taking offline a resource group of the cluster management application to which the Hitachi Command Suite product services are registered.

Procedure

1. Run the following command to take the resource group managed by the cluster management application and the Hitachi Command Suite services offline:

```
installation-destination-path-for-Hitachi-Command-Suite
\Base64\ClusterSetup\hcmds64clustersrvstate /soff /r resource-
group-name
```

- `soff`

  Suppresses failover by taking offline the Hitachi Command Suite services registered to the resource group managed by the cluster management application.

- `r`

  Specify the resource group name. If the name contains a space, comma (,), semicolon (;), or equal sign (=), enclose the name in double quotation marks ("). The following characters cannot be used in a resource group name: exclamation mark (!), double quotation mark ("), ampersand (&), closing parenthesis ( )), asterisk (*), caret (^), vertical bar (|), less-than sign (<), or greater-than sign (>).

2. In order to use the REST API, take offline the scripts on the REST API server that are registered to the resource group for the cluster management application.

Hitachi Command Suite services to register in cluster management applications (Windows)

The following table lists the Hitachi Command Suite product services that can be registered to cluster management applications on the management server by using the **`hcmds64clustersrvupdate`** and the **`hcmds64clustersrvstate`** commands.

Table 32 HCS services to be registered in the cluster management application

Product name	Displayed service name (Resource name)	Service name
Common Component	HiRDB/ClusterService _HD1	HiRDBClusterService_HD1
	HBase 64 Storage Mgmt Web Service	HBase64StgMgmtWebService
	HBase 64 Storage Mgmt Web SSO Service	HBase64StgMgmtWebSSOService
	HBase 64 Storage Mgmt SSO Service	HBase64StgMgmtSSOService
Device Manager	HCS Device Manager Web Service	DeviceManagerWebService 64
	HiCommandServer	HiCommandServer
	HiCommand Tiered Storage Manager	HiCommandTieredStorage Manager
Tuning Manager Server	HCS Tuning Manager REST Application Service	TuningManagerRESTService

Product name	Displayed service name (Resource name)	Service name
	HiCommand Performance Reporter	PerformanceReporter64
	HiCommand Suite TuningManager	HiCommandTuningManager64
	PFM - Name Server [*logical-host-name*]	JP1PCMGR_PN [*logical-host-name*]
	PFM - Master Manager [*logical-host-name*]	JP1PCMGR_PM [*logical-host-name*]
	PFM - Master Store [*logical-host-name*]	JP1PCMGR_PS [*logical-host-name*]
	PFM - View Server [*logical-host-name*]	JP1PCMGR_PP [*logical-host-name*]
	PFM - Correlator [*logical-host-name*]	JP1PCMGR_PE [*logical-host-name*]
	PFM - Trap Generator [*logical-host-name*]	JP1PCMGR_PC [*logical-host-name*]
	PFM - Action Handler [*logical-host-name*]	JP1PCMGR_PH [*logical-host-name*]
	PFM - Agent Store for HealthCheck [*logical-host-name*]	JP1PCAGT_0S [*logical-host-name*]
	PFM - Agent for HealthCheck [*logical-host-name*]	JP1PCAGT_0A [*logical-host-name*]
Compute Systems Manager	HCS Compute Systems Manager Web Service	ComputeSystemsManagerWebService64
	DeploymentManager PXE Management *	PxeSvc
	DeploymentManager PXE Mtftp *	PxeMtftp
	DeploymentManager Transfer Management *	ftsvc

Product name	Displayed service name (Resource name)	Service name
Automation Director	HAutomation Common Event [*logical-host-name*]	JP1_Base_Event [*logical-host-name*]
	HAutomation Common Base [*logical-host-name*]	JP1_Base_[*logical-host-name*]
	HAutomation Engine Web Service	AutomationWebService64
	HAutomation Engine [*logical-host-name*]	JP1_AJS2_[*logical-host-name*]
*This service is available if Deployment Manager is installed.		

New installation in a cluster environment (Red Hat Enterprise Linux)

This section describes setting up a cluster environment by using Red Hat High Availability when the operating system on the Hitachi Command Suite management server is Red Hat Enterprise Linux 6.5.

The examples use Conga when the luci package of the following version is installed:

- Version: 0.26.0
- Release: 48.el6

Conga is a clustering package provided with Red Hat High Availability. For more information about Conga, see the guide for Red Hat High Availability. For information about system requirements, see the *Hitachi Command Suite System Requirements.*

Installation in a cluster environment requires the following tasks:

1. If any other HCS products are included in the cluster environment, remove the HCS product services from the product group.
2. Install HCS on the active node.
3. Install HCS on the standby node.
4. Create and enable scripts for registering HCS services.
5. Register HCS services to the cluster service group to support HCS with both nodes.
6. Select the active node and configure the restart policy.

Note: During the setup of a cluster environment, Hitachi Command Suite services are stopped. Consequently, do not access Hitachi Command Suite while setup is in progress.

Deleting HCS product services from the service group (Red Hat Enterprise Linux)

Delete the HCS product services from the Red Hat High Availability service group.

For information about checking the operating status of HCS product services, see the *Hitachi Command Suite Administrator Guide*.

Procedure

1. From the cluster management application, stop all of the HCS product services.

   When using Conga:

   a. Open the **Service Groups** window and select the service group in which the HCS product services are registered.
   b. Click **stop (disable)** to stop and disable the selected service group in which the HCS product services will be deleted.

2. From the cluster management application, delete all of the following HCS product services.

   When using Conga:

   a. Click **Remove** to delete the services.
   b. Click **Submit** to apply the changes.

   - HiRDB
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
   - HCS Device Manager Web Service
   - HiCommandServer
   - HiCommand Tiered Storage Manager

   If you are using the REST API, delete the Configuration Manager REST API resource.

   If other HCS product services are registered, delete those services also. For information about how to delete them, see the guide for each product.

   Caution: Do not delete the following resources from the service group:

   - Shared disk
   - Cluster management IP address

3. From the cluster management application, select the active node to start the service group.

   When using Conga:

   a. From the list, select the active node.
   b. Click **Start** to start the service group.

   The shared disk and the cluster management IP address become enabled.

Installing Hitachi Command Suite on the active node (Red Hat Enterprise Linux)

Install Hitachi Command Suite on the active node, and then change the environment configurations of Hitachi Command Suite products.

Before you begin

- Provide a service group, which is a group of services to be clustered (units of service failover).
- Configure a service group that includes the shared disks and cluster management IP addresses that can be inherited by the active and standby nodes.
- Verify that Red Hat High Availability can successfully control registration and removal of resources, and monitor operations.
- If there is a service group in which other Hitachi Command Suite products are registered, use that service group.
- Verify that the service group consists of only those resources that are related to Hitachi Command Suite products.
- If other Hitachi Command Suite products are installed on systems that are going to be used in the cluster environment, remove the Hitachi Command Suite product services from the service group.

Procedure

1. Verify that the service group has been moved to the active node.
2. Install Hitachi Command Suite on the active node.

   If other Hitachi Command Suite products are installed on systems that are going to be used in the cluster:

   - Make the shared disk accessible, and then specify a path on the shared disk for the database storage location.
   - Specify a logical host name for the management server IP address (host name of the virtual host allocated to the cluster management IP address).

   If Hitachi Command Suite products are installed on only one system in the cluster:

   - Specify a path on the local disk for the database storage location.
   - For the management server IP address, specify the IP address of the active node.
3. After installation, and by using the graphical user interface (GUI), register the licenses for the products you want to use.
   - Access the IP address of the active node.
   - Enter a license key for each product that is installed.

4. Change the URL for starting the graphical user interface (GUI) to the logical host name.

   Run the following command to verify that the correct logical host name is set:

   *installation-destination-path-for-Hitachi-Command-Suite/*Base64/bin/hcmds64chgurl -print

   If the logical host name is not set, run the following command to change the URL:

   *installation-destination-path-for-Hitachi-Command-Suite/*Base64/bin/hcmds64chgurl -change http://*IP-address-or-host-name-of-the-active-node#:port-number* http://*logical-host-name:port-number*

   Where # is specify the value that was specified during installation.

5. Create a cluster configuration file.

   This step is not required if any other Hitachi Command Suite products are included in the cluster environment.

   If none of the items above apply, create a new cluster configuration file by using a text editor and by specifying the following items:

   mode=online

   virtualhost=*logical-host-name*

   onlinehost=*active-node-host-name*

   standbyhost=*standby-node-host-name*

   Save the file as cluster.conf in *installation-destination-path-for-Hitachi-Command-Suite*/Base64/conf.

   Note: For virtualhost, onlinehost, and standbyhost, an IP address cannot be specified. Also, verify that an IP address can be resolved from the host name.

6. Open the server.properties file and verify that the logical host name is specified in the server.http.host property.

   If the logical host name is not set, change the current value to the logical host name.

   *installation-destination-path-for-Hitachi-Command-Suite/*HiCommandServer/config/server.properties

7. If a cluster environment is not already configured for Hitachi Command Suite products, migrate the data to the shared disk by specifying the database on the shared disk as the database to be used. Go to steps 8 through 11.

   If a cluster environment has been configured for other Hitachi Command Suite products, go to step 12.

8. Run the following commands to back up the database after the new installation, in preparation of possible failure.

installation-destination-path-for-Hitachi-Command-Suite/`Base64/bin/hcmds64backups -dir` *target-directory-for-storing-backup-files* `-auto`

- `dir`

  Using an absolute path, specify the local disk directory for the database backup files. Verify that the `dir` directory is empty.

- `auto`

  Automatically starts or stops Hitachi Command Suite services.

Note: When you run the `hcmds64backups` command, a directory named database is created in the target directory for storing backup files, and a database backup file is created with the name `backup.hdb`.

9. Make a note of the current port number used by HiRDB for either of the following situations because the `hcmds64dbclustersetup` command in step 10 sets the port to the default:
   - Other Hitachi Command Suite products are installed.
   - The port number used by HiRDB was changed to a number other than the default (22032/tcp).
10. Run the following command to migrate the database to the shared disk. This command backs up the content of the database to the directory on the local disk for storing the data. Then the command re-creates the database in the directory on the specified shared disk for re-creating the database.

    installation-destination-path-for-Hitachi-Command-Suite/`Base64/bin/hcmds64dbclustersetup -createcluster -databasepath` *target-directory-on-the-shared-disk-for-re-creating-the-database* `-exportpath` *target-directory-on-the-local-disk-for-storing-data* `-auto`

    - `createcluster`

      This option changes the Hitachi Command Suite product from a non-cluster configuration to a cluster configuration.

    - `databasepath`

      Specify the directory in which you want to re-create the database to be used for a cluster configuration. Use an absolute path to a directory on the shared disk. The path name cannot exceed 63 bytes.

      These characters can be specified in the path: A to Z, a to z, 0 to 9, period (.), underscores (_). Additionally, forward slashes (/) can be used as path delimiters.

- `exportpath`

  Specify the directory in which you want to store the data from the database before migration. Use an absolute path to a directory on a local disk. The path name must not exceed 63 bytes. The characters that can be used to specify the path are the same as for `databasepath`.

- `auto`

  Automatically stops or starts Hitachi Command Suite services.

  Note:

  - If *target-directory-on-the-local-disk-for-storing-data* already exists, empty or delete the directory.
  - Do not disconnect the shared disk from the active node until the `hcmds64dbclustersetup` command finishes successfully.
  - If you restart the server after the `hcmds64dbclustersetup` command has finished abnormally, the node to which the shared disk connects might switch to the standby node.

11. When you run the `hcmds64dbclustersetup` command, the port number used by HiRDB is changed to the default (22032/tcp). Reset the port number using the port number that you noted in step 9.
12. Run the `hcmds64srv -statusall` command to verify that the Hitachi Command Suite product services have stopped.
13. Run the following command to prevent the Hitachi Command Suite product services from automatically starting when the server starts.

    ```
    installation-destination-path-for-Hitachi-Command-Suite/
    Base64/bin/hcmds64srv -starttype manual -all
    ```

14. To prevent the Device Manager server and the Tiered Storage Manager server from automatically starting when the server starts, either move the files below to another directory or change the file names. If you change the file names, do not use the character "K" or "S" as the first letter of the new file names.

    - `/etc/rc3.d/S99hicommand` (for Device Manager)
    - `/etc/rc3.d/S99htsmserver` (for Tiered Storage Manager)
    - `/etc/rc5.d/S99hicommand` (for Device Manager)
    - `/etc/rc5.d/S99htsmserver` (for Tiered Storage Manager)

15. If you are using the REST API, complete the following steps.

    For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

    a. Stop the services on the REST API server.
    b. Create a shared directory for the REST API on the shared disk.
    c. Copy the database files to the shared directory.
    d. Set up the cluster environment for the REST API server.
    e. Copy the environment settings file on the active node to the shared directory.

f. Specify a character string to be used in notifications about changes made to storage system configurations.
g. Start the services on the REST API server.
h. Run the API request for obtaining version information, and then check whether the request is processed properly.
i. Stop the services on the REST API server.
j. Change the settings so that REST API services do not run automatically when the operating system starts on the active node.

16. Move the service group to the standby node.

    For information about checking the operating status of HCS product services, see the *Hitachi Command Suite Administrator Guide*.

Installing Hitachi Command Suite on the standby node (Red Hat Enterprise Linux)

Before you begin

If other Hitachi Command Suite products are installed on systems that are going to be used in the cluster environment, remove the Hitachi Command Suite product services from the service group.

Install Hitachi Command Suite on the standby node, and then change the environment configurations of Hitachi Command Suite products.

Procedure

1. Install Hitachi Command Suite on the standby node.

   Specify the following settings during installation:

   - Specify the same installation location as the active node.
   - If a cluster environment has been configured for another Hitachi Command Suite product, specify a logical host name for the management server IP address (host name of the virtual host allocated to the cluster management IP address). If a cluster environment has been configured for another Hitachi Command Suite product, specify the host name IP address of the standby node.

2. After the installation, and by using the GUI, register the licenses for the products you want to use.

   - Access the IP address of the standby node.
   - A license key must be entered for each product that is installed.

3. Create a cluster configuration file.

   Use a text editor to create a cluster configuration file by specifying the following items:

   `mode=standby`

   `virtualhost=`*logical-host-name*

   `onlinehost=`*active-node-host-name*

`standbyhost=`*standby-node-host-name*

Save the file as `cluster.conf` in *installation-destination-path-for-Hitachi-Command-Suite*`/Base64/conf`.

Note: For `virtualhost`, `onlinehost`, and `standbyhost`, an IP address cannot be specified. Also, verify that an IP address can be resolved from the host name.

Note that if any other Hitachi Command Suite products are included in the cluster environment, you do not need to create a cluster configuration file.

4. Open the `server.properties` file and verify that the logical host name is specified in the `server.http.host` property.

   If the logical host name is not set, change the current value to the logical host name.

   installation-destination-path-for-Hitachi-Command-Suite`/HiCommandServer/config/server.properties`

5. If a cluster environment is not already configured for Hitachi Command Suite products, migrate the data to the shared disk by specifying the database on the shared disk as the database to be used. Go to steps 6 through 7.

   If a cluster environment has been configured for other Hitachi Command Suite products, go to step 8.

6. Run the following command to migrate the database to the shared disk. This command backs up the content of the database to the directory on the local disk for storing the data. Then the command changes the settings so that the database in the directory on the specified shared disk for re-creating the database is used.

   installation-destination-path-for-Hitachi-Command-Suite`/Base64/bin/hcmds64dbclustersetup -createcluster -databasepath` *target-directory-on-the-shared-disk-for-re-creating-the-database* `-exportpath` *target-directory-on-the-local-disk-for-storing-data* `-auto`

   - `createcluster`

     This option changes the Hitachi Command Suite product from a non-cluster configuration to a cluster configuration.

   - `databasepath`

     Specify the directory in which you want to re-create the database to be used for a cluster configuration. Specify the absolute path to the same directory as the one being used by the active node, *target-directory-on-the-shared-disk-for-re-creating-the-database* to re-create its database.

     These characters can be used in the path: A to Z, a to z, 0 to 9, period (.), underscores (_). Additionally, forward slashes (/) can be used as path delimiters.

- `exportpath`

  Specify the directory in which you want to store the data from the database before migration. Use an absolute path to a directory on a local disk. The path name must not exceed 63 bytes. The characters that can be used to specify the path are the same as for `databasepath`.

- `auto`

  Automatically stops or starts Hitachi Command Suite services.

  Note:
  - If *target-directory-on-the-local-disk-for-storing-data* already exists, empty or delete the directory.
  - Do not disconnect the shared disk from the standby node until the `hcmds64dbclustersetup` command finishes successfully.
  - If you restart the server after the `hcmds64dbclustersetup` command has finished abnormally, the node to which the shared disk connects might switch to the active node.

7. When you run the `hcmds64dbclustersetup` command, the port number used by HiRDB is changed to the default (22032/tcp). For this reason, if you want to change the port number for HiRDB to a number other than the default, set the port number of the active node to the port number for HiRDB.
8. Run the `hcmds64srv -statusall` command to verify that the Hitachi Command Suite product services have stopped.
9. Run the following command to prevent Hitachi Command Suite product services from automatically starting when the server starts:

   ```
   installation-destination-path-for-Hitachi-Command-Suite/
   Base64/bin/hcmds64srv -starttype manual -all
   ```

10. To prevent the Device Manager server and the Tiered Storage Manager server from automatically starting when the server starts, either move the files below to another directory or change the file names. If you change the file names, do not use the character "K" or "S" as the first letter of the new file names.
    - `/etc/rc3.d/S99hicommand` (for Device Manager)
    - `/etc/rc3.d/S99htsmserver` (for Tiered Storage Manager)
    - `/etc/rc5.d/S99hicommand` (for Device Manager)
    - `/etc/rc5.d/S99htsmserver` (for Tiered Storage Manager)

    For information about checking the operating status of HCS product services, see the *Hitachi Command Suite Administrator Guide*.

11. If you are using the REST API, complete the following steps.

    For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

    a. Stop the services on the REST API server.
    b. Copy the environment settings file in the shared directory to the standby node.

c. Specify the character string to be used in notifications about changes made to storage system configurations.
d. Start the services on the REST API server.
e. Run the API request for obtaining version information, and then check whether the request is processed properly.
f. Stop the services on the REST API server.
g. Change the settings so that REST API services do not run automatically when the operating system starts on the standby node.

Creating scripts for registering Hitachi Command Suite services (Red Hat Enterprise Linux)

After installing Hitachi Command Suite on the active and standby nodes, download, modify, and enable the LSB (Linux Standard Base) compliant scripts for registering Hitachi Command Suite services to a Red Hat Enterprise Linux service group using Red Hat High Availability on both nodes.

Procedure

1. From the `SAMPLE/CLUSTER_TOOL` directory in the integrated installation media, obtain the following zip file that includes sample script files:

   `HCS_LinuxCluster_SampleScripts_HCS.zip`

   `HCS_LinuxCluster_SampleScripts_Common.zip`

   `HCS_LinuxCluster_SampleScripts_ConfManager.zip` (if you are using the REST API)
2. Unzip the script files to the `/etc/init.d` directory. Script files are included for registering the following HCS services:

Service name	Script name
HiRDB	`sc_hbase64_hirdb`
HBase 64 Storage Mgmt SSO Service	`sc_hbase64_hsso`
HBase 64 Storage Mgmt Web SSO Service	`sc_hbase64_hweb`
HBase 64 Storage Mgmt Web Service	`sc_hbase64_web`
HCS Device Manager Web Service	`sc_hbase64_dm`
HiCommandServer	`sc_hicommand`
HiCommand Tiered Storage Manager	`sc_htsmserver`
Configuration Manager REST API	`sc_confmanagerctrl`*

Service name	Script name
* This is a script file included in HCS_LinuxCluster_SampleScripts_ConfManager.zip. This script file is required only when using the REST API.	

3. Modify the script files to provide the applicable value for the following variables:

   HCMDS_HOME=*<installation-destination-path-for-Hitachi-Command-Suite>*/Base64

   PDHOST=*<logical-host-name>*
4. Save the script files.
5. Run the following command to change the access permissions:

   `# chmod u+x` *script-file-name*

Registering Hitachi Command Suite services (Red Hat Enterprise Linux)

Register Hitachi Command Suite services to a Red Hat High Availability service group.

Before you begin

Create and enable the scripts for registering Hitachi Command Suite services in the service group.

Procedure

1. From the cluster management application, stop all of the HCS services.

   When using Conga:

   a. Open the **Service Groups** window and select the service group in which you want to register the HCS product services.
   b. Click **stop (disable)** to stop and disable the selected service group in which the HCS services will be registered.
2. From the cluster management application, use the created scripts to register the services in the service group:

   When using Conga:

   a. Click **Add Resource**, and then from the **Add Resource to Service** list, select **Script**. For information about the order for registering the services and values for each service item, see the following table.

Table 33 Values to specify for each service item registered in a service group

Order of registration	Service name	(Optional) Script name	Script file path
1	HiRDB	`sc_hbase64_hirdb`	`/etc/init.d/sc_hbase64_hirdb`
2	HBase 64 Storage Mgmt SSO Service	`sc_hbase64_hsso`	`/etc/init.d/sc_hbase64_hsso`
3	HBase 64 Storage Mgmt Web SSO Service	`sc_hbase64_hweb`	`/etc/init.d/sc_hbase64_hweb`
4	HBase 64 Storage Mgmt Web Service	`sc_hbase64_web`	`/etc/init.d/sc_hbase64_web`
5	HCS Device Manager Web Service	`sc_hbase64_dm`	`/etc/init.d/sc_hbase64_dm`
6	HiCommandServer	`sc_hicommand`	`/etc/init.d/sc_hicommand`
7	HiCommand Tiered Storage Manager	`sc_htsmserver`	`/etc/init.d/sc_htsmserver`
8	Configuration Manager REST API	`sc_confmanagerctrl`	`/etc/init.d/sc_confmanagerctrl`

b. If you removed any services, other than those described in the following table, when removing services from the service group before beginning a new installation of Hitachi Command Suite, re-register those services. For more information about registering services, see the guide for each product.

c. Click **Submit** to apply the changes.

Result

Registration of Hitachi Command Suite is now complete. Start operations in the cluster environment by starting the service group.

Configuring the restart policy on the active node (Red Hat Enterprise Linux)

After you install Hitachi Command Suite on both of the Red Hat Enterprise Linux cluster nodes and register the HCS services, configure the restart policy on the active node by using Red Hat High Availability.

Procedure

1. From the cluster management application, start the service group in which the HCS product services are registered.

   When using Conga:

   a. Open the **Service Groups** window, and select the service group in which the Hitachi Command Suite product services are registered.

   b. To start the service group, select the active or standby node from the list, and then click **start**.

2. Depending on the environment in which the REST API is to be used, you might need to complete the following steps.

   For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

   a. Run the API request for registering destinations for notifications about changes made to storage system configurations.

   b. Run the API request for registering storage systems by specifying `true` for the `isNotifiable` attribute.

Upgrading or overwriting Hitachi Command Suite in a cluster environment (Red Hat Enterprise Linux)

This section describes the process of installing Hitachi Command Suite as an upgrade or overwrite installation on the management servers in a Red Hat Enterprise Linux cluster configuration.

Upgrading or overwriting an installation in a cluster environment includes the following process:

1. Remove the Hitachi Command Suite product services from the service group.
2. Upgrade or overwrite an installation of Hitachi Command Suite on the active node.
3. Upgrade or overwrite an installation of Hitachi Command Suite on the standby node.
4. Register the Hitachi Command Suite product services to the service group.
5. Begin using the cluster environment.

Note: During the setup of a cluster environment, Hitachi Command Suite services are stopped. Consequently, do not access Hitachi Command Suite while setup is in progress.

Upgrading or overwriting Hitachi Command Suite on the active node (Red Hat Enterprise Linux)

This section describes installing Hitachi Command Suite by upgrading to a new version or overwriting an existing version of Hitachi Command Suite on the Red Hat Enterprise Linux active node.

Before you begin

Remove the Hitachi Command Suite product services from the service group.

Procedure

1. Verify whether the service group is running on the active node.

   If necessary, move the service group to the active node.
2. Stop the installed Hitachi Command Suite product services.

   For details about stopping the services, see the *Hitachi Command Suite Administrator Guide*.
3. Upgrade or overwrite the existing installation of Hitachi Command Suite.

   Back up the database before the upgrade or overwrite installation by following the instructions of the installer.
4. Stop the installed Hitachi Command Suite product services.

   For details about stopping the services, see the *Hitachi Command Suite Administrator Guide*.
5. Run the following command to prevent Hitachi Command Suite product services from automatically starting when the server starts:

   ```
   installation-destination-path-for-Hitachi-Command-Suite/
   Base64/bin/hcmds64srv -starttype manual -all
   ```
6. To prevent the Device Manager server and the Tiered Storage Manager server from automatically starting when the server starts, on both the active and standby nodes, either move the files below to another directory or change the file names. If you change the file names, do not use the character "K" or "S" as the first letter of the new file names.

   - `/etc/rc3.d/S99hicommand` (for Device Manager)
   - `/etc/rc3.d/S99htsmserver` (for Tiered Storage Manager)
   - `/etc/rc5.d/S99hicommand` (for Device Manager)
   - `/etc/rc5.d/S99htsmserver` (for Tiered Storage Manager)
7. If you are using the REST API, complete one of the following applicable tasks on the active node.

   For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

   - **To configure a cluster environment for the REST API:**

     a. If you are using notifications about changes made to storage system configurations, run the API request for deleting the notification destinations registered in the storage system.

b. Stop the services on the REST API server.
c. Create a shared directory for the REST API on the shared disk.
d. Copy the database files to the shared directory.
e. Set up the cluster environment for the REST API server.
f. Copy the environment settings file on the active node to the shared directory.
g. Specify a character string to be used in notifications about changes made to storage system configurations.
h. Start the services on the REST API server.
i. Run the API request for obtaining version information, and then check whether the request is processed properly.
j. Stop the services on the REST API server.
k. Change the settings so that REST API services do not run automatically when the operating system starts on the active node.

- **To apply settings in a cluster environment where the REST API has been configured:**

a. Stop the services on the REST API server.
b. Specify a character string to be used in notifications about changes made to storage system configurations.#
c. Start the services on the REST API server. #
d. Run the API request for obtaining version information, and then check whether the request is processed properly.#
e. Stop the services on the REST API server.#
f. Change the settings so that REST API services do not run automatically when the operating system starts on the active node.

#: This operation is required when upgrading from version 8.4.1 or earlier.

8. Move the service group to the standby node.

Result

The active node is upgraded or overwritten.

Upgrading or overwriting Hitachi Command Suite on the standby node (Red Hat Enterprise Linux)

This section describes installing Hitachi Command Suite by upgrading to a new version or overwriting an existing version of Hitachi Command Suite on the Red Hat Enterprise Linux standby node.

Before you begin

Remove the Hitachi Command Suite product services from the service group.

Procedure

1. Stop the installed Hitachi Command Suite product services.

   For details about stopping the services, see the *Hitachi Command Suite Administrator Guide*.
2. Upgrade or overwrite the existing installation of Hitachi Command Suite.
3. Stop the installed Hitachi Command Suite product services.

   For details about stopping the services, see the *Hitachi Command Suite Administrator Guide*.
4. Run the following command to prevent Hitachi Command Suite product services from automatically starting when the server starts:

   ```
   installation-destination-path-for-Hitachi-Command-Suite/
   Base64/bin/hcmds64srv -starttype manual -all
   ```
5. To prevent the Device Manager server and the Tiered Storage Manager server from automatically starting when the server starts, on both the active and standby nodes, either move the files below to another directory or change the file names. If you change the file names, do not use the character "K" or "S" as the first letter of the new file names.

   - `/etc/rc3.d/S99hicommand` (for Device Manager)
   - `/etc/rc3.d/S99htsmserver` (for Tiered Storage Manager)
   - `/etc/rc5.d/S99hicommand` (for Device Manager)
   - `/etc/rc5.d/S99htsmserver` (for Tiered Storage Manager)
6. If you are using the REST API, complete one of the following applicable tasks on the standby node.

   For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

   - **To configure a cluster environment for the REST API:**

     a. Stop the services on the REST API server.
     b. Copy the environment settings file in the shared directory to the standby node.
     c. Specify the character string to be used in notifications about changes made to storage system configurations.#
     d. Start the services on the REST API server.#
     e. Run the API request for obtaining version information, and then check whether the request is processed properly.#
     f. Stop the services on the REST API server.#
     g. Change the settings so that REST API services do not run automatically when the operating system starts on the standby node.
     h. Register the script for controlling the activation or stopping of the REST API service in the cluster management application.
   - **To apply settings in a cluster environment where the REST API has been configured:**

     a. Stop the services on the REST API server.

b. Specify the character string to be used in notifications about changes made to storage system configurations.#
c. Start the services on the REST API server.#
d. Run the API request for obtaining version information, and then check whether the request is processed properly.#
e. Stop the services on the REST API server.#
f. Change the settings so that REST API services do not run automatically when the operating system starts on the standby node.

#: This operation is required when upgrading from version 8.4.1 or earlier.

Changing from a non-cluster to a cluster environment (Red Hat Enterprise Linux)

This section describes the procedures for changing the operating environment of a Device Manager, Tiered Storage Manager, or Replication Manager system from a non-cluster to a Red Hat Enterprise Linux cluster environment.

For this procedure, the Device Manager, Tiered Storage Manager, or Replication Manager servers operating in a non-cluster configuration are used for the active node in the cluster.

Note:

- During cluster configuration, Hitachi Command Suite services are stopped. Consequently, do not access Hitachi Command Suite while configuration is in progress.
- For SSL communication between the REST API client and the REST API server, if you are using a certificate signed by a certificate authority (or a self-signed certificate that you created separately) and you want to continue using SSL communication after migrating to a cluster environment, check the IP address or host name that was specified for Common Name in the request for the issuance of a certificate. If this IP address or host name is not the cluster management IP address or a logical host name, then complete the following tasks after migration:
  - Resubmit an application for a server certificate to the certificate authority.
  - Set up SSL communication on each active and standby node.

  For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide.*

Procedure

1. If Tuning Manager is remotely connected, stop the Tuning Manager services on the machine where the Tuning Manager server is installed.
2. Install Hitachi Command Suite on the computer to be used as the standby node.

3. Using the GUI, register the licenses for the products you want to use.
   - Access the IP address of the standby node.
   - A license key must be entered for each product that is installed.
4. From the active node, run the following command to change the URL for starting the GUI to the logical host name:

   installation-destination-path-for-Hitachi-Command-Suite/`Base64/bin/hcmds64chgurl -change http://`*IP-address-or-host-name-of-the-active-node:port-number* `http://`*logical-host-name:port-number*
5. Use a text editor to create a cluster configuration file on the active and standby nodes.

   Specify the following items in the cluster configuration file for the active node:

   `mode=online`

   `virtualhost=`*logical-host-name*

   `onlinehost=`*active-node-host-name*

   `standbyhost=`*standby-node-host-name*

   Specify the following items in the cluster configuration file for the standby node:

   `mode=standby`

   `virtualhost=`*logical-host-name*

   `onlinehost=`*active-node-host-name*

   `standbyhost=`*standby-node-host-name*

   Save each file on its node as `cluster.conf` in *installation-destination-path-for-Hitachi-Command-Suite*`/Base64/conf`.

   Note:
   - Specify `online` for the active node and specify `standby` for the standby node.
   - For `virtualhost`, `onlinehost`, and `standbyhost`, an IP address cannot be specified. Also, verify that an IP address can be resolved from the host name.
6. On both the active and standby nodes, open the `server.properties` file, and then specify a logical host name for the `server.http.host` property.

   installation-destination-path-for-Hitachi-Command-Suite/`HiCommandServer/config/server.properties`
7. Run the following command to back up the database at the active node:

```
installation-destination-path-for-Hitachi-Command-Suite/
Base64/bin/hcmds64backups -dir directory-for-storing-backup-files
-auto
```

- `dir`

  Using an absolute path, specify the local disk directory for the database backup files. Verify that the directory specified with `dir` is empty.

- `auto`

  Automatically starts or stops Hitachi Command Suite services.

> **Note:**
>
> When you run the `hcmds64backups` command, a directory named database is created in the target directory for storing backup files, and a database backup file is created with the name `backup.hdb`.

8. When using the REST API, complete the following steps on the active node.

   For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

   a. If you are using notifications about changes made to storage system configurations, run the API request for deleting the notification destinations registered in the storage system.
   b. Back up the database and the environment settings file.

9. If HiRDB is currently using a different port number than the default (22032/tcp), make a note of the current port number that is being used by the active node.
10. From the active node, run the following command to migrate the database to the shared disk. This command backs up the content of the database to the directory on the local disk for storing the data. Then the command re-creates the database in the directory on the specified shared disk for re-creating the database.

    ```
    installation-destination-path-for-Hitachi-Command-Suite/
    Base64/bin/hcmds64dbclustersetup -createcluster -databasepath
    target-directory-on-the-shared-disk-for-re-creating-the-database
    -exportpath target-directory-on-the-local-disk-for-storing-data -
    auto
    ```

    - `createcluster`

      This option changes the Hitachi Command Suite product from a non-cluster configuration to a cluster configuration.

    - `databasepath`

      Specify the directory in which you want to re-create the database to be used for a cluster configuration. Use an absolute path to a directory on the shared disk. The path name must not exceed 63 bytes.

      These characters can be used in the path: A to Z, a to z, 0 to 9, period (.), underscores (_). Additionally, forward slashes (/) can be used as path delimiters.

- `exportpath`

  Specify the directory in which you want to store the data from the database before migration. Use an absolute path to a directory on a local disk. The path name must not exceed 63 bytes. The characters that can be used to specify the path are the same as for `databasepath`.

- `auto`

  Automatically stops or starts Hitachi Command Suite services.

  Note:

  - If you run the `hcmds64dbclustersetup` command, the settings for remote connection with Tuning Manager are initialized.
  - If *target-directory-on-the-local-disk-for-storing-data* already exists, empty or delete the directory.
  - Do not disconnect the shared disk from the active node until the `hcmds64dbclustersetup` command finishes successfully.
  - If you restart the server after the `hcmds64dbclustersetup` command has finished abnormally, the node to which the shared disk connects might switch to the standby node.

11. On the standby node, run the following command to set the database on the shared disk as the database to be used. This command backs up the content of the database to the directory on the local disk for storing the data. Then the command changes the settings so that the database in the directory on the specified shared disk for re-creating the database is used.

```
installation-destination-path-for-Hitachi-Command-Suite/
Base64/bin/hcmds64dbclustersetup -createcluster -databasepath
target-directory-on-the-shared-disk-for-re-creating-the-database
-exportpath target-directory-on-the-local-disk-for-storing-data -
auto
```

For details about the options that can be specified for the `hcmds64dbclustersetup` command, see step 9.

For `databasepath`, specify the same directory as the one being used by the active node to re-create the database.

12. When you run the `hcmds64dbclustersetup` command, the port number used by HiRDB is changed to the default (22032/tcp). If HiRDB was using a different port number than the default in a non-cluster environment, reset the port number that you noted for the active node to be the port number for HiRDB.

13. On both the active and standby nodes, verify that the Hitachi Command Suite product services have stopped.

For details about checking the operating status of services, see the *Hitachi Command Suite Administrator Guide* and the guide for Hitachi File Services Manager.

14. On both the active and standby nodes, run the following command to prevent Hitachi Command Suite product services from automatically starting when the server starts:

```
installation-destination-path-for-Hitachi-Command-Suite/
Base64/bin/hcmds64srv -starttype manual -all
```

15. To prevent the Device Manager server and the Tiered Storage Manager server from automatically starting when the machine starts, on both the active and standby nodes, either move the files below to another directory or change the file names. If you change the file names, do not use the character "K" or "S" as the first letter of the new file names.

- `/etc/rc3.d/S99hicommand` (for Device Manager)
- `/etc/rc3.d/S99htsmserver` (for Tiered Storage Manager)
- `/etc/rc5.d/S99hicommand` (for Device Manager)
- `/etc/rc5.d/S99htsmserver` (for Tiered Storage Manager)

16. If you are using the REST API, complete the following steps.

For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

a. On each active and standby node, stop the REST API server services.
b. On the active node, create a shared directory for the REST API on the shared disk.
c. On the active node, copy the database files to the shared directory.
d. On the active node, configure a cluster environment for the REST API server.
e. On the active node, specify a character string to be used in notifications about changes made to storage system configurations.
f. On the active node, start the REST API server services.
g. On the active node, run the API request for obtaining version information, and then check whether the request is processed properly.
h. On the active node, stop the REST API server services.
i. On the standby node, restore the database file and environment settings file that were backed up on the active node.
j. Overwrite the environment settings files on the standby node with the following environment settings files on the active node.
   - `StartupV.properties` file
   - `rabbitmq-env-conf.bat` file
   - `rabbitmq.config` file
   - `.erlang.cookie` file
k. On the standby node, specify the character string to be used in notifications about changes made to storage system configurations.
l. On the standby node, start the REST API server services.
m. On the standby node, run the API request for obtaining version information, and then check whether the request is processed properly.

n. On the standby node, stop the REST API server services.
o. On each active and standby node, change the settings so that the REST API services do not run automatically when the operating system starts.

17. Register the Hitachi Command Suite services to the service group.
18. If Tuning Manager was remotely connected with Device Manager and Tiered Storage Manager were being used in a non-cluster environment, if necessary, start the Tuning Manager service and then specify the settings for linking with Tuning Manager.

    For more information about checking the operating status of services or remote connection to the Tuning Manager server, see the *Hitachi Command Suite Administrator Guide*.

Result

Configuration of the cluster environment is now complete. To start operations in the cluster environment, see the instructions on how to start operations in a cluster environment.

Removing Hitachi Command Suite from a cluster environment (Red Hat Enterprise Linux)

This section describes how to remove Hitachi Command Suite from the management servers in a Red Hat Enterprise Linux cluster configuration.

Before you begin

- Preparations for removing Hitachi Command Suite.
- Remove the Hitachi Command Suite services from the service group.

Procedure

1. Check whether the service group has been moved to an active node.

   If the service group has not been moved, move the service group to an active node.
2. Stop the Hitachi Command Suite product services.

   For details about stopping the services, see the *Hitachi Command Suite Administrator Guide*.
3. Run the following command to back up the database:

```
installation-destination-path-for-Hitachi-Command-Suite/
Base64/bin/hcmds64backups -dir directory-for-storing-backup-files
-auto
```

- `dir`

  Using an absolute path, specify the local disk directory for the database backup files.

  Verify that the directory specified with `dir` is empty.

- `auto`

  Automatically starts or stops Hitachi Command Suite services.

> **Note:**
>
> When you run the `hcmds64backups` command, a directory named `database` is created in the target directory for storing backup files, and a database backup file is created with the name `backup.hdb`.

4. When using the REST API, back up the database and the environment settings file. For details, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide.*
5. Stop the Hitachi Command Suite product services.

   For details about stopping the services, see the *Hitachi Command Suite Administrator Guide*.
6. Remove Hitachi Command Suite from the active node.
7. On the active node, delete any files and directories that are no longer necessary, such as those created during installation in the cluster environment.
8. Move the service group to the standby node.
9. Remove Hitachi Command Suite from the standby node.
10. On the standby node, delete any files and directories that are no longer necessary, such as those created during installation in the cluster environment.
11. Re-register the services that have been removed from the service group before uninstalling Hitachi Command Suite, and that are used by other Hitachi Command Suite products.
12. If any of the following resources are not being used by another application, delete the unused resources:
    - Cluster management IP address
    - Shared disk
13. If the service group in which the Hitachi Command Suite product services are registered is no longer necessary, then delete it.
14. To continue to use a service group that has not been deleted, start the service group.

Chapter 6: Removing HCS

This module describes how to remove HCS and its components.

Removing Hitachi Command Suite server

You can remove HCS when you no longer need to manage storage systems and hosts.

There are two methods for removing HCS:

- Use the All-in-One Uninstaller to remove products if they were installed by using the All-in-One Installer. The following HCS products can be removed in batch:
  - HCS (Device Manager, Tiered Storage Manager, and Replication Manager)
  - Tuning Manager
  - Compute Systems Manager
  - Ops Center Automator
- Use the uninstallers of individual products to remove only some HCS products from a management server.

Removing HCS deletes all properties files, database files, log files, and other files as well. In addition, files and folders created within the HCS installation folder are also deleted when HCS is removed.

Note:

- The Common Component files are deleted only if there are not any products that require Common Component on the management servers.
- If a stand-alone installation of Host Data Collector has been performed previously, some folders and files might remain even if HCS is removed. In this case, remove Host Data Collector alone.
- If you are using Hitachi File Services Manager, it needs to be uninstalled after HCS is removed.

Prerequisites for removing the HCS server

If you are using the REST API, in order to delete the REST API server from the registered destinations for sending notifications about changes made to storage system configurations, you must delete the storage system information before uninstalling HCS. For details about deleting storage system information, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

If you are installing HCS on another management server, or if you are continuing system operation with HCS products installed on a different system, export the database before removing HCS.

For more information, see the *Hitachi Command Suite Administrator Guide*.

For information about removing Hitachi Command Suite when linking with Hitachi File Services Manager or Hitachi Storage Navigator Module 2, see the Hitachi Command Suite release notes.

Removing HCS products using the All-in-One Uninstaller (Windows)

The following HCS products can be removed in batch if they were installed using the All-in-One Installer:

- HCS (Device Manager, Tiered Storage Manager, and Replication Manager)
- Tuning Manager
- Compute Systems Manager
- Ops Center Automator

Procedure

1. Log on to Windows as the administrator.
2. Navigate to **Control Panel**.
3. Double-click **Programs and Features**.
4. In the **Programs and Features** window, select **HCS All-in-One Uninstaller**.
5. Click **Uninstall**.
6. Follow the on-screen instructions.

Result

When HCS is removed, the Removal Complete window appears.

Removing Hitachi Command Suite from a Windows host

Remove HCS from Windows hosts using Programs and Features.

Procedure

1. Log on to Windows as the administrator.
2. Navigate to **Control Panel**.
3. Double-click **Programs and Features**.
4. In the **Programs and Features** window, select **Hitachi Command Suite**.
5. Click **Uninstall**.
6. Follow the on-screen instructions.

Note: If you are using Storage Navigator Modular 2, in the removing wizard, from the **Pre-Removal Confirmation** window, select the **After the uninstallation finishes, start the services of all Hitachi Command Suite products** check box.

Result

When Hitachi Command Suite is removed, the Removal Complete window appears.

When you remove v7.4.1 or earlier that is installed on a drive other than the system drive, a `temp` folder might appear in the `root` folder of the drive where the product was installed. You can delete the `temp` folder.

Removing Hitachi Command Suite from a Linux host

Remove Hitachi Command Suite from Linux hosts using the command line.

Procedure

1. Log on to Linux as the root user.
2. Navigate to the root directory.
3. Enter the following command:

   ```
   # installation-destination-path-for-Hitachi-Command-Suite/
   Uninstall/uninstall.sh
   ```
4. Follow the on-screen instructions.

   Note: If you are using Storage Navigator Modular 2, after the following message is displayed, enter `y`.

   ```
   Set the services to start after removal:

   Hitachi Command Suite products services will remain for
   the other products of the suite.

   Start Hitachi Command Suite products services after the
   removal completes? (y/n):
   ```

Result

When Hitachi Command Suite is removed, the following message appears:

```
Hitachi Command Suite removal completed successfully.
```

Removing Storage Navigator Modular 2 and File Services Manager

When removing Hitachi Command Suite in an environment where Hitachi File Services Manager (earlier than v6.2.0) and 32-bit Hitachi Storage Navigator Modular 2 are installed, both need to be removed and reinstalled if you plan to continue using these products.

For 32-bit Storage Navigator Module 2, after removing HCS, change the Common Component settings, and then uninstall 32-bit Storage Navigator Modular 2. To reinstall 32-bit Storage Navigator Module 2, use the individual product installer on the installation media.

Note: For File Services Manager (earlier than v6.2.0), you do not need to run the command to change the Common Component settings. You can uninstall and then reinstall (pre-v6.2.0) File Services Manager.

Procedure

1. Log on as the administrator or root user.
2. Navigate to the root directory (in Linux).
3. Run the following command to change the Common Component settings:
   - For Windows:

     installation-destination-path-for-Storage-Navigator-Modular-2\Base\bin\hcmdsprmset /host 127.0.0.1 /port *non-SSL-port-number* [/sslport *SSL-port-number*]

   - For Linux:

     *installation-destination-path-for-Storage-Navigator-Modular-2/*Base/bin/hcmdsprmset -host 127.0.0.1 -port *non-SSL-port-number* [-sslport *SSL-port-number*]

   For *non-SSL-port-number* and *SSL-port-number*:

   Specify the connection port number for HBase Storage Mgmt Web Service. For non-SSL communication, specify the port number for non-SSL communication (default: 23015). For SSL communication, specify the port number for SSL communication (default: 23016).

About removing Host Data Collector

You can remove Host Data Collector if it is no longer being used for host management. Removing Host Data Collector deletes all property files, log files, and other related files.

Removing Host Data Collector (Windows)

You can remove Host Data Collector if it is no longer needed for host management.

Before you begin

Log in with administrator permissions.

Procedure

1. From the Windows **Start** menu, select **Settings** > **Control Panel** > **Programs and Features**.
2. Select **Host Data Collector** and click **Uninstall**.

3. Follow the instructions in the removal wizard.
   When Host Data Collector has been successfully removed, the **Uninstall Complete** window displays.

   Tip: If v7.4.1 or earlier of Host Data Collector is removed from a drive other than the system drive, the `temp` folder might remain in the `root` folder of the drive where Host Data Collector was installed. If you do not need this folder, delete it.

Removing Host Data Collector (Linux)

You can remove Host Data Collector if it is no longer needed for host management.

Before you begin

Log in as the root user.

Procedure

1. Run the following command:

   installation-destination-path-for-Host-Data-Collector`\HDC\Base\bin\.unsetup.sh`

2. Follow the instructions in the displayed prompts.
   When Host Data Collector has been successfully removed, the following message appears:

   `Host Data Collector removal completed successfully.`

Removing Device Manager agent

You can remove the Device Manager agent when you no longer need it to manage a host. Removing an agent also removes its properties and log files.

Prerequisites for removing Device Manager agent

Before removing the Device Manager agent from a host, note the following:

- For HP-UX: Verify that the **`swagentd`** daemon is running.

  If necessary, start the daemon process by executing:

  `/usr/sbin/swagentd`

- For HP-UX: Verify that the file system mounted on the host matches that defined in `/etc/fstab`.

- If you perform another operation while the Device Manager agent is being removed, the operation terminates with an error. If a program related to the Device Manager agent is installed on the host when this occurs, some Device Manager agent data may remain on the host.
- If you start to remove the Device Manager agent while one of the following commands is executing, the attempt may terminate in an incomplete state, forcing you to restart the system before removing the agent:
  - **`hbsasrv`**
  - **`hdvmagt_setting`**
  - **`HiScan`**

    Note: If you remove the Device Manager agent while **`HiScan`** is executing, the process for removing the agent is canceled. If this occurs, wait until the command terminates, and then remove the agent.
  - **`hldutil`**
  - **`TIC`**
- If the host operating system is Solaris 10 or 11, do not specify settings related to a system zone.
- When the process for removing the Device Manager agent starts, the Device Manager agent and any add-on modules automatically stop.
- The following files are not deleted:
  - Files created by the **`HiScan`** command
  - CCI configuration definition files
  - Error information files created by executing the **`TIC`** command
- If Dynamic Link Manager v05-80 or later, or Global Link Manager agent v6.2 or later is installed, the following data remains after the Device Manager agent is removed:
  - Data in the Device Manager agent installation folder
  - Data in the JRE installation folder

  To delete this data, completely remove the Dynamic Link Manager and the Global Link Manager agent.

Removing Device Manager agent from Windows Server 2008/2012 Server Core hosts

Remove Device Manager agent from Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 Server Core, and Minimal Server

Interface Environment for Windows Server 2012 and Windows Server 2012 R2 hosts by using the **agent_uninstShortcut.bat** file.

Procedure

1. Start a command prompt as an administrator.
2. Run the following command:

   installation-destination-path-for-Device-Manager-agent\bin\agent_uninstShortcut.bat

   When Device Manager agent is removed, the **InstallShield Wizard Completed** window is displayed.
3. Manually remove the following tasks that run the **HiScan** command:
   - Any task that runs **exeHiScan.bat** with a schedule that was changed in the **Scheduled Tasks** window that opens from the Control Panel.
   - Any task that runs **exeHiScan.bat** that is registered on Windows.

Removing Device Manager agent from Windows hosts (other than Windows Server 2008/2012 Server Core)

Remove Device Manager agent from Windows hosts (other than Windows Server 2008, Windows Server 2008 R2, Windows 2012, or Windows 2012 R2 Server Core) by using Programs and Features.

Note:

Instead of using the Windows GUI, you can also run *installation-destination-path-for-Device-Manager-agent*\bin\agent_uninstShortcut.bat from the command line. For Server Core environment for Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 and Minimal Server Interface environment for Windows Server 2012 and Windows Server 2012 R2, you should run the command prompt as an administrator.

Procedure

1. Navigate to **Control Panel**.
2. Double-click **Programs and Features**.
3. In the **Programs and Features** window, select **Hitachi Device Manager agent**.
4. Click **Uninstall**.

Next steps

The following tasks that run the **HiScan** command remain after you remove Device Manager agent and must be removed manually:

- Any task that runs **exeHiScan.bat** with a schedule that was changed in the **Scheduled Tasks** window that opens from the Control Panel (or changed from the Task Scheduler in Administrative Tools).
- Any task that runs **exeHiScan.bat** that is registered on Windows.

Removing Device Manager agent from UNIX hosts

Remove Device Manager agent from UNIX hosts by using the command line.

Procedure

1. Log on to UNIX as the root user.
2. At the command line, enter the following:
   - In Solaris or HP-UX:

     #/opt/HDVM/HBaseAgent/bin/**.uninstall.sh**
   - In AIX:

     #/usr/HDVM/HBaseAgent/bin/**.uninstall.sh**
   - In Linux:

     installation-destination-path-for-Device-Manager-agent

     /bin/.uninstall.sh
3. Follow the instructions on the screen.

Result

When the Device Manager agent is removed, the following message appears:

```
Device Manager - Agent removed successfully.
```

Appendix A: Unattended installation and removal

This appendix describes unattended installation and removal operations.

HCS server unattended installation

HCS provides an unattended feature so that you do not need to provide responses during installation. You can perform an unattended installation by creating and executing a script file when the conditions on multiple management servers are the same.

HCS server unattended installation properties

Before performing an unattended server installation, provide values for the following properties.

- `HINST_INSTDIR`
- `HINST_DBDIR`
- `HINST_IPADDRESS`
- `HINST_DBBACKUP`
- `HINST_DBBACKUPDIR`
- `HINST_HDVMHEAP`
- `HINST_RUNSERVICE`
- `HINST_IGNORE_CAPACITY_CHECK`
- `HINST_IGNORE_NETWORKING_CHECK`
- `HINST_IGNORE_VIRTUAL_MEMORY_CHECK`

The following table explains each property and lists the default values.

Note:

If a property is not specified, the default value is used.

Table 34 Unattended installation property settings

Property Name	Details	Default Value
HINST_INSTDIR	For a new installation: Specify the installation directory.	Windows: *%ProgramFiles%*\HiCommand Linux: /opt/HiCommand
HINST_DBDIR[1]	For a new installation: Specify the directory for database files.	Windows: *value-specified-for-HINST_INSTDIR*\database Linux: /var/*value-specified-for-HINST_INSTDIR*/database
HINST_IPADDRESS[2]	For a new installation: Specify the IP address or host name of the management server.	Host name obtained by the **hostname** command.
HINST_DBBACKUP[3]	Specify whether to back up the databases before performing an upgrade installation on the management server: ▪ TRUE: Back up the databases ▪ FALSE: Do not back up the databases	TRUE
HINST_DBBACKUPDIR[3]	If Hitachi Command Suite products are installed on the management server: Specify the directory for database backup files.	Windows: *value-specified-for-HINST_INSTDIR*\backup Linux: /var/*value-specified-for-HINST_INSTDIR*/backup

Property Name	Details	Default Value
HINST_HDVMHEAP	Specify the memory heap size for the Device Manager server: ▪ Small ▪ Medium ▪ Large	Large
HINST_RUNSERVICE[4]	Specify whether to start the product services after the installation: ▪ TRUE: Start after installation. ▪ FALSE: Do not start after installation.	TRUE
HINST_IGNORE_CAPACITY_CHECK	Specify whether to continue the installation when there is insufficient unused capacity: ▪ TRUE: Continue the installation ▪ FALSE: Stop the installation.	FALSE
HINST_IGNORE_NETWORKING_CHECK	Specify whether to continue the installation when the host name or IP address that was specified in HINST_IPADDRESS is not communicating with the network. ▪ TRUE: Continue the installation. ▪ FALSE: Stop the installation.	FALSE

Property Name	Details	Default Value
`HINST_IGNORE_VIRTUAL_MEMORY_CHECK`	Specify whether to continue the installation when there is insufficient virtual memory. ▪ `TRUE`: Continue the installation. ▪ `FALSE`: Stop the installation.	`FALSE`

Notes:

1. When installing on the active node in a cluster environment, you must specify this property. When installing on the standby node, you do not need to specify this property.
2. When installing in a cluster environment, you must specify this property on both the active and standby nodes.
3. If you perform an installation on the standby node in a cluster environment, databases are not backed up.
4. If you specify this property in a cluster environment, it is ignored.

Prerequisites for HCS server unattended installation

Before performing an unattended installation of HCS server, review system requirements information.

1. Stop Tuning Manager services:
   - If a version earlier than 6.3.0 is installed on the same management server, stop the Tuning Manager Agent for SAN Switch service.
   - If Tuning Manager is remotely connected, stop the Tuning Manager server service.
2. Run Tiered Storage Manager tasks when upgrading from v7.1.0 or earlier:
   - If there are incomplete tasks (standby, running, being canceled), go to the Tasks & Alerts tab and execute or cancel the tasks. After upgrading, register the canceled tasks as new.
3. Check the user group name when upgrading from v7.1.0 through v7.5.0.
   - When upgrading to v7.6.0 or later, private logical groups are created and within these groups, top folders are created for each user group. The user group name is used as the initial folder name. Users that have Admin permission for user management should check the user group name before performing an upgrade installation.
   - For details about private logical groups, see the *Hitachi Command Suite User Guide*.

4. Remove the Plug-in for Virtualization Server Provisioning when upgrading from v7.1.1 through v7.6.1.
   - If you are using Plug-in for Virtualization Server Provisioning, remove it. You cannot use Plug-in for Virtualization Server Provisioning in v8.0.0 or later.
5. Determine the values that are set during installation
6. Verify that the execution result file (`HInstReport.txt`) is closed.

The prerequisite checker verifies whether the installation destination satisfies the requirements.

To access the prerequisite checker on Windows, use the integrated installation media or run the **`prereqchk.exe`** file located in *`DVD-drive`*`:\HCS\`

To access the prerequisite checker in Linux, run the **`prereqchk.sh`** file located in *`DVD-ROM-mount-directory`*`/TOOL/PREREQCHK/`

For system requirements, see the *Hitachi Command Suite System Requirements*. To check task status, see the *Hitachi Command Suite User Guide*.

Installing HCS in Windows (unattended installation)

You can perform unattended installations on Windows environments.

Procedure

1. Log on to the Windows operating system with administrator permissions.
2. Open a command or PowerShell window.

   If the UAC (User Account Control) function is enabled in Windows, use the command or PowerShell window that you opened as an administrator.
3. Navigate to *`DVD-drive`*`:\HCS\`. This is the location of the installer program.
4. Enter the following command:
   - In a command window:

     `setup.exe /v"/qr` *`property-name=value`*`"`

     To specify a value that contains a space, add a backslash and quotation mark (\") before and after the value.
   - In a PowerShell window:

     `setup.exe /v`` `"/qr` *`property-name=value`*`` `"``

     If you specify multiple properties, use a space to separate each entry.

     To specify a value that contains a space, add a slash and quotation mark (/") before and after the value.

Result

When the installation completes, the result is written in the `HInstReport.txt` file on the desktop. If you see `SUCCESS` in the summary section of the file, the installation was successful.

Installing HCS in Linux (unattended installation)

You can perform unattended server installations on Linux.

Procedure

1. Log on to the Linux operating system as the root user.
2. Open a shell window and navigate to the directory that holds the installer program:
   DVD-ROM-mount-directory/HCS/*platform-name*
   The following characters can be used in the mount path of a DVD-ROM: A to Z, a to z, 0 to 9, underscores (_), and forward slashes (/).
3. Enter the following command:
   `#./install.sh -s property-name=value`
   To specify multiple properties, use a space to separate each entry.
   To specify a value that contains a space, add a backslash and quotation mark (\") before and after the value.

Result

When the installation completes, the result is written in the `HInstReport.txt` file in the `/tmp` directory. If you see `SUCCESS` in the summary section of the file, the installation was successful.

Device Manager agent unattended installation

You can automate agent installation by creating and executing a script file. Unattended installation can be used when installing on multiple hosts with the same conditions. By defining items such as the Device Manager server information and the **`HiScan`** command execution time when creating a settings file (`HDVMAgent.conf`), you can also perform basic setup functions during the unattended installation.

When setting up an unattended installation, note the following:

- For an overwrite installation, v04-10 or later of the Device Manager agent must be installed.
- `LocalSystem` is set for the agent service account.

Prerequisites for Device Manager agent unattended installations

Before performing an unattended installation of the Device Manager agent, verify the host requirements and system prerequisites and set up the installation machine.

You must have the Device Manager agent installation folder ready for the new installation and configure the settings for basic setup by editing the `HDVMAgent.conf` file to provide basic setup values that are accessed during the unattended installation.

The `HDVMAgent.conf` file is stored in the following location:

- In Windows: *DVD-drive*`:\AGENTS\HDVM\Windows\HDVMAgent.conf`
- In UNIX: *DVD-ROM-mount-directory*`/AGENTS/HDVM/`*platform-name*`/HDVMAgent.conf`

Note:

If `HDVMAgent.conf` is stored on a write-protected medium such as an installation media, copy the directory that contains the file to a writable location and edit `HDVMAgent.conf`.

If a property is not specified, the default value is used. The following table shows these default values.

Table 35 Data set in HDVMAgent.conf

Property Name	Details	Default value
`serverIP` (required)	Specify the IP address or host name of the Device Manager server.	None
`serverPort` (required)	Specify the port number of the Device Manager server.	`2001`
`HiScanPeriod` (required)	Specify the **`HiScan`** execution interval. ▪ `H`: Once an hour ▪ `D`: Once a day ▪ `W,SUN`: Once every Sunday ▪ `W,MON`: Once every Monday ▪ `W,TUE`: Once every Tuesday ▪ `W,WED`: Once every Wednesday ▪ `W,THU`: Once every Thursday ▪ `W,FRI`: Once every Friday ▪ `W,SAT`: Once every Saturday ▪ `N`: No interval	`D`
`HiScanSchedule` (optional)	If you specify a value other than `N` for `HiScanPeriod`, specify the timing for running the **`HiScan`** command using one of the following methods:	`2:30`

Property Name	Details	Default value
	To specify running the command at a scheduled time, use the following format: ▪ Once an hour: Specify the time as *mm*. ▪ Once a day: Specify the time as *hh*:*mm*. ▪ Once a week: Specify the time as *hh*:*mm*. To specify running the command at random times: Specify this option in an environment where multiple hosts are connecting to the Device Manager server to run the **HiScan** command at random times on the hosts. This can decrease Device Manager loads. Specify the **HiScan** start and end time in the following format: ▪ Once an hour: Specify the start and end time as *mm*-*mm*. ▪ Once a day: Specify the start and end time as *hh*:*mm*-*hh*:*mm*. ▪ Once a week: Specify the start and end time as *hh*:*mm*-*hh*:*mm*. If the start time is later than the end time, the end time is set for the next day or hour (example: 23:00-1:00 or 45-15). If the start time and the end time are the same, **HiScan** runs as if you had specified a scheduled time.	
`configOverwrite` (optional)	Specify whether to overwrite the settings during an overwrite installation. ▪ `enable`: Overwrite the settings ▪ `disable`: Do not overwrite the settings **Caution:** If you enable overwriting installation of the Device Manager agent, the user ID and password used for communication with the Device Manager server are set to the default.	`disable`

Property Name	Details	Default value
`firewallSetup` (optional)	Specify whether to register the port numbers used by the Device Manager agent in the list of firewall exceptions when performing a new installation in a Windows environment. ▪ `enable`: Register the port numbers ▪ `disable`: Do not register the port numbers If you specify `enable`, the following port numbers will be registered in the list of firewall exceptions: ▪ `24041/tcp` ▪ `24042/tcp` ▪ `24043/tcp` These port numbers are the default values for the following properties set in the `server.properties` file of the Device Manager agent. ▪ `server.agent.port` ▪ `server.http.port` ▪ `server.http.localPort`	`disable`

For a complete list of system requirements, see *Hitachi Command Suite System Requirements*.

Installing a Device Manager agent on a Windows host (unattended installation)

An unattended installation uses a script file (`HDvMAgent.conf`) that contains the necessary user input.

Procedure

1. Log on to the Windows operating system with administrator permissions.
2. Open a command or PowerShell window and move to the folder where the installer program (`setup.exe`) is located.

Note: To perform basic setup during installation:

a. Create a new folder in a folder protected by Administrator permissions.
b. Copy the entire folder that contains the files `setup.exe` and `HDvMAgent.conf` into the new folder.
c. Move to the new folder.

If the UAC function is enabled in Windows, use the command prompt window that you opened as an administrator.

3. Enter the following command:

   `start /WAIT setup.exe /s [`*`installation-destination-path-for-Device-Manager-agent`*`] [/u]`

   - Specify *`installation-destination-path-for-Device-Manager-agent`* for new installations only. If you omit this folder name, the Device Manager agent is installed in the default installation folder.
   - Specify `/u` to perform basic setup during installation.

   Caution: If you install Device Manager agent in a folder other than the default installation folder, specify a folder protected by Administrator permissions.

4. To verify the installation, enter the following command:

   `echo %ERRORLEVEL%`

   If the return value is 0x00, the installation completed successfully.

Installing the Device Manager agent on a UNIX host (unattended installation)

An unattended installation uses a script file (`HDvMAgent.conf`) that contains the necessary user input. When starting the installer from a DVD-ROM, these characters can be used in the mount path: A to Z, a to z, 0 to 9, underscores (_), forward slashes (/).

Procedure

1. Log in to the UNIX operating system as the root user.
2. Open a shell window, and change the directory to the location of the installer program (`install.sh`).

   Note: To perform basic setup during installation, change the directory to the location where the `install.sh` and `HDvMAgent.conf` files have been copied.

3. Enter the following command:
   - In Solaris, AIX, or HP-UX:

     # install.sh -s [-u]
   - In Linux:

     # install.sh -s [-u] [-instpath *installation-destination-path-for-Device-Manager-agent***]**

   Specify *installation-destination-path-for-Device-Manager-agent* for new installations. If you omit this folder name, the Device Manager agent is installed in the default installation directory.

   Specify the `-u` option to perform basic setup during installation.
4. To check the success of the installation, enter the following command:

   # echo $?

   If the return value is 0x00, the installation completed successfully.

Verifying Device Manager agent unattended installations

When unattended installation of the Device Manager agent completes, check the returned values.

You can verify the returned values listed in the following table to determine the result.

Table 36 Device Manager agent unattended installation returned values

Return value (hexadecimal)	Description	Action
`0x00`	Ended normally.	None.
`0x90`	A failure occurred during the installation of the Device Manager agent.	The following are likely causes: ▪ There is insufficient free disk space. Secure the required disk space and perform the installation again. ▪ The host operating system is not supported. Verify that the operating system is supported.

Return value (hexadecimal)	Description	Action
		▪ A program other than Device Manager agent is being installed or removed. Wait for the current process to finish and perform the installation again. ▪ The software that provides the Java execution environment cannot run. Verify that the updates required for the Device Manager agent have been applied to the host system. Also, make sure that the software that provides the Java execution environment is installed in the location indicated by the installation path specified in the property `server.agent.JRE.location` of the `server.properties` file. In UNIX, the following causes are also possible: ▪ The software that provides a Java execution environment is not installed. Install the software, then retry installing the Device Manager agent. ▪ The permission for the installer execution file could not be changed. Move all files and subdirectories in the directory where the installer execution file location to a directory where the permission can be changed, and then run the installation again.
`0x91`	The installation command contains a syntax error.	The syntax of the installation command argument is incorrect. Correct the syntax, and then perform the installation again.
	The specified value for the installation directory is not correct.	The installation directory has been specified using characters that cannot be used, or exceeds 64 bytes. Correct the setting, and then perform the installation again.

Return value (hexadecimal)	Description	Action
`0x92`	`HDVMAgent.conf` is not stored in the directory in which the installer execution file is stored, or `HDVMAgent.conf` contains some setting errors.	Installation failed. Perform the following, depending on the cause of the error: ▪ `HDVMAgent.conf` is not stored in the directory in which the installer execution file is stored. Store `HDVMAgent.conf` in the directory in which the installer execution file is stored and run the installation again. ▪ `HDVMAgent.conf` contains some setting errors. Correct the errors and run the installation again.
`0x93`	The Device Manager agent was successfully installed, but the settings for linking to other program products could not be applied.	For an environment in which Protection Manager Console has been installed, run the `hptmguiinst.exe` or `hptmguiinst.sh` command. Check the error message, take the appropriate action to correct the error, and then perform the installation again. If the error persists, contact maintenance personnel for assistance.
`0x95`	The Device Manager agent functionality setup succeeded. However, an error might have occurred while setting up Replication Manager application agent functionality.	Verify that the operating system is supported and the required updates have been applied, and then perform installation again.
`0x96`	The user attempting this operation does not have Administrator permissions.	Retry the operation using a user ID with Administrator permissions.

Return value (hexadecimal)	Description	Action
`0x98`	You cannot downgrade the Device Manager agent because a newer version of the Device Manager agent is installed.	None.
`0x99`	The Device Manager agent or a related program is running.	Take action by following the KAIC25111-W to KAIC25113-W messages.
`0x9A`	`setup.exe` might not have started correctly, or a user might have run an internal command manually.	Take action by following the KAIC25156-E message.
`0x9D`	A failure occurred while connecting to the Device Manager server specified in `HDVMAgent.conf`.	Use the **`hdvmagt_setting`** command to specify the IP address or host name of the Device Manager server again.

Device Manager agent unattended removal

The unattended removal of an agent eliminates the need for user responses during agent removal. This function is useful when agents are installed on multiple hosts.

To perform an unattended agent removal, you create and run a script file.

Removing a Device Manager agent from a Windows host (unattended removal)

You can perform an unattended Device Manager agent removal in a Windows environment.

Procedure

1. Log in to the Windows operating system with a user ID that has administrator permissions.

2. Copy the following file to any location:

   installation-destination-path-for-Device-Manager-agent\bin\agent_uninstShortcut.bat

3. Run the following command at the command prompt:

   copy-destination-folder\agent_uninstShortcut.bat /s

   If the UAC function is enabled in Windows, use the command prompt window that you opened as an administrator.

4. To verify removal, enter the following command:

   echo %ERRORLEVEL%

   If the returned value is 0x00, the Device Manager agent is removed.

5. Delete the copy of **agent_uninstShortcut.bat** you made in step 2.

Removing a Device Manager agent from a UNIX host (unattended removal)

You can perform an unattended Device Manager agent removal in a UNIX environment.

Procedure

1. Log in to UNIX as the root user.
2. Open a shell, and enter the following command:
   - In Solaris or HP-UX:

     /opt/HDVM/HBaseAgent/bin/**.uninstall.sh -s**
   - In AIX:

     /usr/HDVM/HBaseAgent/bin/**.uninstall.sh -s**
   - In Linux:

     installation-destination-path-for-Device-Manager-agent

     /bin/.uninstall.sh -s
3. To check the success of the removal, enter the following command:

   #echo $?

   If the value returned is 0x00, the Device Manager agent is successfully removed.

Verifying the Device Manager agent unattended removal

When the unattended removal of the Device Manager agent completes, check the returned values and verify them against the following table.

Table 37 Device Manager agent unattended removal returned values

Return value (hexadecimal)	Description	Action
0x00	Normal termination	--
0x90	Removing the Device Manager agent failed.	The following are likely causes: ▪ A program other than the Device Manager agent is either being installed or removed. Wait for the current process to finish, and then attempt to remove the Device Manager agent again. ▪ A process for removing a related program failed. ▪ The software that provides the Java execution environment cannot run. Verify that the updates required for the Device Manager agent have been applied to the host system. Verify that the software that provides the Java execution environment is installed in the location specified in property `server.agent.JRE.location` of the `server.properties` file.
0x91	The command entered to remove the agent software contains a syntax error.	The syntax of the command argument is not correct. Correct the syntax, and then repeat the command.
0x93	A failure occurred while removing a program other than the Device Manager agent	The failure may have occurred when the Global Link Manager agent was being removed. Try to remove it again.
0x96	The user attempting this operation does not have Administrator permissions.	Retry the operation by using a user ID that has Administrator permissions.

Return value (hexadecimal)	Description	Action
0x99	The Device Manager agent or a related program is running.	Follow the KAIC25111-W to KAIC25113-W messages and act accordingly.
0x9B	The current directory is in the Device Manager agent installation directory. This return value may be displayed in UNIX.	Move the current directory to another directory, such as the `root` directory, and then try to remove the Device Manager agent again.

Appendix B: Hitachi Command Suite ports

This appendix describes the ports used for Hitachi Command Suite. For a complete list of system requirements, see *Hitachi Command Suite System Requirements*.

HCS server ports

Ensure that HCS ports do not overlap with those used by other programs on the management server.

Some ports can overlap with ports temporarily assigned by the operating system. You can prevent this overlap by defining the ports in the operating system `services` file.

These ports are described in the following table.

For more information, see the *Hitachi Command Suite Administrator Guide*.

Table 38 Port numbers used by HCS

Port Number	Description	If the port is in use by another product, do the following:
`162/udp`	Device Manager ports	The settings cannot be changed from Device Manager. Change the settings for the product that uses this port or follow the message that is output during installation to disable SNMP trap reception.
`2001/tcp` `2443/tcp`		Change the settings for the product that uses this port or change Device Manager settings before starting the Device Manager server.

Port Number	Description	If the port is in use by another product, do the following:
		If another product is using this port, the following message is output to the event log file and Device Manager does not start: `KAIC00114-E An attempt to start the HTTP server on port "port-number" failed.`

`5988/tcp`
`5989/tcp`
`23055/tcp`
		Change the settings for the product that uses this port or change Device Manager settings.

`20352/tcp`	Tiered Storage Manager ports	Change the settings for the product that uses this port or change Tiered Storage Manager settings.

`22015/tcp`
`22016/tcp`
`22032/tcp`
`22121/tcp to 22124/tcp`
	Common Component ports	Change the settings for the product that uses this port or change Common Component settings.
		Note: If Common Component is installed and you changed its ports, you do not need to reset the values.

`22031/tcp`	Common Component port when the management server operating system is Windows	Change the settings for the product that uses this port or change Common Component settings.

`22098/tcp`
`22099/tcp`
`22100/tcp`
	Host Data Collector ports	Change the settings for the product that uses this port or change Host Data Collector settings.

Glossary

capacity

The amount of data storage space available on a physical storage device, generally measured in bytes (MB, GB, TB, and so on).

CCI

See Command Control Interface.

CLI

command line interface

Command Control Interface (CCI)

Software used to control volume replication functionality (such as TrueCopy or ShadowImage) by means of commands issued from a host to a storage system. A command device must be set up in the storage system to enable the storage system to receive commands from CCI.

In an open system, Replication Manager uses the CCI configuration definition files to modify copy pair configurations and to acquire configuration information. Copy pair modification processing, such as splitting and resynchronizing copy pairs, is executed on the storage system via CCI.

copy pair

A primary and secondary volume pair linked by the volume replication functionality of a storage system. The primary volume contains original data, and the secondary volume contains the copy of the original.

Copy operations can be synchronous or asynchronous, and the volumes of the copy pair can be located in the same storage system (local copy) or in different storage systems (remote copy).

CSV

comma-separated values

DEVN

Device number that is assigned to each logical address when using an LDEV on a mainframe host.

HTTP

Hypertext Transfer Protocol

HTTPS

Hypertext Transfer Protocol Secure

Internet protocol (IP)

The protocol that governs the breakup of data messages into packets (units of data), the routing scheme for transmitting them, and the reassembly of the packets into the original data messages at the destination. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a source and a destination.

IOPS

I/Os per second

IP

See Internet protocol.

JRE

Java Runtime Environment

logical device (LDEV)

A volume created in a storage system. See also LU.

logical group

A user-defined collection of managed resources (hosts and volumes) that are grouped according to business operations, geographic locations, or other organizational divisions. Logical groups can be *public* or *private*:

- Public logical groups are accessible by any HCS user.
- Private logical groups are accessible only by HCS users who belong to user groups that are associated with the logical group.

logical unit (LU)

A volume, or LDEV, created in an open storage system, or configured for use by an open-systems host, for example, OPEN-V.

logical unit number (LUN)

A unique management number that identifies a logical unit (LU) in a storage system. A logical unit can be an end user, a file, a disk drive, a port, a host group that is assigned to a port, an application, or virtual partitions (or volumes) of a RAID set.

Logical unit numbers (LUNs) are used in SCSI protocols to differentiate disk drives in a common SCSI target device, such as a storage system. An open-systems host uses a LUN to access a particular LU.

LU

See logical unit.

LUN

See logical unit number.

management client

A computer used to operate a graphical user interface client or a command-line interface client.

NAS

Network attached storage

NIC

Network interface card

pair status

Indicates the condition of a copy pair. A pair must have a specific status for specific operations. When a pair operation completes, the status of the pair changes to a different status determined by the type of operation.

path

A path from a storage system volume to a host group.

In this manual, the term "path" may mean a path, external path, or LUN path without making distinctions among them.

primary volume (P-VOL)

In a volume pair, the source volume that is copied to another volume using the volume replication functionality of a storage system. The data on the P-VOL is duplicated synchronously or asynchronously on the secondary volume (S-VOL).

properties file

A file that defines aspects of the operating environment. The operating environment can be modified by changing the appropriate properties file.

RAID

redundant array of independent disks

A collection of two or more disk drives that presents the image of a single logical disk drive to the system. Part of the physical storage capacity is used to store redundant information about user data stored on the remainder of the storage capacity. In the event of a single device failure, the data can be read or regenerated from the other disk drives.

RAID employs the technique of disk striping, which involves partitioning each drive's storage space into units ranging from a sector (512 bytes) up to several megabytes. The stripes of all the disks are interleaved and addressed in order.

resource group

A collection of resources that are grouped by one or more system resource types.

role

Permissions that are assigned to users in a user group to control access to resources in a resource group. Resource groups can be assigned to different user groups with different roles.

S-VOL

See secondary volume.

SAN

See storage area network.

secondary volume (S-VOL)

After a backup, the volume in a copy pair that is the copy of the original data on the primary volume (P-VOL). Recurring differential data updates keep the data in the S-VOL consistent with the data in the P-VOL.

Secure Sockets Layer (SSL)

A common protocol for managing the security of message transmission over the Internet.

Two SSL-enabled peers use their private and public keys to establish a secure communication session, with each peer encrypting transmitted data with a randomly generated and agreed-upon symmetric key.

SMU

System Management Unit

SNMP

Simple Network Management Protocol

storage area network (SAN)

A network of shared storage devices that contain disks for storing data.

system drive

The basic (logical) storage element that is managed by the Hitachi NAS Platform family of products. A system drive is equivalent to a storage system volume.

tiered storage

A layered structure of performance levels, or tiers, that matches data access requirements with the appropriate performance tiers.

user group

A collection of users who have access to the same resources and have the same permissions for those resources. Permissions for users are determined by the user groups to which they belong. Users and resource groups can be assigned to multiple user groups.

VOLSER

The label of a volume assigned by the mainframe host.

volume (vol or VOL)

A name for the logical device (LDEV), or logical unit (LU), or concatenated LDEVs, that are created in a storage system that have been defined to one or more hosts as a single data storage unit.

web client

An application that is used on a client machine to access a server on which management software is installed. A web client contains two parts: dynamic web pages and the web browser.

Index

H

I

J

K

L

M

N

P

R

S

T

U

V

W

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact