HITACHI
Inspire the Next

Hitachi Command Suite

Compute Systems Manager

Installation and Configuration Guide

Hitachi Data Systems

MK-91HC195-15

Contents

Preface

This manual describes how to install and configure Hitachi Compute Systems Manager (HCSM).

Intended audience

This document provides instructions for server administrators.

Product version

This document revision applies to Hitachi Compute Systems Manager (HCSM) v8.2.0.

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.

Referenced documents

Hitachi Compute Systems Manager documents:

- *Hitachi Command Suite Compute Systems Manager User Guide,* MK-91HC194
- *Hitachi Command Suite Compute Systems Manager CLI Reference Guide*, MK-91HC196
- *Hitachi Command Suite Compute Systems Manager Messages*, MK-91HC197
- *Hitachi Compute Systems Manager Release Notes*, RN-91HC198

Hitachi Data Systems Portal, https://portal.hds.com

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click **OK**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `copy` *`source-file target-file`* **Note:** Angled brackets (< >) are also used to indicate variables.
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`

Convention	Description
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `pairdisplay -g <group>` **Note:** Italic font is also used to indicate variables.
[ ] 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 or consequences (for example, disruptive operations).
	WARNING	Warns the user of severe conditions or consequences (for example, destructive operations).

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

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

Accessing product documentation

Product documentation is available on Hitachi Data Systems 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.

Getting help

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

Hitachi Data Systems Community is a global online community for HDS 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.hds.com, register, and complete your profile.

Comments

Please send us your comments on this document to doc.comments@hds.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 Data Systems Corporation.

Thank you!

1

Hitachi Compute Systems Manager overview

This module provides an overview of Hitachi Compute Systems Manager (HCSM).

- ☐ Hitachi Compute Systems Manager overview
- ☐ Hitachi Compute Systems Manager system configuration
- ☐ About related Hitachi Command Suite products
- ☐ Hitachi Compute Systems Manager overview workflow
- ☐ Installation and initial configuration workflows
- ☐ System configuration workflows
- ☐ Management and maintenance workflows

Hitachi Compute Systems Manager overview

This module provides an overview of the Hitachi Compute Systems Manager management software and the resources that the software manages.

About Hitachi Compute Systems Manager

Hitachi Compute Systems Manager, which is a part of the Hitachi Command Suite (HCS) line of products, helps you to manage and operate remotely distributed server resources in a large-scale system environment.

If you install Compute Systems Manager in an environment that uses Hitachi Command Suite products, you can centrally manage and operate storage and server resources. If you install Compute Systems Manager on the same server where Hitachi Device Manager is installed, the server automatically synchronizes information for hosts managed by Compute Systems Manager and Hitachi Device Manager.

You can streamline system setup and operations as follows:

- After installation, complete the required minimum settings by following the instructions that appear when you first log in to Compute Systems Manager from a management client.
- Configure the Compute Systems Manager system settings by using the Compute Systems Manager user interface.
- Manage Compute Systems Manager users by using an external authentication server.
- Use common Hitachi Command Suite functionality to centrally manage settings for users and security.

Related concepts

- About Hitachi Compute Systems Manager components on page 17
- About Hitachi Compute Systems Manager managed resources on page 16
- About basic system configuration on page 18
- About Hitachi Compute Systems Manager LAN configuration on page 19

About Hitachi Compute Systems Manager managed resources

Hitachi Compute Systems Manager enables you to manage and operate remote server resources in a large-scale system environment.

Remote resources are referred to as *management targets* until you add them to the Compute Systems Manager management system. After you add a target to the system, it becomes a *managed host* (server-specific) or *managed resource* (generic). Compute Systems Manager manages the following resources:

- Windows, Linux, and Solaris hosts
  Compute Systems Manager manages both physical and virtual Windows, Linux, and Solaris hosts.
- Hypervisors
  Compute Systems Manager manages both Hyper-V and VMware.
- Virtual machines (VMs)
  Compute Systems Manager manages virtual machines at the hypervisor level.
- Hitachi servers
  Hitachi blade servers and rack-mounted servers can be discovered. Hitachi manages blade servers at the chassis level.
- LPARs
  Compute Systems Manager manages LPARs at the blade server level.

Related concepts

- About Hitachi Compute Systems Manager on page 16
- About basic system configuration on page 18

Hitachi Compute Systems Manager system configuration

This module provides information about Hitachi Compute Systems Manager system components and basic system configuration.

Related concepts

- About Hitachi Compute Systems Manager LAN configuration on page 19

About Hitachi Compute Systems Manager components

Hitachi Compute Systems Manager consists of the following components:

- Management server
  The management server is a computer on which the Compute Systems Manager software is installed and runs. The Compute Systems Manager management system consists of the following components:
  - Hitachi Command Suite Common Component
    Provides functionality common to Hitachi Command Suite products and related to users and security.
  - Compute Systems Manager server
    Provides central management and operation of remote resources.
- Management clients
  A management client is a computer that runs either the Compute Systems Manager web-based user interface or the Command Line Interface (CLI). You access the web-based management user interface by using a browser. To access the CLI, download the CLI software and install it on the management client.
- Managed resources

Managed resources are hosts, servers, or other related systems that are managed from the management system.

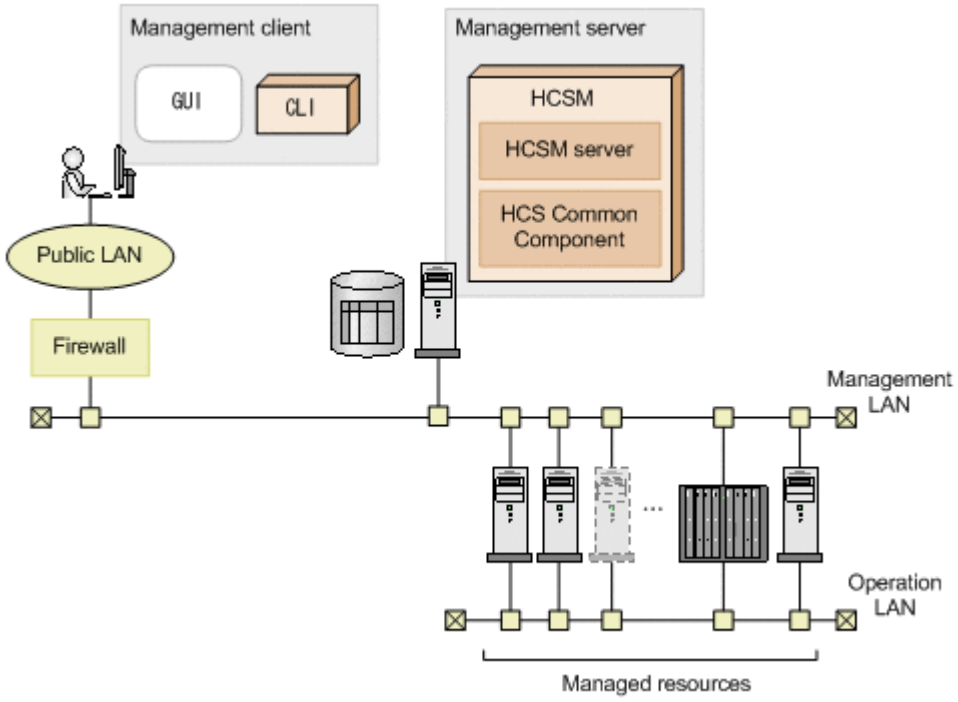
- LANs
  One or more local area networks that manage the TCP/IP connections between the management server and management clients, and managed resources.

Related concepts

- About Hitachi Compute Systems Manager on page 16
- About basic system configuration on page 18

About basic system configuration

Although there are various ways to set up your Hitachi Compute Systems Manager environment, the following figure shows the basic system configuration.



The basic system configuration environment is set up as follows:

- Compute Systems Manager is installed as a standalone product without any additional Hitachi Command Suite products.
- Users are managed with Compute Systems Manager instead of an external authentication server.
- Communication between management servers and management clients does not use SSL for secure communications.

Tip: IPv6 can be used for communication between the management server and chassis.

Related concepts

- About Hitachi Compute Systems Manager LAN configuration on page 19

About Hitachi Compute Systems Manager LAN configuration

When using Hitachi Compute Systems Manager, ensure that you set up separate operation and management LANs to reduce security risks.

When configuring your management LAN, use the following guidelines:

- Install a firewall between the public operation LAN and the management LAN.
- Do not mix traffic from the operation LAN with traffic from the management LAN.

About related Hitachi Command Suite products

Hitachi Compute Systems Manager is a part of the Hitachi Command Suite line of products, which includes the following components:

- Hitachi Device Manager
- Hitachi Tiered Storage Manager
- Hitachi Dynamic Link Manager
- Hitachi Replication Manager
- Hitachi Tuning Manager
- Hitachi Global Link Manager
- Hitachi Automation Director

If you install Compute Systems Manager on the same server as other Hitachi Command Suite products, you can use common settings to manage users and security. In addition, if Compute Systems Manager is installed on a server running Hitachi Device Manager, the host information managed by the two products is automatically synchronized, which improves host management work efficiency.

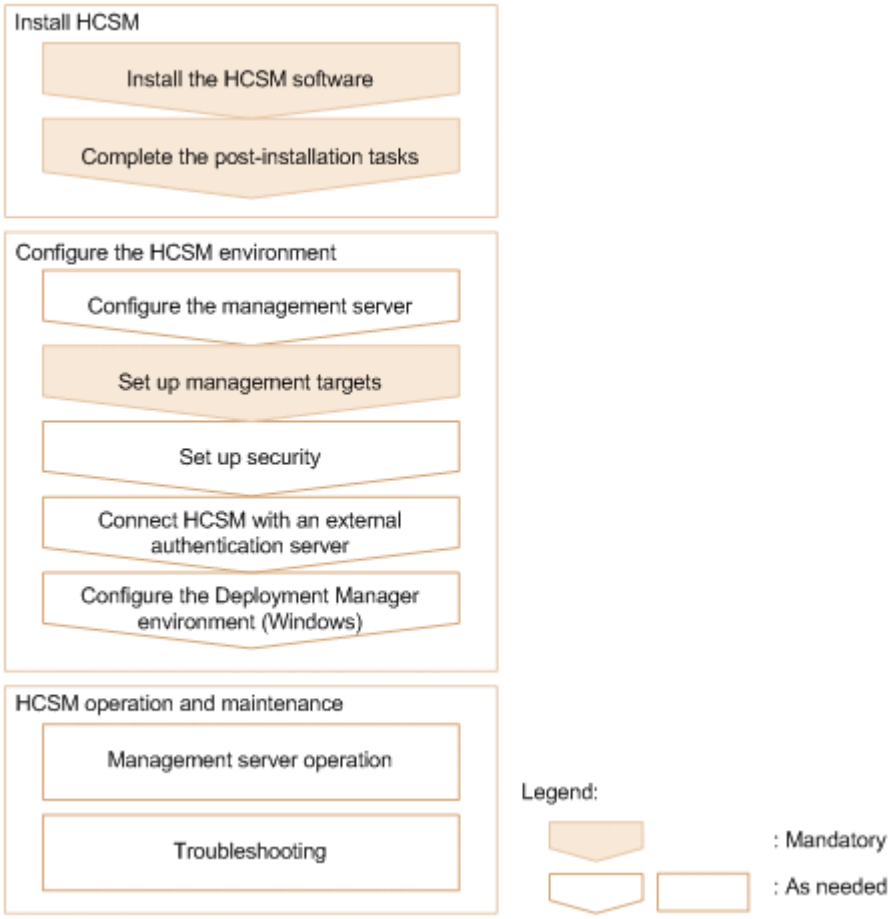
Note: Only the host information is synchronized when using both Compute Systems Manager and Hitachi Device Manager, not information for other types of resources.

Related concepts

- About Hitachi Compute Systems Manager on page 16

Hitachi Compute Systems Manager overview workflow

The following figure illustrates an overview workflow, which includes installing, configuring, and using Hitachi Compute Systems Manager.



This manual includes system installation, setup, management, and maintenance information. For details about managing resources, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Related concepts

- Installation workflow on page 21
- Post-installation workflow on page 21
- SNMP trap setup workflow on page 23
- Managed host setup workflow on page 23
- Workflow for setting up secure communication with managed servers on page 27
- Workflow for setting up secure communication with a Device Manager server on page 27
- Workflow for setting up secure communication with management clients on page 25
- Workflow for setting up secure communication with an SMTP server on page 26
- Workflow for setting up secure communication with an LDAP directory server on page 28
- Workflow for setting up a Kerberos authentication server on page 29

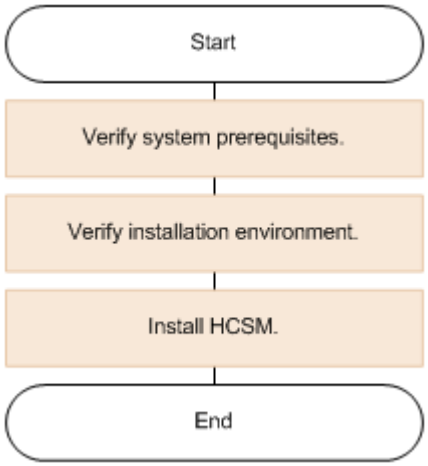
- Database management workflow on page 32
- Workflow for setting up an LDAP directory server on page 28
- Management server migration workflow on page 31
- Workflow for updating the network configuration on page 33
- Troubleshooting workflow on page 34

Installation and initial configuration workflows

This module provides workflows for Hitachi Compute Systems Manager installation and initial configuration.

Installation workflow

The following figure illustrates the workflow for installing Hitachi Compute Systems Manager.

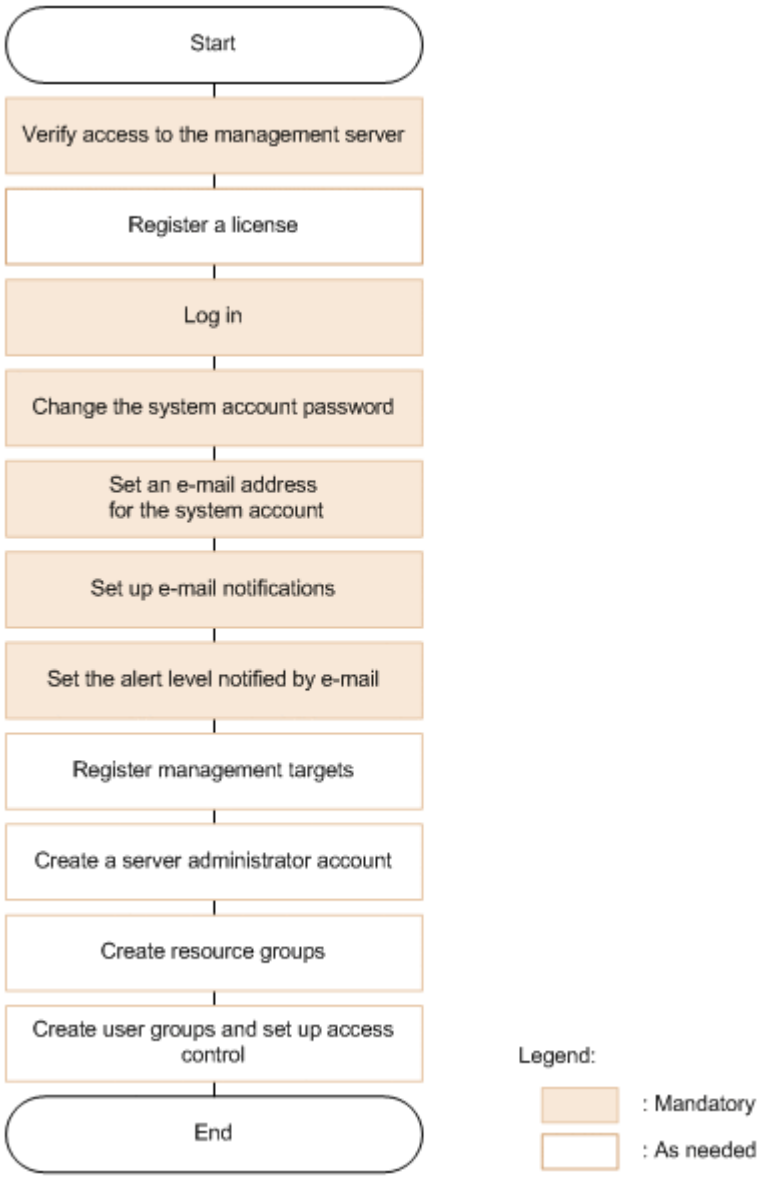


Related concepts

- Post-installation workflow on page 21
- Managed host setup workflow on page 23
- About installing Hitachi Compute Systems Manager on page 46
- About verifying system prerequisites on page 38

Post-installation workflow

The following figure illustrates the Hitachi Compute Systems Manager post-installation tasks that enable you to finish the initial setup.



Related concepts

- About Hitachi Compute Systems Manager post-installation tasks on page 51
- Managed host setup workflow on page 23

Related tasks

- Verifying access to the management server on page 52
- Registering a license on page 53
- Changing the System account password on page 54
- Setting an e-mail address for the System account on page 54
- Setting up e-mail notifications on page 55
- Setting up the alert level for e-mail notifications on page 55
- Adding resources to Hitachi Compute Systems Manager on page 56

- Creating a server administrator account on page 57
- Creating resource groups on page 58
- Creating user groups and setting up access control on page 58

System configuration workflows

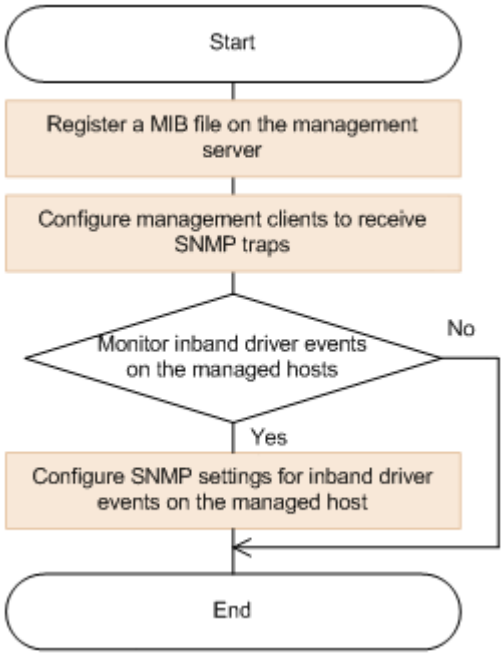
This module provides workflows for Hitachi Compute Systems Manager system configuration.

SNMP trap setup workflow

To enable Hitachi Compute Systems Manager to receive SNMP traps sent from managed hosts, you need to configure the settings for SNMP traps on both the management server and management clients.

To send inband driver events that occurred on a managed host, you also need to configure the SNMP settings for inband driver events on the managed host.

The following figure show the workflow for configuring SNMP traps:



Related concepts

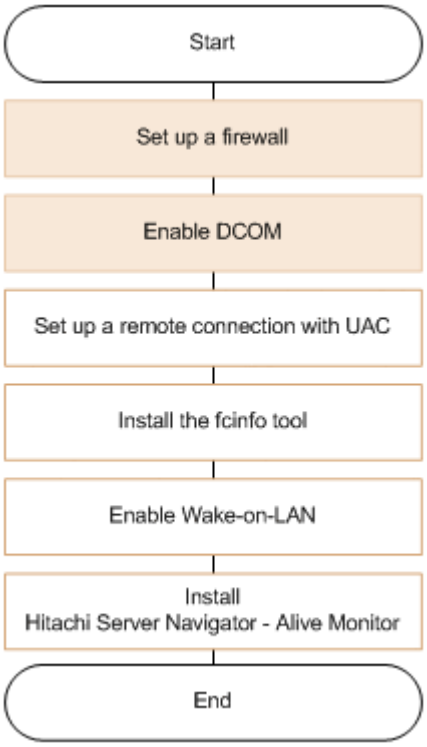
- About SNMP trap settings on page 66
- About monitoring inband SNMP traps on page 67

Managed host setup workflow

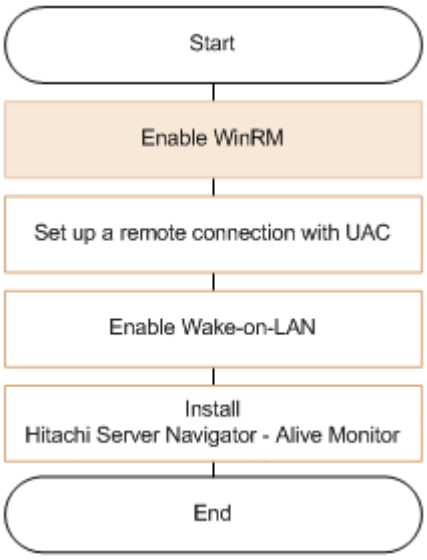
As part of the post-installation workflow, you must set up the managed hosts that you plan to manage using Hitachi Compute Systems Manager. You can

manage physical and virtual hosts. The required tasks differ depending on the management server or the host operating system.

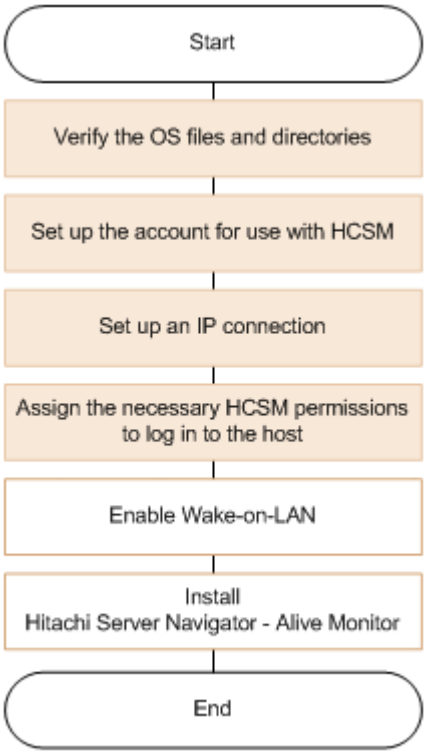
The following figure illustrates the management target setup workflow for a Windows host and a Windows management server:



The following figure illustrates the management target setup workflow for a Windows host and a Linux management server:



The following figure illustrates the management target setup workflow for a Linux or Solaris host:



Related tasks

- Enabling Wake-on-LAN on page 90
- Enabling DCOM for Windows hosts on page 94
- Enabling WinRM on Windows hosts on page 94
- Setting up a remote connection with UAC on Windows Server 2008 or 2012 on page 95

Related references

- Prerequisites for managing Windows hosts on page 91
- Prerequisites for managing Linux or Solaris hosts on page 98

Secure communications workflows

This module provides workflows for setting up secure communications between the management server and the management clients, SMTP server, and external authentication server.

Workflow for setting up secure communication with management clients

To set up secure communications between the management server and the management clients, you must first complete a set of tasks on the management server to obtain a certificate and enable Secure Socket Layers (SSL). After you finish the set up on the management server, you must install the certificate on each management client and complete the configuration.

The following figure illustrates the basic workflow for setting up secure communications between the management server and management clients.

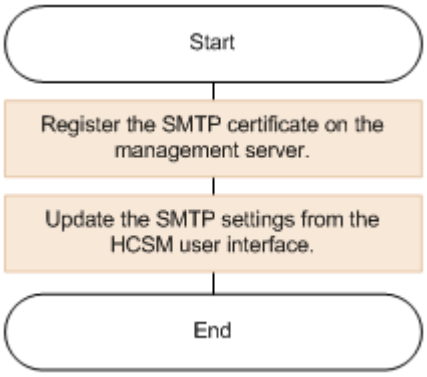
Related tasks

- Setting up SSL on the server for secure client communication on page 115
- Setting up SSL on web-based management clients on page 121
- Setting up SSL on management clients running the CLI on page 122

Workflow for setting up secure communication with an SMTP server

To set up secure communications between the management server and the SMTP server, you must add the SMTP server certificate to the management server and then modify the SMTP setting from the Hitachi Compute Systems Manager user interface.

The following figure illustrates the basic workflow for setting up secure communications between the management server and the SMTP server.



Related concepts

- About using an external authentication server on page 134

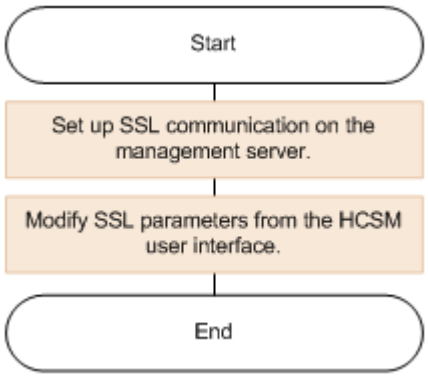
Related tasks

- Setting up SSL for communicating with the SMTP server on page 124

Workflow for setting up secure communication with managed servers

Communication between Hitachi servers and the management server uses SSL by default so that no additional configuration is required. However, if you want to strengthen security for alerts sent from the chassis to Hitachi Compute Systems Manager, you can create a new self-signed certificate on the server and enable it from the Compute Systems Manager user interface.

The following figure illustrates the basic workflow for increasing communication security for alerts sent from the server to the management server.



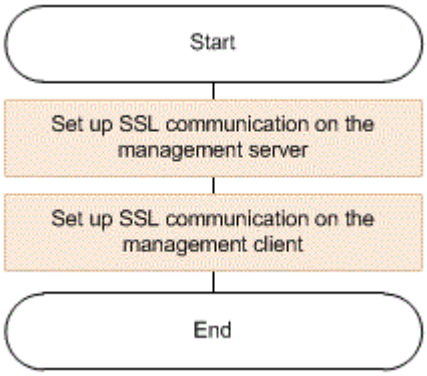
Related concepts

- About secure communications for management clients on page 115

Workflow for setting up secure communication with a Device Manager server

You can set up secure communications between the Hitachi Compute Systems Manager management server and the Hitachi Device Manager server.

The following figure illustrates the basic workflow for setting up secure communications between the management server and the Device Manager server:



Related concepts

- About secure communications for the Device Manager server on page 129

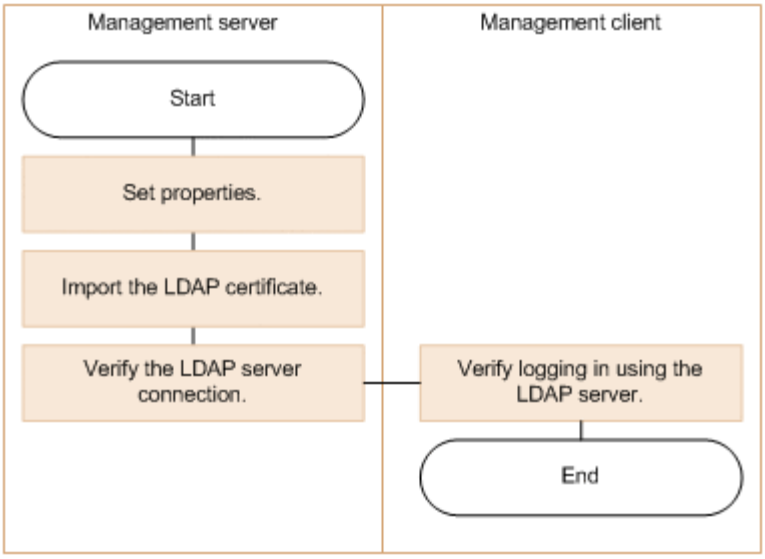
Related tasks

- Setting up SSL for communicating with the Device Manager server on page 130

Workflow for setting up secure communication with an LDAP directory server

To set up secure communications between the management server and an external LDAP server, you must add the LDAP server certificate to the management server and then verify communication.

The following figure illustrates the basic workflow for setting up secure communications between the management server and the LDAP directory server.



Related concepts

- About setting up secure communication for an external authentication server on page 131

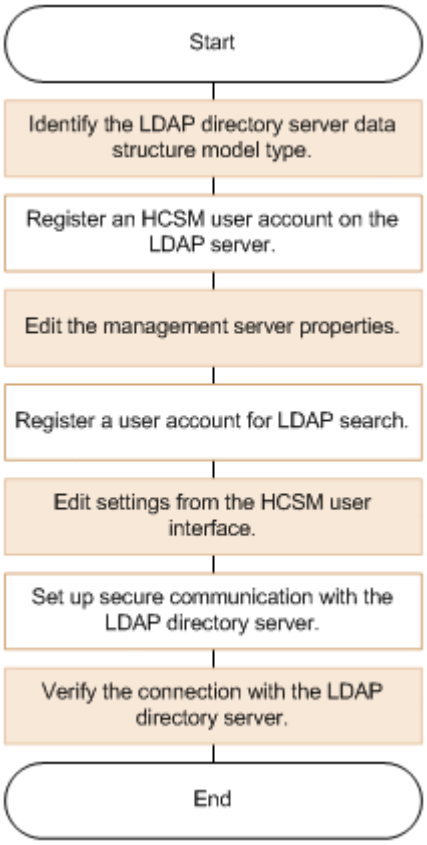
Related tasks

- Configuring SSL for a secure LDAP server connection on page 141

Workflow for setting up an LDAP directory server

To set up an LDAP directory server for authentication, you must check the LDAP data structure and register a Hitachi Compute Systems Manager user account for use with the LDAP directory server. In addition, based on the information in the LDAP directory server, you must specify connection settings on the management server and use the Compute Systems Manager interface to register a user account or set permissions for operations.

The following figure illustrates the basic workflow for setting up an LDAP directory server for Compute Systems Manager authentication.



Related concepts

- About using an external authentication server on page 134

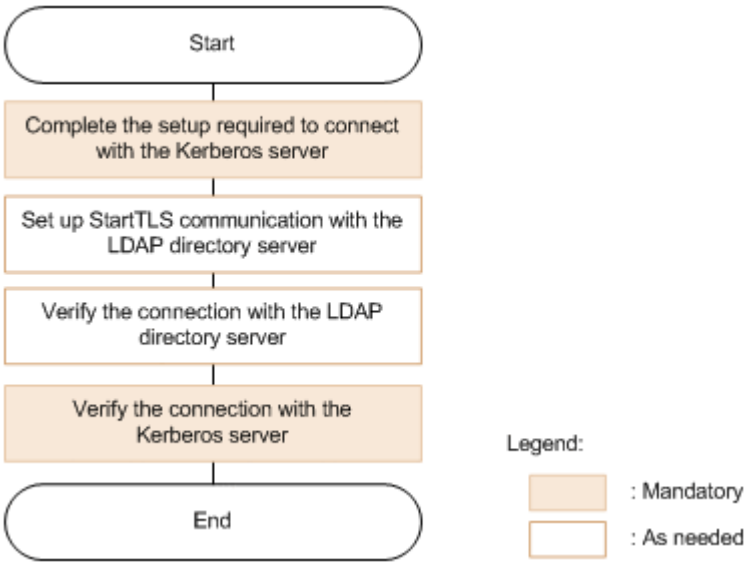
Related tasks

- Configuring an LDAP server connection on page 139
- Configuring SSL for a secure LDAP server connection on page 141
- Verifying an LDAP server connection on page 143

Workflow for setting up a Kerberos authentication server

To set up a Kerberos server for authentication, you must register a Hitachi Compute Systems Manager user account and specify connection settings on the management server and the Compute Systems Manager interface.

The following figure illustrates the basic workflow for setting up a Kerberos server for Compute Systems Manager authentication.



Related concepts

- About using an external authentication server on page 134

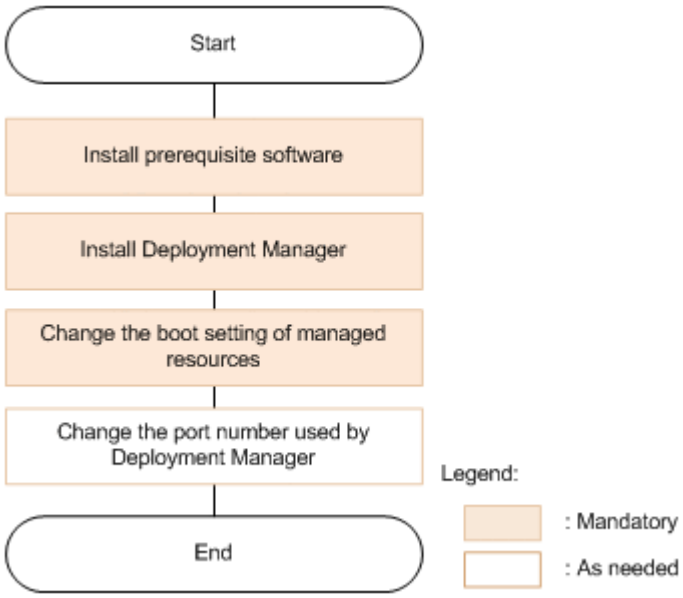
Related tasks

- Configuring a Kerberos server connection on page 144
- Verifying a Kerberos server connection on page 146

Deployment Manager configuration workflow

The following figure illustrates the basic workflow for setting up the Deployment Manager on the management server. Deployment Manager can be installed when installing Hitachi Compute Systems Manager.

Deployment Manager can only be used when the management server is running Windows.



Related concepts

- About Deployment Manager environment settings on page 166

Related tasks

- Installing Deployment Manager on page 169
- Configuring managed resources for use with Deployment Manager on page 170
- Changing the Deployment Manager port number on page 171

Related references

- Prerequisites for installing Deployment Manager on page 166

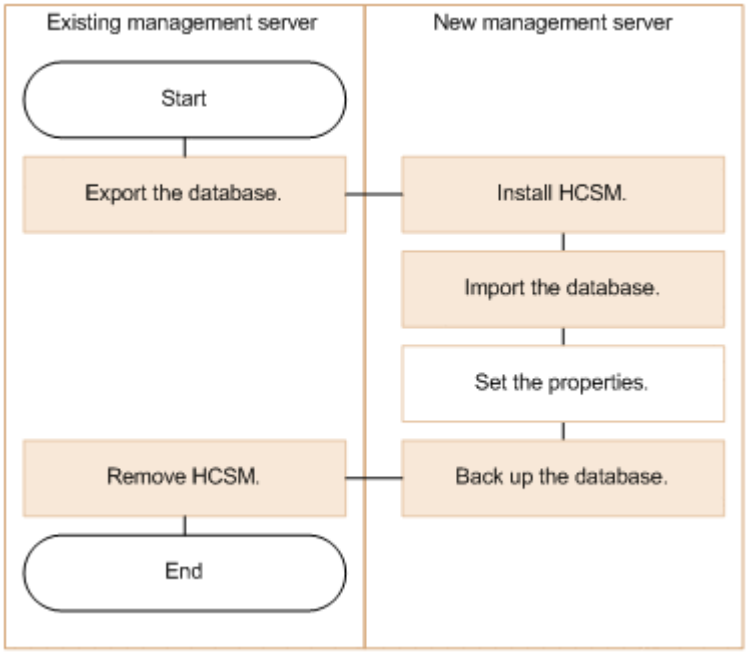
Management and maintenance workflows

This module provides workflows for administering the management server.

Management server migration workflow

To migrate an existing Hitachi Compute Systems Manager management server to a different server, you must install Compute Systems Manager on a new server, and then transfer the database from the existing server.

The following figure illustrates the basic workflow for migrating from an existing management server to a new server.



Related concepts

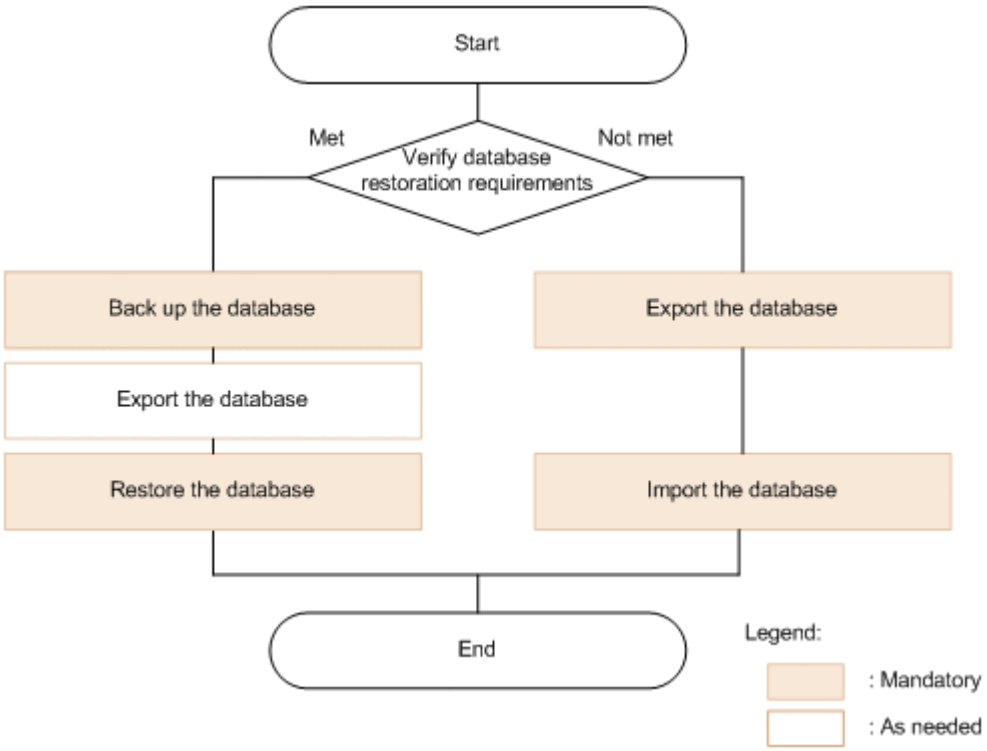
- About database management on page 179

Database management workflow

When using Hitachi Compute Systems Manager, you can manage database information in the following ways:

- Back up database information
- Restore database information
- Export database information to a file
- Import database information from a file

The following figure illustrates the basic workflow for managing the Compute Systems Manager database.



Related concepts

- About database management on page 179

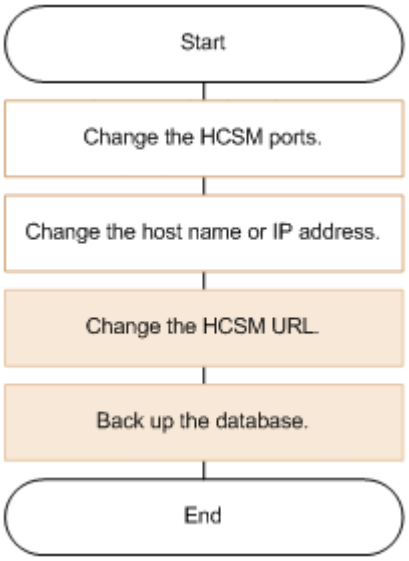
Related tasks

- Backing up the database on page 181
- Exporting the database on page 184
- Restoring the database on page 182
- Importing the database on page 185

Workflow for updating the network configuration

If you change your network configuration, you must also update the Hitachi Compute Systems Manager management server settings.

The following figure illustrates the basic workflow for updating the management server after you implement network configuration changes.



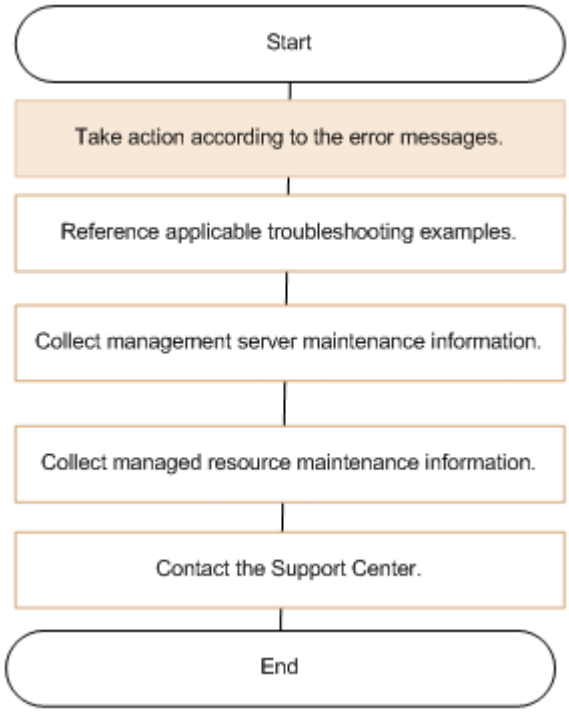
Related tasks

- Changing Hitachi Compute Systems Manager ports on page 74
- Changing the management server host name or IP address on page 75
- Changing the management server URL on page 79
- Backing up the database on page 181

Troubleshooting workflow

When using Hitachi Compute Systems Manager, if the system does not function properly, you might have to troubleshoot the system.

The following figure illustrates the basic workflow for troubleshooting Compute Systems Manager.



Related concepts

- Troubleshooting overview on page 254

2

Installing Hitachi Compute Systems Manager

This module describes how to install, set up, and remove Hitachi Compute Systems Manager (HCSM).

- ☐ Verifying system prerequisites required for installation
- ☐ Verifying the installation environment
- ☐ Installing Hitachi Compute Systems Manager
- ☐ Post-installation tasks
- ☐ Removing Hitachi Compute Systems Manager

Verifying system prerequisites required for installation

This module provides information about the system prerequisites that you must verify before installing Hitachi Compute Systems Manager (HCSM).

About verifying system prerequisites

Before installing Hitachi Compute Systems Manager, you must verify that your environment meets all prerequisites. These include network setup, and hardware and software requirements. You also need to consider whether to install Deployment Manager as well at this time, because it can be installed during the Compute Systems Manager installation.

Note: You must have Windows administrator permissions in Windows or be logged in as the root user in Linux to complete the installation and configuration tasks included in this guide.

Related concepts

- About verifying the installation environment on page 41

Related tasks

- Verifying the system prerequisites on page 38
- Avoiding port conflicts on page 38
- Verifying the server time setting on page 40
- Adding the management server host name to the hosts file (Linux) on page 39
- Configuring kernel parameters and shell restrictions (Linux) on page 39
- Verifying requirements when using IPv6 on page 40
- Registering firewall exceptions (Linux) on page 40

Verifying the system prerequisites

Before installing Hitachi Compute Systems Manager, you must verify that your environment and the management server meet all hardware and software prerequisites. For details about system requirements, see the Release Notes.

Related concepts

- About verifying system prerequisites on page 38

Avoiding port conflicts

Before a new installation of Hitachi Compute Systems Manager, verify that the ports used by Compute Systems Manager on the management server are not in use by other products. If a port is in use by another product, neither product may operate correctly.

To ensure that the necessary ports are not in use, use the **netstat** command.

Note: Compute Systems Manager uses the 162 UDP port to receive SNMP traps. If a product other than Compute Systems Manager is currently using this port, a message is displayed during installation that recommends changing the port. Before continuing with the installation, you must change the port for the other product using port 162 UDP or change the port used by Compute Systems Manager by following the instructions provided in the message. When you finish making the port change, you can proceed with the installation.

When you use the all-in-one installer, the port is automatically changed to 22601.

Related concepts

- About verifying system prerequisites on page 38

Related references

- Hitachi Compute Systems Manager server ports on page 286
- Hitachi Command Suite Common Component ports on page 286

Adding the management server host name to the hosts file (Linux)

Before you install Hitachi Compute Systems Manager on a server running Linux, you must add localhost and the host name of the management server in the `/etc/hosts` file.

If localhost and the management server hostname are not in the `/etc/hosts` file, an error might occur during installation.

Related concepts

- About verifying system prerequisites on page 38

Configuring kernel parameters and shell restrictions (Linux)

Before you install Hitachi Compute Systems Manager on a server running Linux, you must configure kernel parameters and shell restrictions. For more information about which kernel parameters to set and the values for shell restrictions, see the Release Notes.

To configure kernel parameters and shell restrictions, complete the following tasks:

1. Before modifying any files, create backup files for all files that contain kernel parameters and shell restrictions.
2. Determine the new values to enter for each parameter.
3. Open the required files and modify the values as needed.
4. Restart the operating system.

Related concepts

- About verifying system prerequisites on page 38

Registering firewall exceptions (Linux)

In the firewall exceptions list, register the port number for use with Hitachi Compute Systems Manager.

Related concepts

- About verifying system prerequisites on page 38

Related tasks

- Registering management server firewall exceptions (Linux) on page 86

Verifying requirements when using IPv6

Hitachi Compute Systems Manager supports IPv6 communication between the management server and chassis.

Before using IPv6, confirm that the management server supports both IPv6 and IPv4. IPv4 is required for communications with other managed resources including internal communications.

Verifying the server time setting

All Hitachi Compute Systems Manager task and alert occurrence times are based on the management server time setting. Therefore, it is important that you verify the accuracy of the server operating system time setting and reset it if necessary before installing Compute Systems Manager. If you change the management server time while the Hitachi Command Suite Common Component and Hitachi Command Suite product services are running, Compute Systems Manager may not operate correctly.

If you plan to use a service such as NTP that automatically adjusts the server time, you must configure the service as follows:

- Configure the settings so that the time is adjusted gradually when the service discovers a time discrepancy.
- The service adjusts the time setting gradually only as long as the time difference remains within a certain range. Based on the maximum range value, set the frequency so that the time difference never exceeds the fixed range.
  An example of a service that can adjust the time gradually as long as the time difference does not exceed a fixed range is the Windows Time service.

Note: When running Compute Systems Manager in a U.S. or Canadian time zone, you must configure the management server operating system so that it supports the new Daylight Savings Time (DST) rules. Compute Systems

Manager cannot support the new DST rules unless the server provides support.

Related concepts

- About verifying system prerequisites on page 38

Related tasks

- Resetting the management server time setting manually on page 82

Related references

- Conditions that require resetting the management server time setting on page 82

Verifying the installation environment

This module provides information about verifying the Hitachi Compute Systems Manager server environment and recording required information before installation.

Related concepts

- About verifying the installation environment on page 41

Related tasks

- Preparing the installation directories on page 44
- Specifying management server information during installation on page 45

Related references

- Rules for specifying path names on page 43

About verifying the installation environment

During the Hitachi Compute Systems Manager installation, the installation wizard prompts you for an installation directory, management server, and other installation-related information. Accept the default values that the wizard provides for all entries unless you have a specific installation scenario that requires modifying the default values. If your installation requires values other than the default, determine the required values and record them before you begin the installation.

The installation directories that you can specify and the default values are:

- Compute Systems Manager software (new installation)
  In Windows:
  Program-Files-folder\HiCommand
  (where *Program-Files-folder* is a system environment variable set in Windows)

Because Deployment Manager runs on x86 architectures, it is installed in a different directory from Compute Systems Manager. For programs to run on x86 architectures, *Program-Files-folder* is the same directory as is set for the *%ProgramFiles(x86)%* environment variable.

In Linux:

`/opt/HiCommand`

- Compute Systems Manager database (new installation)

  In Windows:

  HCSM-installation-folder`\database\x64\HCSM`

  In Linux:

  `/var/`*HCSM-installation-directory*`/database/x64/HCSM`

Note: If you change the database storage location, the installation program creates the x64 directory within the specified directory.

- Database backup directory (when installing Compute Systems Manager in an environment in which a Hitachi Command Suite product has already been configured)

  In Windows:

  HCSM-installation-folder`\ComputeSystemsManager_backup`

  When installing Compute Systems Manager by using the all-in-one installer, the default backup directory is:

  HCSM-installation-folder`\backup`

  In Linux:

  `/var/`*HCSM-installation-directory*`/backup`

Tip: Hitachi Command Suite Common Component is installed in the following directory by default.

In Windows:

HCSM-installation-folder`\Base64`

In Linux:

HCSM-installation-directory`/Base64`

If you install Compute Systems Manager on a server already running another Hitachi Command Suite product, the Common Component is always installed in the same location as the existing product.

Related tasks

- Specifying management server information during installation on page 45
- Preparing the installation directories on page 44

Related references

- Rules for specifying path names on page 43

Rules for specifying path names

During new Hitachi Compute Systems Manager installations, the installation wizard prompts you for the location of the installation and database directories. If you decide to install in a directory other than the default, you must determine the location and create the directory before beginning the installation.

When creating a Compute Systems Manager directory, ensure that directory path name adheres to the following rules:

- Character requirements:
  - In Windows, valid characters are: `A-Z a-z 0-9. _` space `\:`
  - In Linux, valid characters are: `A-Z a-z 0-9. _ /`
    Periods (.) can be used for the database installation path.
  - Installation path name cannot exceed 64 characters.
  - Database path name cannot exceed 90 characters.
  - Database backup path name cannot exceed 150 characters.
- Directory name and path requirements in Windows:
  - Directory name cannot contain consecutive spaces.
  - Do not include a period or space at the end of a directory name.
  - Do not include symbolic links or junctions.
  - Do not specify the directory directly under the drive (such as `D:\`).
  - Do not specify a network drive.
  - Do not use any of the following directories:
    Any directory or subdirectory specified by the `%ProgramFiles(x86)%` environment variable.
    Any directory or subdirectory specified by the `%CommonProgramFiles(x86)%` environment variable.
    Any directory or subdirectory under `%systemroot%\system32`.
    Any directory or subdirectory under `%systemroot%\SysWOW64`.
    (Windows Server 2012) Any directory or subdirectory under `%ProgramFiles%\WindowsApps`.
    `%ProgramFiles(x86)%`, `%CommonProgramFiles(x86)%`, `%ProgramFiles%` and `%systemroot%` are environment variables for Windows.
- Directory name and path requirements in Linux:
  - Do not include any of the following directories: `root`, `/usr`, `/usr/local`, or `/var`.
  - Do not include symbolic links.
  - Do not specify a slash (/) at the end of the directory path.

Related concepts

- About verifying the installation environment on page 41

Related tasks

- Preparing the installation directories on page 44

Preparing the installation directories

During new Hitachi Compute Systems Manager installations, the installation wizard prompts you for the location of the installation directory and the database directory. Regardless of whether you choose to install in the default directories or different directories, you must verify that the installation directories meet the required prerequisites.

If you are installing Compute Systems Manager on a machine that is already running another Hitachi Command Suite product, the installation program installs the Hitachi Command Suite Common Component in the same location as the existing Hitachi Command Suite product regardless of whether you change the Compute Systems Manager installation directory.

Procedure

1. Determine whether to modify the default installation directories.
2. To install in the default directories for a new installation, verify that the following default installation directories do not exist. If any of these directories exists, delete them.
   - Compute Systems Manager software:
     Windows default:
     Program-Files-folder\HiCommand
     Linux default:
     /opt/HiCommand
   - Compute Systems Manager database:
     Windows default:
     HCSM-installation-folder\database
     For installations in which another Hitachi Command Suite is already installed, the default database backup directory is *HCSM-installation-directory*\ComputeSystemsManager_backup
     Linux default:
     /var/HiCommand/database

   Tip: You can use the **hcmds64dbtrans** command to import a database backup obtained during an installation.

   For installations in which you use the all-in-one installer, the default database backup directory is *HCSM-installation-directory*/database
3. To install in directories other than the default:

1. Determine where to install Compute Systems Manager or the database based on your specific installation environment.
2. Create the new installation directory(s) and verify that the new directories are empty.
3. When prompted for the Compute Systems Manager or database directory location during the installation, browse to the new directory.

4. If you are installing Deployment Manager, verify that the following directories do not exist:

   `C:\Deploy` (This directory contains files used for internal processing)

   `C:\DeployBackup` (This is the default directory for storing image files. After installing Deployment Manager, you can use the GUI to change the directory path.)

Related concepts

- About verifying the installation environment on page 41

Related references

- Rules for specifying path names on page 43

Specifying management server information during installation

During new Hitachi Compute Systems Manager installations, the installation wizard prompts you for the management server name. In most cases, accept the default server name. By default, this is the host name set for the operating system. When specifying the management server host name, ensure the following:

- The host name uses the following valid characters only:
  A to Z, a to z, 0 to 9, hyphen (-), period (.)
  A hyphen (-) cannot be used at the beginning or end of the host name.
- The length of the host name does not exceed 128 bytes.

Also ensure that the host name or IP address is included in the URL that management clients use to access the management server.

Related concepts

- About verifying the installation environment on page 41

Installing Hitachi Compute Systems Manager

This module provides information about installing Hitachi Compute Systems Manager from different types of media.

Related concepts

- About installing Hitachi Compute Systems Manager on page 46

Related tasks

- Installing the software (Windows) on page 47
- Installing the software (Linux) on page 50
- Installing from the integrated media by using the all-in-one installer (Windows) on page 49

About installing Hitachi Compute Systems Manager

The Hitachi Compute Systems Manager media differs depending on whether you purchase Compute Systems Manager as a separate component or as part of a set in another Hitachi Command Suite product.

If you purchase Compute Systems Manager as a component of another Hitachi Command Suite product, you install the product from integrated installation media for Windows by using the all-in-one installer. The all-in-one installer installs Compute Systems Manager along with the following products:

- Hitachi Device Manager
- Hitachi Tiered Storage Manager
- Hitachi Replication Manager
- Hitachi Tuning Manager
- Hitachi Automation Director
- Hitachi Storage Navigator Modular 2

You cannot use the all-in-one installer to install Deployment Manager.

Note:

- When you use the all-in-one installer, you must install Hitachi Device Manager, Hitachi Tiered Storage Manager, and Hitachi Replication Manager.
- When you use the all-in-one installer, there are limitations on the characters that you can use for the host name. If you are not able to use the current host name with the all-in-one installer, use the Compute Systems Manager installer instead and specify an IP address.

The Compute Systems Manager installation types are as follows:

- New installation
  Install Compute Systems Manager in an environment where it is not already installed.
- Overwrite installation
  Reinstall the same version of Compute Systems Manager in an environment where it is already installed.
  You should use an overwrite installation when:
  - The installed Compute Systems Manager files are corrupt.
  - The installation or removal of Compute Systems Manager fails.
- Upgrade installation

Install a newer version of Compute Systems Manager than the version that is already installed.

The procedure for installing Compute Systems Manager is the same for all installation types except for an upgrade from version 7.*x*.

Note:
- If you install Compute Systems Manager in an environment in which a virus scanning program is running, you must change the virus scanning program settings after installation.
- If you plan to install Compute Systems Manager in a cluster environment, you must specify environment settings in advance. For details about the environment settings and the installation procedure, see the descriptions about environment settings and operations for using clusters.

Related concepts

- About upgrading from Hitachi Compute Systems Manager v7.x on page 324

Related tasks

- Installing the software (Windows) on page 47
- Installing the software (Linux) on page 50
- Installing from the integrated media by using the all-in-one installer (Windows) on page 49

Related references

- Setting requirements for virus scanning program settings on page 51

Installing the software (Windows)

If you purchased Hitachi Compute Systems Manager with another Hitachi Command Suite product, install the software from the integrated product DVD. If you purchased Compute Systems Manager as a separate component, install it from the standalone media.

Note: If you want to install other Hitachi Command Suite products, ensure that your system meets the installation requirements for all the products.

Procedure

1. Ensure that your system meets all management server prerequisites as listed in the pre-installation checklist.
2. If you plan to install Deployment Manager, verify that your system meets the Deployment Manager installation prerequisites.
3. If the server is running any products that use the Compute Systems Manager Common Component, stop the services for those products.
4. Verify the following conditions:

- Windows firewall service is running.
- Windows Services and Event Viewer dialog boxes are closed.

5. Insert the installation media into the DVD drive.

   If you are using the integrated media DVD and the installation program window does not open, double-click `index.html`.
6. Start the installation wizard.
   - If you are using the integrated installation media, select **HCSM** in the installation program window, and then click **Install**.
   - If you are using the Compute Systems Manager media, access the DVD contents and run *DVD-drive*`:\HCSM_SERVER\setup.exe`.
7. Follow the on-screen prompts and specify the required information.

   In most cases, accept the default installation selections.

   The **Install Complete** window opens.
8. If you received a message prompting you to restart the system during the installation, ensure that you select the **After the installation finishes, restart your computer** check box before continuing. If you do not select the check box before clicking **Finish**, you must restart the operating system manually before using the Compute Systems Manager system.
9. Click **Finish**.

Note:

- If Compute Systems Manager is installed in an environment where SSL communication is enabled or in which the port number for Hitachi Command Suite Common Component has been changed, the graphical user interface might not start, even if the **After the installation finishes, start Hitachi Command Suite GUI** check box is selected in the **Install Complete** window.

  If this problem occurs, check the changed management server information, and then enter the URL for Compute Systems Manager in the address bar of the web browser to start the interface.
- If Internet Explorer 11 is the default browser, a blank or transitional window might display after logging on to Compute Systems Manager. If this problem occurs, restart the web browser and enter the URL for Compute Systems Manager in the address bar.

Result

Compute Systems Manager is now installed and DCOM is enabled.

Related concepts

- About installing Hitachi Compute Systems Manager on page 46

Related tasks

- Installing Deployment Manager on page 169

Related references

- Setting requirements for virus scanning program settings on page 51

Installing from the integrated media by using the all-in-one installer (Windows)

If you purchased Hitachi Compute Systems Manager with another Hitachi Command Suite product, you can install the Compute Systems Manager software from an integrated product DVD using the all-in-one installer.

Note: If you want to install other Hitachi Command Suite products, ensure that your system meets the installation requirements for all the products.

Procedure

1. Ensure that your system meets all management server prerequisites as listed in the pre-installation checklist.
2. If the server is running any products that use the Hitachi Command Suite Common Component, stop the services for those products.
3. Verify the following conditions:
   - Windows firewall service is running.
   - Windows Services and Event Viewer dialog boxes are closed.
4. Insert the integrated installation media into the DVD drive.

   If the installation window does not open, choose one of the following options:
   - Access the DVD contents and double-click `index.html`.
   - Access the DVD contents and run *DVD-drive*`:\HCS2\setup.exe`.
5. In the Installation window, click **All-in-One Installer**.
6. In the **Select Products** window, select **Hitachi Compute Systems Manager**.
7. Follow the on-screen instructions and enter the required information.
8. If you are prompted to restart the system, select **Restart the system now**.

   Note: If you choose **Restart the system later**, you must restart the system before you use any of the Hitachi Command Suite products.

9. Click **Finish**.

Related concepts

- About installing Hitachi Compute Systems Manager on page 46

Related references

- Setting requirements for virus scanning program settings on page 51

Installing the software (Linux)

Before installing Hitachi Compute Systems Manager on Linux, make sure that the services are stopped on any products that use the Hitachi Command Suite Common Components.

Caution: If localhost and the host name of the management server are not in the `/etc/hosts` file, an error might occur during installation.

To install Compute Systems Manager:

Procedure

1. Ensure that your system meets all management server prerequisites as listed in the pre-installation checklist.

   Note: If you want to install other Hitachi Command Suite products, ensure that your system meets the installation requirements for all the products.

2. Insert the installation media into the DVD drive.

   If the installation media is not automatically mounted, mount it manually.
3. Move to the installation directory:

   DVD-drive/HCSM_SERVER/*PLATFORM-NAME*
4. Run the **./install.sh** command to install Compute Systems Manager.

   Note: After the installation starts, do not interrupt the process by using **Ctrl**+**C**.

5. Enter the required information when prompted.

Related concepts

- About installing Hitachi Compute Systems Manager on page 46

Related tasks

- Verifying access to the management server on page 52

Related references

- Setting requirements for virus scanning program settings on page 51

Setting requirements for virus scanning program settings

If you plan to use a virus scanning program on the management server, you must first exclude the following directories from the scope of the scan. This is required to ensure the virus scanning program does not access database files, which might cause a failure because of delayed I/O operations, file exclusion, or other similar issues.

To use a virus scanning program on the management server, exclude the following directories from the scope of the scan.

In Windows:

- Exclude the Hitachi Command Suite Common Component folder: *HCS-Common-Component-installation-folder*\HDB
- Exclude the database folder: *HCSM-installation-folder*\database

In Linux:

- Exclude the Hitachi Command Suite Common Component directory: *HCS-Common-Component-installation-directory*/HDB
- Exclude the database directory: *HCSM-installation-directory*/database

Note: If you changed the default database directory, specify the directory that you are using.

Related concepts

- About installing Hitachi Compute Systems Manager on page 46

Post-installation tasks

This module provides information about required Hitachi Compute Systems Manager post-installation tasks, including accessing the management server, setting up user accounts and passwords, and setting up e-mail notification for alerts.

About Hitachi Compute Systems Manager post-installation tasks

After you install Hitachi Compute Systems Manager, you must complete the following post-installation tasks:

- Verify access to the Compute Systems Manager management server.
- Register the plug-in licenses (if necessary).

- Change the system account password (recommended).
- Configure the initial settings.
  The first time you log in to Compute Systems Manager from a management client, the initial settings wizard opens in the Dashboard To Do list. The wizard provides you with direct access to the initial setup steps and only opens the first time you log in. For subsequent logins, after you complete the initial settings, you can access specific tasks through the standard user interface.

All post-installation tasks require that you log in using the System account.

Related tasks

- Verifying access to the management server on page 52
- Registering a license on page 53
- Changing the System account password on page 54
- Setting an e-mail address for the System account on page 54
- Setting up e-mail notifications on page 55
- Setting up the alert level for e-mail notifications on page 55
- Adding resources to Hitachi Compute Systems Manager on page 56
- Creating a server administrator account on page 57
- Creating resource groups on page 58
- Creating user groups and setting up access control on page 58
- Completing the initial setup on page 59

Verifying access to the management server

After you install Hitachi Compute Systems Manager, you must verify access to the management server from a web browser located on a management client.

Procedure

1. Verify that you have the IP address or host name of the management server.
2. Open a web browser that is supported by Compute Systems Manager.
3. Check the browser settings and modify them as required. For details about browser settings, see the *Hitachi Command Suite Compute Systems Manager User Guide*.
4. In the address bar, specify the Compute Systems Manager URL by using the following format:

   Protocol://*Management-server-IP-address-or-hostname:port-number*/ComputeSystemsManager/

   Where
   - *Protocol*
     Specify http for non-SSL communication, and https for SSL communication.

- *Management-server-IP-address-or-hostname*
  Specify the IP address or host name of the management server on which Compute Systems Manager was installed.
- *port-number*
  Specify the port number that is set for Listen line in the `user_httpsd.conf` file.
  For non-SSL communication, specify the port number for non-SSL communication (default: 22015).
  For SSL communication, specify the port number for SSL communication (default: 22016).
  The `user_httpsd.conf` file is stored in the following locations:
  In Windows:
  HCS-Common-Component-installation-folder`\uCPSB\httpsd\conf\user_httpsd.conf`
  In Linux:
  HCS-Common-Component-installation-directory`/uCPSB/httpsd/conf/user_httpsd.conf`

Result

The management client login window opens and verifies that you can access the management server.

Related concepts

- About Hitachi Compute Systems Manager post-installation tasks on page 51

Registering a license

You must register plug-in licenses to use specific functions of Hitachi Compute Systems Manager.

Procedure

1. In the product login window, click **Licenses**.
2. Enter the license key, or browse to the location of a license file, and then click **Save**.

Result

The registered Compute Systems Manager license key displays in the **License** window.

To register or update a license after the initial login, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Related concepts

- About Hitachi Compute Systems Manager post-installation tasks on page 51

Changing the System account password

If you installed Hitachi Compute Systems Manager in an environment in which no other Hitachi Command Suite products are installed, make sure that you change the System account password.

The System account is a default account that has user management and execute permission for all Hitachi Command Suite products.

Procedure

1. From a management client log in using the following credentials:
   - **User ID:** system
   - **Password (default):** manager

   The **To Do** list opens and opens the initial setup wizard.
2. From the **To Do** list, select **Edit Profile and Set e-mail address**.
3. In the **User Profile** window, click **Change Password**, type the required password fields, and click **OK**.

   Remain in the **User Profile** window and continue to the following topic, that describes setting up the System account e-mail address.

Result

The default password is changed.

For details about changing user account passwords, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Related concepts

- About Hitachi Compute Systems Manager post-installation tasks on page 51

Setting an e-mail address for the System account

Before Hitachi Compute Systems Manager can send e-mail notifications about Compute Systems Manager system operations, you must set up a System account e-mail account.

Procedure

1. From the **User Profile** window, go to the next step. Otherwise, from the **To Do** list, select **Edit Profile and set e-mail address**.
2. In the **User Profile** window, click **Edit Profile**, type the full name and the e-mail address, and then click **OK**.

Result

The System account e-mail address is set up.

For details about editing user profiles, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Related concepts

- About Hitachi Compute Systems Manager post-installation tasks on page 51

Setting up e-mail notifications

Before Hitachi Compute Systems Manager can send e-mail notifications when Compute Systems Manager alerts occur or when a Compute Systems Manager task is finished, you must set up an SMTP server.

Procedure

1. From the **To Do** list, select **Configure E-mail Settings**.
2. Select the **E-mail Notification Enabled** check box and type the required SMTP server information.
3. Optionally, to configure security settings, expand **Advanced Settings**.

Result

E-mail notification is set up.

You can also set up e-mail notification by using the Compute Systems Manager Administration tab System Settings option. For details about setting up e-mail notification, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Related concepts

- About Hitachi Compute Systems Manager post-installation tasks on page 51

Setting up the alert level for e-mail notifications

After you set up e-mail notifications, you must also set notification alert levels. This setting specifies which alerts to send by e-mail.

Procedure

1. From the **To Do** list, select **Configure E-mail Notification Settings**.
2. Select an alert level and click **OK**.

Result

The e-mail notification alert level is set up.

You can also set e-mail notification alert levels by using the Compute Systems Manager Administration tab Automated Event Handling option. For

details about setting the alert level for e-mail notifications, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Related concepts

- About Hitachi Compute Systems Manager post-installation tasks on page 51

Related tasks

- Setting up e-mail notifications on page 55

Adding resources to Hitachi Compute Systems Manager

Before you begin using Hitachi Compute Systems Manager to manage resources, set up the management targets and then add them to the system as managed resources.

Procedure

1. Ensure that you configured the required prerequisite settings for the management targets.
2. From the **To Do** list, complete the tasks listed in the **Discovery** section.

   The **Discovery** section includes discovering and adding management targets, that consists of the following:
   - Specifying an IP address range
   - Discovering resources

   Complete these steps using the instructions provided in the *Hitachi Command Suite Compute Systems Manager User Guide*.

   All discovered resources are automatically added as managed resources.
3. From the **To Do** list **Finish** section, select the first step, **Select Resources to Manage**.
4. Verify the managed resources that were added during the discovery process.
   - To stop managing a resource, clear the check box for the resource.
   - To start managing a resource, select the check box for the resource.
5. When prompted to confirm a change, click **OK**.

Result

After you verify the managed resources list, you are ready to finish the initial setup process as described in the following topic.

Postrequisites

Tip: If you install Compute Systems Manager on a management server that is running the Hitachi Device Manager component, all existing hosts that meet Compute Systems Manager management target requirements are

automatically imported into Compute Systems Manager as managed hosts. This applies only to discovered hosts, not other discovered resources. Note that VMware information discovered in Hitachi Device Manager is not synchronized with Compute Systems Manager.

Related concepts

- About Hitachi Compute Systems Manager post-installation tasks on page 51

Related references

- Prerequisites for managing Windows hosts on page 91
- Prerequisites for managing Linux or Solaris hosts on page 98

Optional initial setup tasks

The remaining initial setup tasks described in this module for user group and resource group management are optional. You can create users and groups now or wait until later and access these tasks from the Hitachi Compute Systems Manager Administration tab.

Creating a server administrator account

As part of the initial setup, create a server administrator account for managing Hitachi Compute Systems Manager. To ensure that the server administrator can manage other users, you assign the user management permission.

Procedure

1. From the **To Do** list, select **Create Users**.
2. Click **Users** and then click **Add User**.
3. Specify the required information and click **OK**.
4. Click the new user entry in the list and click **Change Permission**.
5. Specify the required administrative permissions and click **OK**.

Result

The system administrator account is set up.

For details about adding users and required permissions, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Related concepts

- About Hitachi Compute Systems Manager post-installation tasks on page 51

Creating resource groups

As part of the initial setup, you can create resource groups to control access to a specific set of managed resources. There are built-in and user-defined resource groups. You must register your resources before you can add them to a resource group.

Procedure

1. From the **To Do** list, select **Create Resource Group**.
2. Specify the name of the Resource Group and optionally add a description.
3. Select the resource type and then select the resources to add to the group.
4. Click **OK**.

Result

The system adds the new resource group.

You can also create resource groups by using the Compute Systems Manager Administration tab Resource Groups option. For details about creating resource groups, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Related tasks

- Creating a server administrator account on page 57
- Adding resources to Hitachi Compute Systems Manager on page 56

Creating user groups and setting up access control

As part of the initial setup, you can create user groups that consists of one or more users having the same permissions (role) for the same resources. There are built-in and user-defined user groups and three different user group roles for Admin, Modify, and View. After creating the user groups, you can set up access control by assigning resource groups (with assigned roles) to the user group.

Procedure

1. From the **To Do** list, select **Create User Group and Assign Resource Groups**.
2. Specify the name of the User Group and optionally add a description.
3. Select the users to add to the group.
4. Select the Resource Groups to assign, edit the role as needed, and click **OK**.

Result

The system adds the new user group.

You can also create user groups by using the Compute Systems Manager Administration tab User Groups option. For details about creating user groups and setting up access control, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Related tasks

- Changing the System account password on page 54
- Creating a server administrator account on page 57

Completing the initial setup

Before you can view managed resource information using Hitachi Compute Systems Manager, you must complete the initial setup of the Compute Systems Manager dashboard.

To set up the dashboard and complete the initial setup, go to the last step in the To Do list and click Launch Dashboard.

The Dashboard tab displays four panes that include information about managed resources. After you complete the initial setup, the wizard no longer appears in the To Do list.

The initial setup is now complete and you can begin using Compute Systems Manager to manage resources.

Related concepts

- About Hitachi Compute Systems Manager post-installation tasks on page 51

Removing Hitachi Compute Systems Manager

This module provides information about removing Hitachi Compute Systems Manager.

About removing Hitachi Compute Systems Manager

You must remove the Hitachi Compute Systems Manager software from the management server under the following circumstances:

- Reinstalling Compute Systems Manager (clean installation).
- Migrating Compute Systems Manager to a different environment.
- Stopping Compute Systems Manager operation on the server.

In Windows, you can remove Compute Systems Manager only or you can use the all-in-one uninstaller. The all-in-one uninstaller also removes the following products installed on the management server:

- Hitachi Device Manager
- Hitachi Tiered Storage Manager
- Hitachi Replication Manager

- Hitachi Tuning Manager
- Hitachi Automation Director
- Hitachi Storage Navigator Modular 2

If you use the all-in-one uninstaller, all Hitachi Command Suite product files are removed.

If you remove Compute Systems Manager only, the properties files, database files, log files, and other Compute Systems Manager-related files are deleted. The files and directories that are not deleted when Compute Systems Manager is removed are as follows:

- Files for products that require Hitachi Command Suite Common Component as a prerequisite such as property files, database files, log files, and so on.
- When Deployment Manager is installed, `C:\DeployBackup`. You can remove this file if you no longer need it.

Related tasks

- Removing the software (Windows) on page 61
- Removing the software (Linux) on page 62
- Removing the software by using the all-in-one uninstaller (Windows) on page 62

Related references

- Prerequisites for removing the software on page 60

Prerequisites for removing the software

The Hitachi Compute Systems Manager installation directory and database directory are deleted when you remove the Compute Systems Manager software. To reuse the content in either of these directories, you must back up the directories before removing the software.

Before removing the Compute Systems Manager software, you must verify the following:

- If you plan to reinstall or migrate to another server after removing the software, export the existing database.
- If you want to reuse directories and files added by Compute Systems Manager users, back up the user directories and files.
  In Windows, these files are located in the folder:
  HCSM-installation-folder`\ComputeSystemsManager`
  In Linux, these files are located in the directory:
  HCSM-installation-directory`/ComputeSystemsManager`

Note: If you remove all the Hitachi Command Suite products that are v8.0 or later from a management server on which products are installed that use the 32-bit version of Hitachi Command Suite Common Component (Hitachi File

Services Manager and Hitachi Storage Navigator Modular 2), you will no longer be able to use the 32-bit products. To continue using these products after the installation, use the following procedure to reinstall the products:

1. Remove products that use the 32-bit Hitachi Command Suite Common Component.
2. Remove the Hitachi Command Suite products that are v8.0 or later.
3. Reinstall the products that use the 32-bit Hitachi Command Suite Common Component.

Related concepts

- About removing Hitachi Compute Systems Manager on page 59

Related tasks

- Removing the software (Windows) on page 61

Removing the software (Windows)

You can remove the Hitachi Compute Systems Manager software from the management server if you want to reinstall (clean install), migrate to a different server, or stop Compute Systems Manager operation.

Note: If you remove Compute Systems Manager, the properties files, database files, log files, and other product-related files are deleted.

Procedure

1. From the Control Panel, select **Programs and Features**.
2. Select **Hitachi Compute Systems Manager** from the list of programs and click **Remove** or **Uninstall**.
3. Follow the on-screen prompts.
4. If no other programs on the server use Distributed Component Object model (DCOM), disable DCOM.

Result

The Compute Systems Manager software is removed from the server.

Related concepts

- About removing Hitachi Compute Systems Manager on page 59

Related tasks

- Removing the software by using the all-in-one uninstaller (Windows) on page 62

Related references

- Prerequisites for removing the software on page 60

Removing the software by using the all-in-one uninstaller (Windows)

You can remove the Hitachi Compute Systems Manager software and all other Hitachi Command Suite products from the management server by using the all-in-one uninstaller.

Note: If you remove Hitachi Command Suite software, the properties files, database files, log files, and other product-related files are deleted.

Procedure

1. From the Control Panel, select **Programs and Features**.
2. Select **HCS All-in-One Uninstaller** from the list of programs and click **Remove** or **Uninstall**.
3. Follow the on-screen prompts.
4. If no other programs on the server use Distributed Component Object model (DCOM), disable DCOM.

Result

The Hitachi Command Suite software is removed from the server.

Related concepts

- About removing Hitachi Compute Systems Manager on page 59

Related references

- Prerequisites for removing the software on page 60

Removing the software (Linux)

You can remove the Hitachi Compute Systems Manager software from the management server if you want to reinstall (clean install), or stop Compute Systems Manager operation.

Note: If you remove Compute Systems Manager, the properties files, database files, log files, and other product-related files are deleted.

Procedure

1. From the `/root` directory, run the following command:

   HCSM-installation-directory`/CSMUninstall/uninstall.sh`
2. Follow the on-screen prompts.

Result

The Compute Systems Manager software is removed from the management server.

Related concepts

- About removing Hitachi Compute Systems Manager on page 59

Related references

- Prerequisites for removing the software on page 60

3

Configuring the management server

This module describes how to configure the Hitachi Compute Systems Manager (HCSM) management server.

- Configuring SNMP
- Configuring optional user account settings
- Changing management server system settings

Configuring SNMP

This module provides information about configuring Hitachi Compute Systems Manager to receive and use standard Simple Network Management Protocol (SNMP) management traps.

About SNMP trap settings

You can configure Hitachi Compute Systems Manager to receive alerts if managed hosts that are not mounted on Hitachi servers generate Simple Network Management Protocol (SNMP) traps. Because SNMP traps provide information about failure types and where the failures occur, you can use the information to determine the causes of errors.

Configure Compute Systems Manager as follows to receive SNMP traps as alerts:

- Register a Management Information Base (MIB) file for the management server.
- Set up SNMP trap reception on the management client.

For details about management client settings, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Related tasks

- Registering an SNMP MIB file on page 66

Registering an SNMP MIB file

To associate specific SNMP traps with alerts other than 0x0000, you can register an MIB file that defines default SNMP traps to the management server.

Prerequisites

Before you register an SNMP MIB file, complete the following tasks:

- Verify that the management server SNMP receiver port is available for use (port 162/UDP by default).
- If the management server is running Red Hat Linux, install the 64-bit version net-snmp-libs package.

To register a MIB file:

Procedure

1. Prepare a MIB file. You can use any name for the file.
2. Copy the MIB file to the following directory:
   - In Windows:

HCSM-installation-folder\ComputeSystemsManager\mibs\mib
    - In Linux:
      HCSM-installation-directory/ComputeSystemsManager/mibs/mib
3. Stop Compute Systems Manager.
4. To register the file, run the following command:
    - In Windows:
      HCSM-installation-folder\ComputeSystemsManager\bin
      \hcsmtraptoxml -c
    - In Linux:
      HCSM-installation-directory/ComputeSystemsManager/bin/
      hcsmtraptoxml -c
5. Start Compute Systems Manager.

Result

The SNMP trap information is now registered.

Related concepts

- About SNMP trap settings on page 66

Related tasks

- Changing Hitachi Compute Systems Manager ports on page 74
- Starting Hitachi Compute Systems Manager on page 174
- Stopping Hitachi Compute Systems Manager on page 175

About monitoring inband SNMP traps

If you want Hitachi Compute Systems Manager to monitor SNMP traps generated for inband driver events on managed hosts, you must configure specific SNMP-related settings on each managed host and on the Compute Systems Manager management server.

Configuring Compute Systems Manager to monitor inband driver traps consists of the following tasks:

- Configuring managed hosts to send SNMP traps
- Configuring the Compute Systems Manager management server to receive SNMP traps

Related tasks

- Configuring the management server to receive inband SNMP traps on page 68
- Configuring a Windows host to send SNMP inband traps (optional) on page 96
- Configuring a Linux host to send SNMP inband traps (optional) on page 107
- Configuring a Solaris host to send SNMP inband traps (optional) on page 108

Configuring the management server to receive inband SNMP traps

Before Hitachi Compute Systems Manager can monitor inband driver traps received from managed hosts, you must configure the management server by installing specific SNMP-related MIB files. In addition, you must also configure each Compute Systems Manager managed host.

You need to register MIB files when the managed host runs Windows or Linux.

Procedure

1. If the managed host runs Windows or Linux, register the MIB files to use for monitoring inband driver events that occur on the managed host.

   Copy the following files from the installation media, and use them to register MIB files:
   - For Windows management servers:
     `\HCSM_SERVER\HCSM\snmp\mibs\hfcwdd-win.mib` (for managed hosts running Windows)
     `\HCSM_SERVER\HCSM\snmp\mibs\hfcldd-lin.mib` (for managed hosts running Linux)
   - For Linux management servers:
     `/HCSM_SERVER/HCSM/snmp/mibs/hfcwdd-win.mib` (for managed hosts running Windows)
     `/HCSM_SERVER/HCSM/snmp/mibs/hfcldd-lin.mib` (for managed hosts running Linux)
2. Specify settings to receive SNMP traps.

   For more information, see the *Hitachi Command Suite Compute Systems Manager User Guide*.
3. Configure the managed hosts to send inband driver events using SNMP.

Related concepts

- About monitoring inband SNMP traps on page 67

Related tasks

- Registering an SNMP MIB file on page 66
- Configuring a Windows host to send SNMP inband traps (optional) on page 96
- Configuring a Linux host to send SNMP inband traps (optional) on page 107
- Configuring a Solaris host to send SNMP inband traps (optional) on page 108

Configuring optional user account settings

This module provides information about configuring optional user account settings related to increasing system security.

About optional user account settings

When using Hitachi Compute Systems Manager, you can register users, set passwords, and configure other user account-related settings by using the management client interface. In addition to these settings, there are also optional user account settings that you must set using the CLI.

The optional user account settings are as follows:

- System account locking
  When you install Compute Systems Manager, the default System account settings do not provide automatic or manual locking. You can enable System account locking by modifying the initial settings.
- Unlocking accounts
  If an account is locked, the account user cannot access Compute Systems Manager until the account is unlocked. You can unlock accounts by using a management client.
  Although you can unlock other accounts by using a management client, you must use the management server to unlock your own account.

Note: If your system runs other Hitachi Command Suite products along with Compute Systems Manager, the settings you specify for Compute Systems Manager apply to all Hitachi Command Suite user accounts.

Related tasks

- Enabling System account locking on page 69
- Unlocking user accounts on page 70

Enabling System account locking

When you install Hitachi Compute Systems Manager, the default System account settings do not allow you to lock the System account. You can enable automatic or manual System account locking by modifying the initial default settings.

Procedure

1. Access the Hitachi Command Suite Common Component properties file as follows:
   - In Windows:
     HCS-Common-Component-installation-folder\conf\user.conf
   - In Linux

HCS-Common-Component-installation-directory/conf/user.conf

If the `user.conf` file does not exist, create it.

2. Change the following user account property value to true:

   `account.lock.system`

   If you specify true, the System account is subject to automatic and manual locking. If you specify false, the System account is not subject to automatic or manual locking.
3. Save and close the properties file.

Result

You can now automatically or manually lock the System account.

Related concepts

- About optional user account settings on page 69

Related references

- Properties related to System account locking (user.conf) on page 306

Unlocking user accounts

You can unlock user accounts other than your own by using the Hitachi Compute Systems Manager interface from a management client. To unlock your own account, you must use the management server.

To unlock a user account other than your own, follow the instructions in the *Hitachi Command Suite Compute Systems Manager User Guide*.

Procedure

1. Start Compute Systems Manager.
2. Log in to the management server and access a command prompt.
3. Unlock the account by using the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64unlockaccount [/user *user-ID*][/pass *password*]
   - In Linux:
     HCS-Common-Component-installation-directory/bin/hcmds64unlockaccount [-user *user-ID*] [-pass *password*]

   For *user-ID*, specify the user ID of the account that you want to unlock. For *password*, specify the user account password.

   If you omit the user ID or password, the system prompts you to enter them. If the user account does not have a password, you cannot unlock the account by using this command.

Result

The user account is unlocked.

Related concepts

- About optional user account settings on page 69

Related tasks

- Checking the status of Hitachi Compute Systems Manager services on page 178
- Starting Hitachi Compute Systems Manager on page 174

Changing management server system settings

This module provides information about changing Hitachi Compute Systems Manager management server system settings.

Changing Hitachi Compute Systems Manager port numbers

This module provides information about changing Hitachi Compute Systems Manager port numbers.

Hitachi Command Suite properties requiring updates for port number changes

After modifying the Hitachi Compute Systems Manager port numbers, you must update the Hitachi Command Suite Common Component properties listed in the following table.

Note: If a product that uses the 32-bit version of Hitachi Command Suite Common Component is installed (Hitachi File Services Manager or Hitachi Storage Navigator Modular 2), make sure that you set port numbers that do not conflict with the port number used by these products.

Port Number (default)	Properties File Path (Hitachi Command Suite Common Component installation directory)	Location to Edit

22015/TCP	In Windows:
	`\uCPSB\httpsd\conf\user_httpsd.conf`
	In Linux:
	`/uCPSB/httpsd/conf/user_httpsd.conf`
		`Listen`
		`Listen [::]:`
		`#Listen 127.0.0.1:`

22016/TCP	In Windows:
	`\uCPSB\httpsd\conf\user_httpsd.conf`
	In Linux:
	`/uCPSB/httpsd/conf/user_httpsd.conf`
		`host-name:port-number` in the `<VirtualHost>` tag
		`Listen`
		`Listen [::]:`

22027/TCP	In Windows:	`worker.ComputeSystemsManagerWebService.port`

Port Number (default)	Properties File Path (Hitachi Command Suite Common Component installation directory)	Location to Edit
	\uCPSB\CC\web\redirector\workers.properties In Linux: /uCPSB/CC/web/redirector/workers.properties	
	In Windows: \uCPSB\CC\web\containers\ComputeSystemsManagerWebService\usrconf\usrconf.properties In Linux: /uCPSB/CC/web/containers/ComputeSystemsManagerWebService/usrconf/usrconf.properties	webserver.connector.ajp13.port
22028/TCP	In Windows: \uCPSB\CC\web\containers\ComputeSystemsManagerWebService\usrconf\usrconf.properties In Linux: /uCPSB/CC/web/containers/ComputeSystemsManagerWebService/usrconf/usrconf.properties	webserver.shutdown.port
22031/TCP	In Windows: \uCPSB\httpsd\conf\user_hsso_httpsd.conf In Linux: /uCPSB/httpsd/conf/user_hsso_httpsd.conf	Listen
22032/TCP	In Windows: \HDB\CONF\emb\HiRDB.ini In Linux: /HDB/CONF/emb/HiRDB.ini	PDNAMEPORT
	In Windows: \HDB\CONF\pdsys In Linux: /HDB/CONF/pdsys	pd_name_port
	In Windows: \database\work\def_pdsys In Linux: /database/work/def_pdsys	pd_name_port

Port Number (default)	Properties File Path (Hitachi Command Suite Common Component installation directory)	Location to Edit

22033/TCP	In Windows:
	`\uCPSB\CC\web\redirector\workers.properties`
	In Linux:
	`/uCPSB/CC/web/redirector/workers.properties`
		`worker.HBase64StgMgmtSSOService.port`

	In Windows:
	`\uCPSB\CC\web\containers\HBase64StgMgmtSSOService\usrconf\usrconf.properties`
	In Linux:
	`/uCPSB/CC/web/containers/HBase64StgMgmtSSOService/usrconf/usrconf.properties`
		`webserver.connector.ajp13.port`

22034/TCP	In Windows:
	`\uCPSB\CC\web\containers\HBase64StgMgmtSSOService\usrconf\usrconf.properties`
	In Linux:
	`/uCPSB/CC/web/containers/HBase64StgMgmtSSOService/usrconf/usrconf.properties`
		`webserver.shutdown.port`

Related tasks

- Changing Hitachi Compute Systems Manager ports on page 74

Hitachi Compute Systems Manager properties requiring updates for port number changes

After modifying the Hitachi Compute Systems Manager port numbers, you must update the Compute Systems Manager properties listed in the following table:

Port Number (default)	Properties File Path (Hitachi Compute Systems Manager installation directory)	Location to Edit

162/UDP or
22601/UDP
	In Windows:
	`ComputeSystemsManager\conf\user.properties`
	In Linux:
	`ComputeSystemsManager/conf/user.properties`
		`snmp.trap.receive.port`

Port Number (default)	Properties File Path (Hitachi Compute Systems Manager installation directory)	Location to Edit
	Note: The default is 162/UDP. If 162/UDP is in use for another product, 22601/UDP becomes the default.	

22610/TCP	In Windows:
	`ComputeSystemsManager\conf\user.properties`
	In Linux:
	`ComputeSystemsManager/conf/user.properties`
		`server.rmi.port`

22611/TCP	In Windows:
	`ComputeSystemsManager\conf\user.properties`
	In Linux:
	`ComputeSystemsManager/conf/user.properties`
		`svp.alert.receive.port`

Related tasks

- Changing Hitachi Compute Systems Manager ports on page 74
- Changing the management server URL on page 79

Related references

- Hitachi Compute Systems Manager server ports on page 286
- Hitachi Compute Systems Manager server properties files on page 290

Changing Hitachi Compute Systems Manager ports

You can change the port numbers used for Hitachi Compute Systems Manager after installation if necessary.

Procedure

1. Stop Compute Systems Manager.
2. Edit the Compute Systems Manager properties or the Hitachi Command Suite Common Component properties.
3. Start Compute Systems Manager.
4. If you changed the port used for communication between the management server and management clients (22015/TCP or 22016/TCP by default), you need to change the URL for accessing Compute Systems Manager.

Related tasks

- Changing Hitachi Compute Systems Manager ports on page 74
- Starting Hitachi Compute Systems Manager on page 174

- Stopping Hitachi Compute Systems Manager on page 175

Related references

- Hitachi Command Suite properties requiring updates for port number changes on page 71
- Hitachi Compute Systems Manager properties requiring updates for port number changes on page 73
- Hitachi Compute Systems Manager server ports on page 286
- Hitachi Compute Systems Manager server properties files on page 290
- Hitachi Command Suite Common Component ports on page 286
- Properties files for Hitachi Command Suite Common Component on page 294

Changing the management server host name or IP address

This module provides information about changing the management server host name or IP address.

Changing the management server host name or IP address

You can change the host name or IP address of the management server after installing Hitachi Compute Systems Manager.

Prerequisites

Ensure that you have a record of the new management server host name (if the host name was changed) and IP address.

If you already changed the host name of the management server, use the `hostname` command to display the host name.

If you need to verify the host name on a Windows machine, use the `ipconfig /ALL` command to display the host name.

The management server host name must meet the following requirements:

- The host name uses the following valid characters only:
  A to Z, a to z, 0 to 9, hyphen (-), period (.)
  A hyphen (-) cannot be used at the beginning or end of the host name.
- The length of the host name does not exceed 128 bytes.

Also ensure that the new host name or IP address is included in the URL that management clients use to access the management server.

Procedure

1. If you are changing the IP address, you must first unmanage all the chassis. If you are only changing the management server name, go to the next step.
2. Stop Compute Systems Manager.

3. Edit the Hitachi Command Suite Common Component properties.
4. If the OS of the management server is Linux and you want to change the host name, edit the `/etc/hosts` file.

   Change the host name of the management server to the new host name. Enter the new host name in the line above the `localhost` line.
5. If you are also using other Hitachi Command Suite products, revise the settings for these products as needed.
6. Change the IP address or the host name of the management server.

   Make sure to specify the case-sensitive host name exactly.
7. After restarting the computer, verify that all Compute Systems Manager services are running.
8. If you use the old host name or IP address to access the management server from a browser, update the Compute Systems Manager URL.
9. Verify that you can access Compute Systems Manager using the new URL.
10. If you changed the IP address, you must access the chassis resource list and change the status from unmanaged back to managed.
11. Back up the database.

    This step is required because you cannot restore your system using any backup that you created before the IP address or host name change.

Result

The management server host name or IP address is changed.

Related tasks

- Changing the management server URL on page 79
- Starting Hitachi Compute Systems Manager on page 174
- Stopping Hitachi Compute Systems Manager on page 175

Related references

- Hitachi Command Suite properties requiring changes for management server host name changes on page 76
- Hitachi Command Suite properties requiring changes for management server IP address changes on page 78
- Properties files for Hitachi Command Suite Common Component on page 294
- Hitachi Compute Systems Manager server properties files on page 290

Hitachi Command Suite properties requiring changes for management server host name changes

After modifying the host name of the management server, you must update the Hitachi Command Suite Common Component properties listed in the following table:

Note: We recommend that you specify the host name in the `user_httpsd.conf` file.

Properties File Path (Hitachi Command Suite Common Component installation directory)	Properties	Required Edit

In Windows:
`\uCPSB\httpsd\conf\user_httpsd.conf`
In Linux:
`/uCPSB/httpsd/conf/user_httpsd.conf`
	`ServerName`	Change the value to the new host name.

	`<VirtualHost>` tag	If TLS or SSL is used for communication between the management server and management clients and a host name is specified, change the value to an asterisk (*).
	`Servername` in the `<VirtualHost>` tag	If TLS or SSL is used for communication between the management server and management clients, change the value to the new host name.

In Windows:
`\HDB\CONF\pdsys`
`\database\work\def_pdsys`
In Linux:
`/HDB/CONF/pdsys`
`/database/work/def_pdsys`
	the `-x` option of pdunit	Change the value to the loopback address 127.0.0.1.

In Windows:
`\HDB\CONF\pdutsys`
`\database\work\def_pdutsys`
In Linux:
`/HDB/CONF/pdutsys`
`/database/work/def_pdutsys`
	`pd_hostname`	

In Windows:
`\HDB\CONF\emb\HiRDB.ini`
In Linux:
`/HDB/CONF/emb/HiRDB.ini`
	`PDHOST`	

In Windows: `\CONF\cluster.conf`	`virtualhost`	If the management server is in a cluster configuration, change the applicable host
	`onlinehost`	
	`standbyhost`	

Properties File Path (Hitachi Command Suite Common Component installation directory)	Properties	Required Edit
In Linux: /CONF/cluster.conf		name value to the new host name.

Related tasks

- Changing the management server host name or IP address on page 75

Related references

- Properties files for Hitachi Command Suite Common Component on page 294

Hitachi Command Suite properties requiring changes for management server IP address changes

After modifying the IP address of the management server, you must update the Hitachi Command Suite common properties listed in the following table:

Note: Please specify the host name in the user_httpsd.conf file.

Properties File Path (Hitachi Command Suite Common Component installation directory)	Properties	Required Edit
In Windows: \uCPSB\httpsd\conf \user_httpsd.conf In Linux: /uCPSB/httpsd/conf/ user_httpsd.conf	ServerName	Change the value to the new host name or new IP address.
In Windows: \HDB\CONF\pdsys \database\work\def_pdsys In Linux: /HDB/CONF/pdsys/ database/work/def_pdsys	the -x option of pdunit	If the old IP value is specified, change the value to the loopback address 127.0.0.1.
In Windows: \HDB\CONF\pdutsys \database\work\def_pdutsys In Linux:	pd_hostname	

Properties File Path (Hitachi Command Suite Common Component installation directory)	Properties	Required Edit
/HDB/CONF/pdutsys /database/work/def_pdutsys		
In Windows: \HDB\CONF\emb\HiRDB.ini In Linux: /HDB/CONF/emb/HiRDB.ini	PDHOST	

Related tasks

- Changing the management server host name or IP address on page 75

Changing the Hitachi Compute Systems Manager URL

This module provides information about changing the management server URL.

Changing the management server URL

You must change the Hitachi Compute Systems Manager management server URL if you change the management server host name or IP address, the Compute Systems Manager ports, or any SSL settings. If Compute Systems Manager runs on the same management server as other Hitachi Command Suite products, you can change all the URLs with one command.

Note: You must use a complete URL that contains a protocol and a port number, for example, `http://HostA:22015`.

Procedure

1. Verify the current URL by using the following command:

   In Windows:

   HCS-Common-Component-installation-folder\bin\hcmds64chgurl /list

   In Linux:

   HCS-Common-Component-installation-directory/bin/hcmds64chgurl -list

   If you still want to change the URL, go to the next step.
2. Change only the Compute Systems Manager URL by using the following command:

   In Windows:

HCS-Common-Component-installation-folder\bin\hcmds64chgurl /change *new-URL* /type HCSM

In Linux:
HCS-Common-Component-installation-directory/bin/hcmds64chgurl -change *new-URL* -type HCSM

3. Change all Hitachi Command Suite and Compute Systems Manager URLs running on this management server by using the following command:

   In Windows:
   HCS-Common-Component-installation-folder\bin\hcmds64chgurl /change *old-URL new-URL*

   In Linux:
   HCS-Common-Component-installation-directory/bin/hcmds64chgurl -change *old-URL new-URL*

4. In Windows, change the URL for the shortcut file:
   - For Windows Server 2008 R2:
     Select **Start > All Programs > Hitachi Command Suite > Compute Systems Manager** and then right-click **Login - HCSM**. Select **Properties**, and then on the **Web Document** tab, change the URL.
   - For Windows Server 2012:
     Select **Start > All apps > Hitachi Command Suite > Compute Systems Manager** and then right-click **Login - HCSM**. Select **Properties**, and then on the **Web Document** tab, change the URL.

   The URL format is as follows:

   Protocol://*Management-server-IP-address-or-host-name*:*port-number*/ComputeSystemsManager/

   Where:
   - *Protocol*
     Specify http for non-SSL communication, and https for SSL communication.
   - *Management-server-IP-address-or-host-name*
     Specify the IP address or host name of the management server on which Compute Systems Manager was installed.
   - *port-number*
     Specify the port number that is set for Listen line in the user_httpsd.conf file.
     For non-SSL communication, specify the port number for non-SSL communication (default: 22015).
     For SSL communication, specify the port number for SSL communication (default: 22016).
     The user_httpsd.conf file is stored in the following locations:
     In Windows:

HCS-Common-Component-installation-folder\uCPSB\httpsd\conf\user_httpsd.conf

In Linux:

HCS-Common-Component-installation-directory/uCPSB/httpsd/conf/user_httpsd.conf

5. Verify that you can access Compute Systems Manager using the new URL.

Related references

- Configuration changes that require updating the management server URL on page 81

Configuration changes that require updating the management server URL

You must update the URL that you use to access Hitachi Compute Systems Manager if you change any of the following parameters:

- Ports used for communication between the management server and management clients
- Host name or IP address of the management server
- Settings for enabling or disabling SSL communication

Related tasks

- Changing the management server URL on page 79

Using a different Oracle JDK version

You can change the version of Oracle™ JDK that you use with Hitachi Compute Systems Manager after installation if necessary. Refer to the Release Notes for supported Oracle JDK versions.

Procedure

1. Stop Compute Systems Manager.
2. To change the Oracle JDK version, use the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64chgjdk
   - In Linux:
     HCS-Common-Component-installation-directory/bin/hcmds64chgjdk
3. Within the window that opens, select the JDK version to use.
4. Start Compute Systems Manager.
5. If you use TLS or SSL communication, you must re-import the following certificates on the management server:
   - Server certificate for Hitachi Command Suite Common Component and a certificate from a certificate authority
   - Server certificate for Compute Systems Manager and a certificate from a certificate authority

- Server certificate for the LDAP directory server

Re-importing the certificates changes the certificate storage location.

6. Start Compute Systems Manager.

Result

If you install a new version of Oracle JDK using an overwrite or upgrade installation, you must use the `hcmds64chgjdk` command again to set the Oracle JDK version.

To return to the original JDK after installing and configuring a new version, run the `hcmds64chgjdk` command and reselect the JDK bundled with the product.

Related tasks

- Starting Hitachi Compute Systems Manager on page 174
- Stopping Hitachi Compute Systems Manager on page 175
- Setting up SSL on the server for secure client communication on page 115
- Setting up SSL on web-based management clients on page 121
- Setting up SSL on management clients running the CLI on page 122
- Configuring SSL for a secure LDAP server connection on page 141

Updating the management server time setting

This module provides information about updating the management server OS time setting.

Conditions that require resetting the management server time setting

Under certain circumstances, you may need to reset the server time setting manually after installing Hitachi Compute Systems Manager. For example, in some cases your time service might send incorrect time information (this is not common, but on occasion occurs in virtual environments). If you do not use a time service, a problem with the server may affect the time setting.

Related tasks

- Resetting the management server time setting manually on page 82

Resetting the management server time setting manually

If the Hitachi Compute Systems Manager server time is incorrect due to time service or server failure, or you need to reset the time immediately, reset the time manually. This ensures that the Compute Systems Manager task schedules and alert times are accurate.

Procedure

1. Stop Compute Systems Manager.
2. Record the current server time and then reset the time.

3. Determine when to restart the services.
   - If you set the time of the machine back (meaning that the server time was ahead), wait until the server clock shows the time you recorded (the time on the server when you made the change) and then restart the machine.
   - If you set the machine time forward, restart the machine now.

Result

Verify that the Compute Systems Manager Management server reflects the correct time.

Postrequisites

Note: When running Compute Systems Manager in a U.S. or Canadian time zone, you must configure the management server OS so that it supports the new Daylight Savings Time (DST) rules. Compute Systems Manager cannot support the new DST rules unless the server provides support.

Related references

- Conditions that require resetting the management server time setting on page 82

Changing the timeout period for commands

If commands run on the management server, the server allows a certain amount of processing time, called the timeout period, before ending the command due to lack of response. If you plan to run commands that you know require a long processing time, you can change the timeout period so that the commands do not fail due to a timeout.

Procedure

1. Stop Compute Systems Manager.
2. Open the `user.properties` file:
   - In Windows:
     HCSM-installation-folder`\ComputeSystemsManager\conf\user.properties`
   - In Linux:
     HCSM-installation-directory`/ComputeSystemsManager/conf/user.properties`
3. For the `server.process.timeout` property, specify a timeout period for running commands.

   The timeout is specified in seconds (the default is 1800 seconds).

   If you do not want a command to timeout before processing finishes, specify 0.

4. Start Compute Systems Manager.

Result

The command processing timeout period is updated.

Related references

- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 291

Changing the Hitachi Compute Systems Manager temperature measurement unit

You can change the temperature measurement unit that is displayed in the Hitachi Compute Systems Manager user interface. This is the unit that is used for measuring the temperature of managed resources. Compute Systems Manager monitors the temperature to ensure that the temperature remains within a certain range to prevent failure due to overheating. You can choose to display the temperature reading in either Fahrenheit (default) or Celsius.

Procedure

1. Stop Compute Systems Manager.
2. Open the `user.properties` file:
   - In Windows:
     HCSM-installation-folder`\ComputeSystemsManager\conf\user.properties`
   - In Linux:
     HCSM-installation-directory`/ComputeSystemsManager/conf/user.properties`
3. For the `powermonitoring.temperature.unit` property, specify the temperature measurement unit as either F (Fahrenheit) or C (Celsius).

   If this property does not exist in the file, create it.
4. Start Compute Systems Manager.

Result

The temperature measurement unit is updated.

Related references

- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 291

Registering management server firewall exceptions (Windows)

If Windows Firewall is enabled after installing Hitachi Compute Systems Manager, you must register Hitachi Command Suite Common Component services into the Windows Firewall exception list.

Note: If Windows firewall is enabled before you install Compute Systems Manager, the installation program automatically changes the firewall settings.

Procedure

1. From a command prompt, run the following command:
   ```
   HCS-Common-Component-installation-folder\bin\hcmds64fwcancel
   ```
2. After the command finishes processing, run the following command:
   ```
   netsh advfirewall firewall add rule name="HBase(trap)" dir=in
   action=allow program="HCS-Common-Component-installation-
   folder\uCPSB\CC\web\bin\cjstartweb.exe" description="HCS-
   Common-Component-installation-folder\uCPSB\CC\web\bin
   \cjstartweb.exe" enable=yes
   ```
3. Restart Compute Systems Manager.

Result

Compute Systems Manager can now access the required resources through Windows firewall.

Related tasks

- Configuring a firewall for Windows Server 2003 hosts on page 92
- Configuring a firewall for Windows Server 2008 or Windows Server 2012 hosts on page 93

Ports to register as management server firewall exceptions (Linux)

If you changed the port number from the default, make sure that you also change the port number to register as a firewall exception.

The ports that you must register to the firewall exception list are listed in the following table.

Port number (default)	Explanation
162/UDP	Used to receive SNMP traps from management clients. If, during installation, you change the port number to the recommended port number 22601/UDP because 162/UDP is used by another product, you must add the changed port number to the exception list.
22015/TCP	Used for access to the Hitachi Command Suite Common Component service (HBase 64 Storage Mgmt Web Service) during non-SSL communication with management clients (GUI and CLI).
22016/TCP	Used for access to the Hitachi Command Suite Common Component service (HBase 64 Storage

Port number (default)	Explanation
	Mgmt Web Service) when SSL is used for communication with management clients (GUI).
22610/TCP	Used for communication with Hitachi Device Manager.
22611/TCP	Used for receiving alerts from a Hitachi server.

Related tasks

- Registering management server firewall exceptions (Linux) on page 86

Registering management server firewall exceptions (Linux)

If the management server is running Linux and either of the following is true, you must register the port number used in Hitachi Compute Systems Manager into the firewall exception list:

- You install Compute Systems Manager in an environment in which the firewall is enabled.
- You enable the firewall after installing Compute Systems Manager.

Note: The following procedure is an example based on Red Hat Linux v6.2. For details about setting up the firewall for a different version, see the documentation for the applicable operating system.

Procedure

1. In a terminal window, run the `setup` command.
   The Choose a Tool window of the text mode setup utility opens.
2. Select **Firewall configuration**, use the **Tab** key to move to the **Run Tool** button, and then press **Enter**.
   The Firewall Configuration window is displayed.
3. Set **Security Level** to **Enabled** by pressing the **space** key to select **Enabled**, use the **Tab** key to move to the **Customize** button, and then press **Enter**.
   The Firewall Configuration - Customize window opens.
4. In **Other ports** specify the port register as an exception, use the **Tab** key to move to the **OK** button, and then press **Enter.**
   For example,

   ```
   Other ports 162:udp 22015:tcp
   ```

   Note: If a port is already specified, use a space to separate it from the newly added entry.

5. After returning to the Firewall Configuration window, check that **Security Level** is **Enabled**, use the **Tab** key to move to the **OK** button, and then press **Enter**.

Applying WinRM settings (Linux)

If the management server is running Linux, and you specify a value other than the recommended value for `MaxEnvelopeSizekb` and enable WinRM on Windows managed hosts, you must edit a property in the `user.properties` file to apply the WinRM settings.

If the `MaxEnvelopeSizekb` values set on multiple managed hosts are different, you must use the maximum value among these values.

Procedure

1. Stop Compute Systems Manager.
2. Open the following properties file:
   HCSM-installation-directory`/ComputeSystemsManager/conf/user.properties`
3. Set the `MaxEnvelopeSizekb` value that you verified in advance for the `winrm.maxEnvelopeSize` property.
4. Start Compute Systems Manager.

Related tasks

- Enabling WinRM on Windows hosts on page 94
- Starting Hitachi Compute Systems Manager on page 174
- Stopping Hitachi Compute Systems Manager on page 175

Related references

- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 291

4

Configuring management target settings

This module describes how to set up management targets so that they are available for Hitachi Compute Systems Manager (HCSM) host discovery.

- ☐ Setting up power management options for management targets
- ☐ Setting up a Hitachi server target
- ☐ Setting up a Windows management target
- ☐ Setting up a Linux or Solaris management target
- ☐ Updating information after replacing or modifying a managed host
- ☐ Changing the IP address of a chassis management module

Setting up power management options for management targets

By default, Hitachi Compute Systems Manager controls the power functions on managed hosts based on the host lights-out-management (LOM) information. If the host uses Wake-on-LAN (WoL), Compute Systems Manager can power on the host without using the LOM settings.

Enabling Wake-on-LAN

Wake-on-LAN (WoL) is an optional feature that enables a network message to turn on or "wake up" a server. If lights-out-management (LOM) information is not available for a particular host, Hitachi Compute Systems Manager can power on the host using WoL. If you want Compute Systems Manager to maintain the ability to power on a host if LOM information is not available, you must ensure that WoL is enabled on the host network adapter.

To enable WoL on the host network adapter, follow the instructions provided with the host server hardware.

When using WoL, be aware of the following restrictions:

- If there is a switch or router on the network, magic packets might be stopped, and power management might not be possible for the managed host.
- If there is a switch or router on the network and the power is cut, the IP address of the managed host might disappear from the ARP table (magic packet recipient), preventing power management for the managed host.

Related references

- Prerequisites for managing Windows hosts on page 91
- Prerequisites for managing Linux or Solaris hosts on page 98

Enabling lights-out-management monitoring

If you want to monitor the lights-out-management (LOM) module on a managed machine, you must install the Hitachi Server Navigator - Alive Monitor software.

Hitachi Server Navigator - Alive Monitor is an optional feature that enables mutual monitoring between lights-out-management (LOM) and hosts. You can install the Alive Monitor software on Windows and Linux machines. When an error occurs on a managed host, the system sends an alert to Hitachi Compute Systems Manager. When Alive Monitor is running, LOM errors are reported to the host so that Compute Systems Manager also receives alerts for LOM errors.

For information about installing the Alive Monitor software, refer to the Hitachi Server Navigator documentation.

Setting up a Hitachi server target

This section provides information about setting up a Hitachi server management target.

Related references

- Prerequisites for managing a Hitachi blade server on page 91
- Prerequisites for managing a Hitachi rack-mounted server on page 91

Prerequisites for managing a Hitachi blade server

Before you can manage Hitachi blade servers using Hitachi Compute Systems Manager, you must ensure that your blade servers meet the following prerequisites:

- The Hitachi blade server and chassis management module meet the latest firmware requirement. See the Release Notes for details.
- The chassis management module is configured to use the HTTPS port. Use the Element Manager application for checking and configuring HTTPS port settings.

Prerequisites for managing a Hitachi rack-mounted server

Before you can manage Hitachi rack-mounted servers using Hitachi Compute Systems Manager, you must ensure that your rack-mounted servers meet the following prerequisites:

- The Hitachi rack-mounted server LOM module meets the latest firmware requirement. See the Release Notes for details.
- The LOM module is configured to use the HTTPS port. Use the Element Manager application for checking and configuring HTTPS port settings.

Setting up a Windows management target

This module provides information about setting up a Windows management target.

Prerequisites for managing Windows hosts

Before you can manage Windows hosts using Hitachi Compute Systems Manager, you must ensure that your Windows hosts meet the following prerequisites:

- The Windows operating system and all prerequisite software is installed.
- The Windows host hardware meets the minimum requirements specified for Compute Systems Manager target hosts.

- The Windows host runs a version of the Windows operating system that is supported by Compute Systems Manager.
- The account used for remote connections belongs to the Administrators group and is registered on the host.
- Windows Server 2003 hosts are not using Quality of Service Packet Scheduler. If Quality of Service Packet Scheduler is installed, ensure that you disable it before using Compute Systems Manager to monitor performance data. If Quality of Service Packet Scheduler is enabled, Compute Systems Manager cannot monitor network interface card performance data.

After you verify the prerequisites, you must also complete the following setup tasks on the Windows host:

- Configure the Windows firewall (Windows management server).
- Enable WinRM (Linux management server).
- Enable Distributed Component Object Model (DCOM) (Windows management server).
- Set up a remote connection that uses User Access Control (UAC) (optional).
- If managing SAN resources, install the Fibre Channel Information Tool (fcinfo tool) (optional).
- Enable Wake-on-Lan (optional).

Related tasks

- Configuring a firewall for Windows Server 2003 hosts on page 92
- Configuring a firewall for Windows Server 2008 or Windows Server 2012 hosts on page 93
- Enabling DCOM for Windows hosts on page 94
- Enabling WinRM on Windows hosts on page 94
- Setting up a remote connection with UAC on Windows Server 2008 or 2012 on page 95
- Installing the fcinfo tool on Windows Server 2003 (optional) on page 96
- Enabling Wake-on-LAN on page 90
- Configuring a Windows host to send SNMP inband traps (optional) on page 96

Configuring a firewall for Windows Server 2003 hosts

Before Hitachi Compute Systems Manager can communicate with a Windows host, you must configure the Windows Firewall to allow access for Windows Management Instrumentation (WMI) communication if the management server is also running Windows.

Note: If Windows Firewall functionality is disabled, you do not need to configure the firewall.

Procedure

1. Ensure that the host is configured to allow firewall exceptions by using the following command:

   ```
   netsh firewall set opmode mode=ENABLE exceptions=ENABLE
   ```
2. Register the firewall exception for WMI by using the following command:

   ```
   netsh firewall set service RemoteAdmin enable
   ```

Result

WMI communication is now allowed through the firewall so that Compute Systems Manager can communicate with the host.

Related references

- Prerequisites for managing Windows hosts on page 91

Configuring a firewall for Windows Server 2008 or Windows Server 2012 hosts

Before Hitachi Compute Systems Manager can communicate with a Windows host, you must configure the Windows Firewall to allow access for Windows Management Instrumentation (WMI) communication if the management server is also running Windows.

Note: If Windows Firewall functionality is disabled, you do not need to configure the firewall.

Procedure

1. Verify the firewall settings by accessing the Windows **Server Manager** and selecting **Windows Firewall with Advanced Settings Inbound Rules**.
   - If the inbound rules are set to **Allow**, no further steps are required.
   - If the inbound rules are set to **Block**, go to step 3.
   - If the inbound rules are set to **Block all connections**, continue to the next step.
2. If inbound connections is set to **Block all connections**, change the setting:
   - Change the setting to **Allow** if you want to allow all connections. No further steps are required.
   - Change the setting to **Block** (default) if you want to block connections and allow only WMI. Continue to the next step.
3. If you set inbound connections to **Block**, you must enable the WMI rules in the Windows Firewall by using the following command:

   ```
   netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
   ```

Result

WMI communication is now allowed through the firewall so that Compute Systems Manager can communicate with the host.

Related references

- Prerequisites for managing Windows hosts on page 91

Enabling DCOM for Windows hosts

Before Hitachi Compute Systems Manager can obtain the required management information from a host, you must enable Distributed Component Object Model (DCOM) on the host if the management server is running Windows.

Procedure

1. Access the DCOM configuration tool by using the following command:
   `dcomcnfg`
2. In the left pane, expand **Component Services**, and then expand **Computers**.
3. Right-click **My Computer** and select **Properties**.
4. Click the **Default Properties** tab and confirm that the **Enable Distributed COM on this computer** check box is selected.
5. Click the **COM Security** tab and complete the following tasks:
   - In the **Access Permissions** section, click **Edit Limits** and confirm that the **Allow** check box under **Remote Access** is selected for the Everyone group.
   - In the **Launch and Activation Permissions** section, click **Edit Limits** and confirm that the **Allow** check box under **Remote Activation** is selected for the Administrators group.
6. Close the configuration tool and restart the server.

Result

DCOM is enabled on the host so that Compute Systems Manager can obtain server management information.

Related references

- Prerequisites for managing Windows hosts on page 91

Enabling WinRM on Windows hosts

By enabling Windows Remote Management (WinRM), Hitachi Compute Systems Manager you can obtain information from a Windows Server 2008 or Windows Server 2012 host if the management server is running Linux.

Procedure

1. To enable WinRM, run the following commands:

   ```
   winrm qc

   winrm set winrm/config/service @{AllowUnencrypted="true"}

   winrm set winrm/config @{MaxEnvelopeSizekb="512"}
   ```

   Specify a value of 512 (recommended) or larger for `MaxEnvelopeSizekb`. If, however, the number of recognized LUs exceeds 25 for the host that is connected to a Fibre Channel, specify *`number-of-LUs`* `x 20` as the value.
2. To change the port number used by WinRM, run the following commands:

   ```
   winrm delete winrm/config/Listener?Address=*+Transport=HTTP

   winrm create winrm/config/Listener?Address=*+Transport=HTTP
   @{Port="port-number-after-change"}
   ```

   The default port number used by WinRM is 80 or 5985. The default value differs according to the WinRM version.

   If you specify a value other than the recommended (512) for MaxEnvelopeSizekb in the first step, you must edit the properties file on the management server and then apply the WinRM settings.

Related tasks

- Applying WinRM settings (Linux) on page 87

Related references

- Prerequisites for managing Windows hosts on page 91

Setting up a remote connection with UAC on Windows Server 2008 or 2012

Before Hitachi Compute Systems Manager can communicate with a Windows Server 2008 or Windows Server 2012 host using User Access Control (UAC), you must ensure that the management server can establish a remote connection with the host. By default, UAC only allows remote connections using the built-in administrator account or a domain user account. To set up a remote connection that uses a local user account, you must specify that the host allows UAC remote connections.

Note: If the host server uses the built-in administrator account or a domain user account, you do not need to allow remote connections as described in the following task.

To allow remote connections on a host using UAC, use the following command:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies
\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

You do not need to restart the server.

Remote connections are now possible between the management server and the Windows Server 2008 or Windows Server 2012 host using UAC.

Tip: If you need to remove the changes that you made to the registry, use the following command and then restart the server: `reg delete HKLM \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /f`

Related references

- Prerequisites for managing Windows hosts on page 91

Installing the fcinfo tool on Windows Server 2003 (optional)

If you want Hitachi Compute Systems Manager to obtain Fibre Channel SAN resource information from a Windows Server 2003 host, you must install the fcinfo tool. Fcinfo is a command-line tool that enables Compute Systems Manager to obtain Fibre Channel Host Bus Adapter (HBA) information.

Procedure

1. Access the Microsoft download website.
2. Download the fcinfo tool software that corresponds to your Windows server.
3. Follow the `readme.txt` file for instructions about installing the tool.

Result

Compute Systems Manager is now able to obtain HBA information for managed SAN resources.

Related references

- Prerequisites for managing Windows hosts on page 91

Configuring a Windows host to send SNMP inband traps (optional)

If you want Hitachi Compute Systems Manager to monitor inband driver traps on management targets, you must configure specific SNMP-related settings on each Windows host and on the management server.

To configure Windows management targets to send inband driver traps using SNMP:

Procedure

1. Install the Windows SNMP Service on each management target.

The SNMP Service is required to send SNMP Traps when the system detects inband driver events.

For Windows Server 2003:

a. On the management target, log in as an administrator, and then select **Start > Control Panel > Add or Remove Programs > Add/ Remove Windows Components**.

b. Select **Management and Monitoring Tools**, and then click **Details**. Do not select or clear its check box.

c. Select the **Simple Network Management Protocol** check box, click **OK**, and then click **Next**.

For Windows Server 2008:

a. On the management target, log in as an administrator, and then start **Server Manager**.

b. Click **Add Features**.

c. Select **SNMP Service**, click **Next**, and then click **Install**.

For Windows Server 2012:

a. On the management target, log in as an administrator, and then start **Server Manager**.

b. Select **Manage** and then add **Add Roles and features**.

c. Follow the instructions in the window and proceed to **Select Features**.

d. Select **SNMP Service**, click **Next**, and then click **Install**.

2. Configure the Windows SNMP Service so that it sends traps to the Compute Systems Manager server.

a. From the Windows **Services** dialog box, right-click **SNMP Service**, and then select **Properties**.

b. Select the **Traps** tab and under **Community name**, type the case-sensitive community name to which this computer will send trap messages, and then click **Add to list**.

c. Under **Trap destinations**, click **Add**.

d. In the **Host name**, **IP** or **IPX address** field, type the host name or IP address of the Compute Systems Manager server, and then click **Add**.

e. If the port number of the Compute Systems Manager server's SNMP trap listening port is not 162 (the default number), you also need to change the SNMP trap destination port number.

3. Configure trap events for sending inband driver events through the SNMP Service.

a. On the management target, log in as an administrator, and then open a command prompt.

b. From the command prompt, enter the following command:

```
evntcmd Windows-configuration-file-path
```

where *Windows-configuration-file-path* is the path to the `hfcwdd.cnf` file. This file is located in the `\HCSM_SERVER\HCSM\snmp\windows` directory on the Compute Systems Manager installation disk.

4. Repeat this entire procedure for each Windows managed target on which you want to monitor inband events using SNMP.

Related references

- Prerequisites for managing Windows hosts on page 91

Setting up a Linux or Solaris management target

This module provides information about setting up a Linux or Solaris management target.

Prerequisites for managing Linux or Solaris hosts

Before you can manage Linux or Solaris hosts using Hitachi Compute Systems Manager, you must ensure that your Linux or Solaris hosts meet the following prerequisites:

- All prerequisite software is installed.
- Host hardware meets the minimum requirements specified for Compute Systems Manager target hosts.
- Host runs a version of the Linux or Solaris OS that is supported by Compute Systems Manager.
- Linux hosts are running the required software packages as listed in the product Release Notes.

After you verify the prerequisites, you must also complete the following setup tasks on the Linux or Solaris host:

- Set up the account used with Compute Systems Manager.
- Permit access for the Compute Systems Manager IP connection.
- Verify the required Linux or Solaris files and directories.
- Enable Wake-on-Lan (optional).

Related concepts

- About permissions for logging into a Linux or Solaris managed host on page 101

Related tasks

- Setting up an account on a Linux or Solaris host for Hitachi Compute Systems Manager on page 99
- Verifying the Linux or Solaris files and directories on page 99
- Setting up an IP connection with a Linux or Solaris host on page 100
- Setting up root user access for a Linux or Solaris host on page 102
- Setting up permission for normal users to use the Linux or Solaris su command on page 103

- Setting up permission for normal users to use the Linux sudo command on page 104
- Configuring a Linux host to send SNMP inband traps (optional) on page 107
- Enabling Wake-on-LAN on page 90

Verifying the Linux or Solaris files and directories

Before Hitachi Compute Systems Manager can manage Linux or Solaris hosts, you must verify that the required OS files and directories exist on the host.

Procedure

1. Ensure that the following standard OS command paths have not been changed:

   `/sbin`, `/bin`, `/usr/sbin`, `/usr/bin`
2. Confirm that the following directories exist:

   For Linux hosts: `/proc`, `/sys`

   For Solaris hosts: `/proc`, `/system`
3. For Linux hosts, confirm that the following distribution information file exists and has not been changed:

   For Red Hat Linux: `/etc/redhat-release`

   For SUSE Linux: `/etc/SuSE-release`

   For Oracle Linux: `/etc/oracle-release` or `/etc/enterprise-release`

Related references

- Prerequisites for managing Linux or Solaris hosts on page 98

Setting up an account on a Linux or Solaris host for Hitachi Compute Systems Manager

Before Hitachi Compute Systems Manager can communicate with and manage a Linux or Solaris host, you must set up an account on the host specifically for use with Compute Systems Manager.

Procedure

1. Set the login shell to either bash or tcsh:
   - To change the login shell for an existing account, use the `usermod` command.
   - To specify the login shell when creating a new account, use the -s option with the `useradd` command.
2. If any of the following initialization scripts for the Compute Systems Manager account were modified from the default, restore the default scripts that existed when the operating system was installed:

- For bash: `/etc/profile, ~/.bash_profile, ~/.bashrc`
- For tcsh: `/etc/csh.login, /etc/csh.cshrc, ~/.login, ~/.cshrc`

Note: A modified initialization script may cause a failure during host discovery.

Result

Remote connections are now possible between the management server and the Linux or Solaris host.

Related concepts

- About permissions for logging into a Linux or Solaris managed host on page 101

Related references

- Prerequisites for managing Linux or Solaris hosts on page 98

Setting up an IP connection with a Linux or Solaris host

Before Hitachi Compute Systems Manager can communicate with and manage a Linux or Solaris host, you must set up the host to allow an IP connection with the management server using the SSH protocol.

Procedure

1. If the TCP Wrapper functionality is enabled in the operating system, register the IP address of the management server by adding the following entry to the `/etc/hosts.allow` file:

   `sshd:`*`management-server-IP-address`*

   Example entry:

   `sshd:168.1.2.3`
2. Ensure that no other users can connect using the SSH protocol by verifying the settings in the `/etc/ssh/sshd_config` file:
   a. Open the `/etc/ssh/sshd_config` file.
   b. Edit the file so that the settings match the following:

      `PermitRootLogin: yes` (see below for exceptions)

      `PasswordAuthentication: yes`

      `Protocol: "2,1" or "2"`

      Exceptions: Set the `PermitRootLogin` setting to `no` if you are using only normal users for login.
   c. Save and close the file.

3. Execute the following command to restart the daemon:

   For Red Hat Linux 6 or earlier and Oracle Linux 6: `/etc/rc.d/init.d/sshd restart`

   For Red Hat Linux 7 and Oracle Linux 7: `systemctl restart sshd`

   For SUSE Linux: `service sshd restart`

   For Solaris: `svcadm restart ssh`
4. If you set up a firewall on a managed host, change the settings to allow an SSH port connection. For details about firewall settings, see the relevant OS documentation.

Result

The management server can now connect to the Linux or Solaris host by using an SSH IP connection.

Related references

- Prerequisites for managing Linux or Solaris hosts on page 98

About permissions for logging into a Linux or Solaris managed host

Hitachi Compute Systems Manager uses a registered user account on a Linux or Solaris host to access host information. This user account requires root access.

When using Compute Systems Manager, users access Linux or Solaris hosts using one of the following methods. You determine with method to use based on the operations the user must complete and your network environment.

- Access as a root user
  By providing root user access, you ensure that users have the rights to do all tasks. Although this may seem like a simple solution, it is the biggest security risk. To ensure that the root password is kept secure and that the settings of managed resources remain safe, only use root user access if your environment uses precautions that prevent unauthorized access.
- Access as a normal user with root user privileges using the `su` command
  Accessing a host as a normal user with root user privileges using with the `su` command is more secure than accessing hosts as a root user, as long as unauthorized personnel do not obtain the user ID or password. The root user password is required to grant a normal user root user privileges.
- Access as a normal user with root user privileges using the `sudo` command (for Linux) or the `pfexec` command (for Solaris).
  Accessing a host as a normal user with root user privileges using the `sudo` or `pfexec` command is the safest of the three methods, but requires that you set up the `sudo` or `pfexec` command on each managed host. To execute commands with root user privileges, the `sudo` command (for

Linux) or the `pfexec` command (for Solaris) must be set up on the managed host.

Related tasks

- Setting up an account on a Linux or Solaris host for Hitachi Compute Systems Manager on page 99
- Setting up an IP connection with a Linux or Solaris host on page 100
- Setting up root user access for a Linux or Solaris host on page 102
- Setting up permission for normal users to use the Linux or Solaris su command on page 103
- Setting up permission for normal users to use the Linux sudo command on page 104
- Setting up permission for normal users to use the Solaris pfexec command on page 105

Setting up root user access for a Linux or Solaris host

Before Hitachi Compute Systems Manager can communicate with a Linux or Solaris host using the SSH protocol, you must set up login access. If you want Compute Systems Manager to access the Linux or Solaris host using the root user, you must set up root access. Additionally, the root user account needs to have been used to set up IP connections over the SSH protocol.

Note: You do not need to set up root access if you are going to log in to the managed host as a normal user using the Linux `su`, `sudo` or the Solaris `pfexec` command.

Procedure

1. Configure the following managed host authentication information on the Compute Systems Manager management server:
   - IP address: host IP address
   - Port number: host SSH port number
   - User name: root
   - Password: root user password
   - su Password: blank

   For details about how to set up managed hosts by using the management client, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Result

Compute Systems Manager can now communicate with the Linux or Solaris host using root user login access.

Related tasks

- Setting up permission for normal users to use the Linux or Solaris su command on page 103
- Setting up permission for normal users to use the Linux sudo command on page 104

Related references

- Prerequisites for managing Linux or Solaris hosts on page 98

Setting up permission for normal users to use the Linux or Solaris su command

Before Hitachi Compute Systems Manager can communicate with a Linux or Solaris host using the SSH protocol, you must set up login access. If you want normal users (users without root permissions) to log in to the Linux or Solaris host using the su command, you must set up the correct access permissions. A normal user account must be used to set up IP connections over the SSH protocol.

Note: You do not need to complete this setup task if you are going to log in to the managed host as a root user or a normal user using the Linux `sudo` command or the Solaris `pfexec` command.

Procedure

1. Configure the following managed host authentication information on the Compute Systems Manager management server:
   - IP address: host IP address
   - Port number: host SSH port number
   - User name: normal user name
   - Password: normal user password
   - su Password: root user password

   For details about how to set up managed hosts using the Compute Systems Manager interface, see the *Hitachi Command Suite Compute Systems Manager User Guide*.
2. Optionally, you can ensure that root access to the host is not permitted by editing the `/etc/ssh/sshd_config` file on the Linux or Solaris machine and setting the `PermitRootLogin` parameter to `no`.

   Note: Hitachi recommends that you set `PermitRootLogin` to `no` for increased security except if you are running other programs that require root access.

Result

Normal users can now log in to the Linux or Solaris host and use the su command.

Related concepts

- About permissions for logging into a Linux or Solaris managed host on page 101

Related tasks

- Setting up root user access for a Linux or Solaris host on page 102
- Setting up permission for normal users to use the Linux sudo command on page 104

Related references

- Prerequisites for managing Linux or Solaris hosts on page 98

Setting up permission for normal users to use the Linux sudo command

Before Hitachi Compute Systems Manager can communicate with a Linux host using the SSH protocol, you must set up login access. If you want normal users (users without root permissions) to log in to the Linux host using the `sudo` command, you must set up the correct access permissions. A normal user account must be used to set up IP connections over the SSH protocol.

Note: You do not need to complete this setup task if you are going to log in to the managed host as a root user or a normal user using the `su` command.

To set up normal users to log in and use the `sudo` command:

Procedure

1. Add the following definitions to the sudo command settings:

   normal-user-name managed-host-name =NOPASSWD: /usr/sbin/dmidecode

   normal-user-name managed-host-name =NOPASSWD: /usr/sbin/smartctl

   normal-user-name managed-host-name =NOPASSWD: /sbin/ethtool

   normal-user-name managed-host-name =NOPASSWD: /sbin/shutdown

   For Red Hat Linux 6 or later, Oracle Linux 6 or later, SUSE Linux 11 SP1 or later, and SUSE Linux 12 only, also add:

   normal-user-name managed-host-name =NOPASSWD: /usr/sbin/exportfs

For SUSE Linux only, also add:

```
normal-user-name managed-host-name =NOPASSWD: /bin/cat

normal-user-name managed-host-name =NOPASSWD: /bin/df
```

2. Optionally, you can ensure that root access to the host is not permitted by editing the `/etc/ssh/sshd_config` file on the Linux machine and setting the `PermitRootLogin` parameter to `no`.

   Note: Hitachi recommends that you set `PermitRootLogin` to `no` for increased security except if you are running other programs that require root access.

3. Configure the following managed host authentication information on the Compute Systems Manager management server:
   - IP address: host IP address
   - Port number: host SSH port number
   - User name: normal user name
   - Password: normal user password
   - su Password: blank

   For details about how to set up managed hosts using the Compute Systems Manager user interface, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Result

Normal users can now log in to the Linux host and use the sudo command.

Related concepts

- About permissions for logging into a Linux or Solaris managed host on page 101

Related tasks

- Setting up root user access for a Linux or Solaris host on page 102
- Setting up permission for normal users to use the Linux or Solaris su command on page 103

Related references

- Prerequisites for managing Linux or Solaris hosts on page 98

Setting up permission for normal users to use the Solaris pfexec command

Before Hitachi Compute Systems Manager can communicate with a Solaris host using the SSH protocol, you must set up login access. If you want normal users (users without root permissions) to log in to the Solaris host using the `pfexec` command, you must set up the correct access permissions.

A normal user account must be used to set up IP connections over the SSH protocol.

Note: You do not need to complete this setup task if you plan to log in to the managed host as a root user or a normal user using the `su` command.

To set up normal users to log in and use the `pfexec` command:

Procedure

1. Add the following profile definition to the `/etc/security/prof_attr`:
   ```
   HCSM::::
   ```
2. Add the following execution-rights definitions to `/etc/security/exec_attr`:

   For Solaris 10:
   ```
   HCSM:suser:cmd:::/sbin/ifconfig:uid=0;euid=0
   HCSM:suser:cmd:::/usr/sbin/prtvtoc:uid=0;euid=0
   HCSM:suser:cmd:::/usr/sbin/luxadm:uid=0;euid=0
   HCSM:suser:cmd:::/usr/sbin/iscsiadm:uid=0;euid=0
   HCSM:suser:cmd:::/usr/sbin/shutdown:uid=0;euid=0
   ```

   For Solaris 11:
   ```
   HCSM:solaris:cmd:::/usr/sbin/ifconfig:uid=0;euid=0
   HCSM:solaris:cmd:::/usr/sbin/prtvtoc:uid=0;euid=0
   HCSM:solaris:cmd:::/usr/sbin/luxadm:uid=0;euid=0
   HCSM:solaris:cmd:::/usr/sbin/iscsiadm:uid=0;euid=0
   HCSM:solaris:cmd:::/usr/sbin/shutdown:uid=0;euid=0
   ```
3. Execute the following command to apply the profile definition to a normal user:
   ```
   usermod -p HCSM normal-user-name
   ```
4. Optionally, you can ensure that root access to the host is not permitted by editing the `/etc/ssh/sshd_config` file on the Solaris machine and setting the `PermitRootLogin` parameter to `no`.

   Note: Hitachi recommends that you set `PermitRootLogin` to `no` for increased security except if you are running other programs that require root access.

5. Configure the following managed host authentication information on the Compute Systems Manager management server:
   - IP address: host IP address
   - Port number: host SSH port number
   - User name: normal user name
   - Password: normal user password

- su Password: blank

  For details about how to set up managed hosts using the Compute Systems Manager user interface, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Related concepts

- About permissions for logging into a Linux or Solaris managed host on page 101

Related tasks

- Setting up an account on a Linux or Solaris host for Hitachi Compute Systems Manager on page 99
- Setting up an IP connection with a Linux or Solaris host on page 100

Related references

- Prerequisites for managing Linux or Solaris hosts on page 98

Configuring a Linux host to send SNMP inband traps (optional)

If you want Hitachi Compute Systems Manager to monitor inband driver traps on management targets, you must configure specific SNMP-related settings on each Linux host and on the management server.

The following procedure for configuring Linux management targets to send inband SNMP events uses Red Hat Linux v6.2 as an example. For other versions of Linux, replace the Red Hat file names with the file names to apply to your Linux version.

Prerequisites

Before you configure Linux management targets to send inband driver events, install the following packages on each Linux management target:

- lm_sensors-libs
- lm_sensors
- net-snmp-libs
- net-snmp
- net-snmp-utils

To register a MIB file:

To configure Linux management targets to send inband driver events using SNMP:

Procedure

1. Log in to the Linux target machine as a super user, and then back up the following file:

   `/etc/snmp/snmp.conf`

2. If the `snmp.conf` file is not configured correctly on the Linux machine, create a new file by using the following command:

   ```
   snmpconf -g basic_setup
   ```

   Overwrite the `/etc/snmp/snmpd.conf` file with the new `snmpd.conf` file.
3. In the `/etc/snmp/snmpd.conf` file, find the line that starts with `trapsink`, and modify the line as follows:

   ```
   trapsink HCSM-server-address community-name port-number
   ```

   where *HCSM-server-address* is the host name or IP address of the Compute Systems Manager server, *community-name* is a proper SNMP community name, and optional *port-number* is the port number of the Compute Systems Manager server trap listening port. If the port number of the Compute Systems Manager server's SNMP trap listening port is not 162 (the default number), you also need to change the SNMP trap destination port number.

   If there is not such line, add a new line starting with `trapsink`.
4. Access the `hfcldd-snmpd-conf.txt` file located on the Compute Systems Manager installation disk in the following directory:

   ```
   /HCSM_SERVER/HCSM/snmp/linux
   ```
5. Append the contents of `hfcldd-snmpd-conf.txt` file to the end of the following file:

   ```
   /etc/snmp/snmpd.conf
   ```
6. Restart snmpd by entering the following command:

   ```
   /etc/init.d/snmpd restart
   ```
7. Repeat this entire procedure for each Linux management target on which you want to monitor inband events using SNMP.

Related concepts

- About monitoring inband SNMP traps on page 67

Related tasks

- Configuring the management server to receive inband SNMP traps on page 68
- Changing Hitachi Compute Systems Manager ports on page 74

Configuring a Solaris host to send SNMP inband traps (optional)

If you want Hitachi Compute Systems Manager to monitor inband driver traps on management targets, you must configure specific SNMP-related settings on each Solaris host and on the management server.

If you want to use inband SNMP traps to send inband driver event traps from a managed host, you must install SNMP-related packages on the host, and then configure `snmpd`. You must do this on each Solaris host from which you want to send inband driver event traps.

Prerequisites

Before you configure Solaris managed hosts targets to send inband driver events, install the following packages on each Solaris management target:

For Solaris 10:
- SUNWsmagt
- SUNWsmcmd
- SUNWsmdoc
- SUNWsmmgr

For Solaris 11:
- `system/management/snmp/net-snmp`
- `system/management/snmp/net-snmp/addons`

To configure Solaris managed hosts to send inband driver events using SNMP:

Procedure

1. Back up the following files:
   - For Solaris 10:
     `/etc/sma/snmp/snmpd.conf`
   - For Solaris 11:
     `/etc/net-snmp/snmp/snmpd.conf`
2. If the `snmpd.conf` file is not configured correctly on the Solaris host, create a new file by using the following command:
   - For Solaris 10:
     `/usr/sfw/bin/snmpconf –g basic_setup`
   - For Solaris 11:
     `/usr/bin/snmpconf -g basic_setup`

   The `snmpd.conf` file will be overwritten in the new `snmpd.conf` file.
3. In the `snmpd.conf` file, find the line that starts with `trapsink`, and modify the line as follows:

   `trapsink` *`HCSM-server-address community-name port-number`*

   where:
   - *`HCSM-server-address`* is the host name or IP address of the Compute Systems Manager server
   - *`community-name`* is a proper SNMP community name.
   - *`port-number`* is the port number of the Compute Systems Manager server trap listening port (optional). If the port number of the Compute Systems Manager server's SNMP trap listening port is not 162 (the default number), you also need to change the SNMP trap destination port number.

If there is no such line, add a new line starting with `trapsink`.

4. Restart `snmpd` by entering the following command:
   - For Solaris 10:
     `kill -9 snmpd-process-ID`
     `/usr/sfw/sbin/snmpd`
   - For Solaris 11:
     `/usr/sbin/svcadm -v restart net-snmp`
5. Repeat this procedure for each Solaris managed host on which you want to monitor inband events using SNMP.

Related concepts

- About monitoring inband SNMP traps on page 67

Related tasks

- Configuring the management server to receive inband SNMP traps on page 68
- Changing Hitachi Compute Systems Manager ports on page 74

Updating information after replacing or modifying a managed host

If you replace managed hosts by either replacing a motherboard or reassigning an existing managed host IP address, you must run host discovery again to update the new host information. When running host discovery to update host information, you must use specific discovery type settings to ensure that Hitachi Compute Systems Manager obtains all host information updates.

Note: If you reassign an IP address that was previously used only as an IP address assigned to additional network card on a managed host, you must first update the host information using the Refresh option. Then you discover the host without using specific discovery type settings. IP addresses assigned to additional network cards appear only in the host information details on the IP Network tab.

For details about using host discovery to update host information, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Related tasks

- Adding resources to Hitachi Compute Systems Manager on page 56

Changing the IP address of a chassis management module

If you changed the IP address of the chassis management module, specify the new IP address and then re-discover the chassis.

For details about using chassis discovery to update chassis information, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

5

Configuring secure communications

This module describes how to configure secure communications for Hitachi Compute Systems Manager (HCSM).

- ☐ About Hitachi Compute Systems Manager security settings
- ☐ Configuring secure communications for management clients
- ☐ Configuring secure communications for the SMTP server
- ☐ Configuring secure communications for managed servers
- ☐ Configuring secure communications for the Device Manager server
- ☐ About setting up secure communication for an external authentication server
- ☐ Restricting management client access to Hitachi Compute Systems Manager

About Hitachi Compute Systems Manager security settings

You can increase security by using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for Hitachi Compute Systems Manager network communication. SSL or TLS enable Compute Systems Manager to verify communication partners, enhance authentication for identifying partners, and detect falsified data within sent and received information. In addition, communication channels are encrypted so that data is protected from eavesdropping.

Compute Systems Manager can use SSL or TLS for the following types of communication:

- Communication between the management server and management clients
- Communication between the management server and the SMTP server
- Communication between the management server and management targets
- Communication between the management server and the Hitachi Device Manager server
- Communication between the management server and an external authentication server (LDAP directory server)

In addition, you can restrict access so that only specific management clients can access the management server.

Note: When you use Compute Systems Manager with security enabled, make sure that the server certificate is not expired. If the server certificate is expired, you need to register a valid certificate to Compute Systems Manager because users might not be able to connect to it.

Related concepts

- About secure communications for management clients on page 115
- About secure communications for the SMTP server on page 124
- About secure communications for the Device Manager server on page 129

Related tasks

- Setting up SSL on the server for secure client communication on page 115
- Setting up SSL on web-based management clients on page 121
- Setting up SSL on management clients running the CLI on page 122
- Setting up SSL on web-based management clients on page 121
- Setting up SSL for communicating with the Device Manager server on page 130
- Configuring SSL for a secure LDAP server connection on page 141

Configuring secure communications for management clients

This module provides information about setting up secure SSL/TLS communication between the management server and management clients.

About secure communications for management clients

Implement secure communication between the Hitachi Compute Systems Manager management server and management clients using SSL. To implement SSL, first set up SSL on the management server and then on the management clients. The process for setting up SSL on a web-based interface clients is different from CLI clients.

Related tasks

- Setting up SSL on the server for secure client communication on page 115
- Setting up SSL on web-based management clients on page 121
- Setting up SSL on management clients running the CLI on page 122

Setting up SSL on the server for secure client communication

To implement secure communication between the management server and management clients, you must set up SSL on the management server.

Prerequisites

Before setting up SSL on the server, verify the following prerequisites:

- The Web browser version running on the management client is supported by Hitachi Compute Systems Manager.
- The signature algorithm of the server certificates is supported by the management client Web browser.
- The location of the existing private key, certificate signing request, and the self-signed certificate is confirmed (ensure that you check the location when re-creating them).

Verify the following information for the certificate authority that you are using:

- The certificate signing request you created by using the hcmds64ssltool command is in PEM format, and the key size of the private key is 2048 bits.
- The server certificate issued by the certificate authority uses X.509 PEM format and supports the signature algorithm.
- The server certificate application process is understood.

In addition to a private key and a certificate signing request, the following procedure creates a self-signed certificate. We recommend that you use the self-signed certificate for testing purposes only.

Procedure

1. Start Compute Systems Manager.
2. To create a private key (`httpsdkey.pem`), a certificate signing request (`httpsd.csr`), and a self-signed certificate (`httpsd.pem`) for the Hitachi Command Suite Common Component, use the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64ssltool /key *HCS-Common-Component-installation-folder*\uCPSB\httpsd\sslc\bin\demoCA\httpsdkey.pem /csr *HCS-Common-Component-installation-folder*\uCPSB\httpsd\sslc\bin\demoCA\httpsd.csr /cert *HCS-Common-Component-installation-folder*\uCPSB\httpsd\sslc\bin\demoCA\httpsd.pem /certtext *HCS-Common-Component-installation-folder*\uCPSB\httpsd\sslc\bin\demoCA\httpsd.txt /validity 365
   - In Linux:
     HCS-Common-Component-installation-directory/bin/hcmds64ssltool -key *HCS-Common-Component-installation-directory*/uCPSB/httpsd/sslc/bin/demoCA/httpsdkey.pem -csr *HCS-Common-Component-installation-directory*/uCPSB/httpsd/sslc/bin/demoCA/httpsd.csr -cert *HCS-Common-Component-installation-directory*/uCPSB/httpsd/sslc/bin/demoCA/httpsd.pem -certtext *HCS-Common-Component-installation-directory*/uCPSB/httpsd/sslc/bin/demoCA/httpsd.txt -validity 365

   This command outputs the content of the self-signed certificate to `httpsd.txt`. We recommend that you use the self-signed certificate for testing purposes only.

   When you run this command, the signature algorithm uses SHA256 with RSA and creates a self-signed certificate with an expiration day (of 365 days) specified by the `validity` option.

   You can specify the signature algorithm using the `sigalg` option. If you omit this option, SHA256 with RSA is used. In addition, you can also specify SHA1 with RSA or MD5 with RSA.

   Note: If a file with the same name exists in the output destination path, running the `hcmds64ssltool` command overwrites the file. We recommend storing the file in a different destination when you re-create the file.

3. When prompted, enter the following information after the colon(:).
   - Server Name (management server host name) - for example, HCSM_SC1.

- Organizational Unit (section) - for example, Compute Systems Manager.
- Organization Name (company) - for example, Hitachi.
- City or Locality Name - for example, Santa Clara.
- State or Province Name (full name) - for example, California.
- Country Name (2 letter code) - for example, US.

To leave a field blank, type a period (.). To select a default value displayed within the brackets ([]), press **Enter**.

4. Send the certificate signing request (`httpsd.csr`) to the certificate authority to apply for a server certificate.

Note: This step is not required if you plan to use a self-signed certificate, but we recommend that you use a signed server certificate in a production environment.

The server certificate issued by the certificate authority is usually sent by email. Ensure that you save the email and the server certificate sent by the certificate authority.

5. Stop Compute Systems Manager.
6. Copy the private key (`httpsdkey.pem`) and the server certificate or the self-signed certificate (`httpsd.pem`) to the following directory:
   - In Windows:
     HCS-Common-Component-installation-folder\uCPSB\httpsd\conf\ssl\server
   - In Linux:
     HCS-Common-Component-installation-directory/uCPSB/httpsd/conf/ssl/server
7. Open `user_httpsd.conf` file from the following location:
   - In Windows:
     HCS-Common-Component-installation-folder\uCPSB\httpsd\conf\user_httpsd.conf
   - In Linux:
     HCS-Common-Component-installation-directory/uCPSB/httpsd/conf/user_httpsd.conf
8. Within the `user_httpsd.conf` file, do the following:
   a. Uncomment the following lines by removing the hash [#] signs:

      ```
      #Listen 22016

      #<VirtualHost *:22016>
      ```

      through

      ```
      #HWSLogSSLVerbose On
      ```

with the exception of `#SSLCACertificateFile`, which must remain commented out.

The following is an example of editing `user_httpsd.conf`:

```
ServerName host-name
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName host-name
SSLEnable
SSLProtocol TLSv1 TLSv11 TLSv12
SSLRequiredCiphers AES256-SHA256:AES256-SHA:AES128-
SHA256:AES128-SHA:DES-CBC3-SHA
SSLRequireSSL
SSLCertificateKeyFile
"HCS-Common-Component-installation-directory/uCPSB/httpsd/
conf/ssl/server/httpsdkey.pem"
SSLCertificateFile
"HCS-Common-Component-installation-directory/uCPSB/httpsd/
conf/ssl/server/httpsd.pem"
# SSLCACertificateFile
"HCS-Common-Component-installation-directory/uCPSB/httpsd/
conf/ssl/cacert/anycert.pem"
</VirtualHost>
HWSLogSSLVerbose On
```

b. Edit the following lines as required:

ServerName in the first line

ServerName in the <VirtualHost> tag

SSLCertificateKeyFile

SSLCertificateFile

#SSLCACertificateFile

When using a chained server certificate issued from a certificate authority, delete the hash sign (#) from the line "# SSLCACertificateFile", and specify the chained certificate file (created by certificate authority) by using an absolute path.

Note: To block non-SSL communication from external servers to the management server, comment out the lines `Listen 22015` and `Listen [::]:22015` by adding a hash mark (#) to the beginning of each line. After you comment out these lines, remove the hash mark (#) from the line `#Listen 127.0.0.1:22015`.

To block non-SSL communication within the management server, close the HBase 64 Storage Mgmt Web Service port.

The following is an example of how to edit the `user_httpsd.conf` file. The numbers represent the default ports.

```
ServerName host-name
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName host-name
SSLEnable
SSLProtocol TLSv1 TLSv11 TLSv12
SSLRequiredCiphers AES256-SHA256:AES256-SHA:AES128-
SHA256:AES128-SHA:DES-CBC3-SHA
SSLRequireSSL
SSLCertificateKeyFile
"HCS-Common-Component-installation-directory/uCPSB/httpsd/
conf/ssl/server/httpsdkey.pem"
SSLCertificateFile
"HCS-Common-Component-installation-directory/uCPSB/httpsd/
conf/ssl/server/server-certificate-or-self-signed-
certificate-file"
# SSLCACertificateFile
"HCS-Common-Component-installation-directory/uCPSB/httpsd/
conf/ssl/cacert/certificate-file-from-certificate-authority"
</VirtualHost>
HWSLogSSLVerbose On
```

9. Start Compute Systems Manager.
10. Update the Compute Systems Manager URL using the `hcmds64chgurl` command as follows:
    - Change the protocol from http: to https:
    - Change the port number used for secure communication.

Result

SSL is now implemented on the Compute Systems Manager server.

Related concepts

- About secure communications for management clients on page 115

Related tasks

- Setting up SSL on web-based management clients on page 121
- Setting up SSL on management clients running the CLI on page 122
- Closing the non-SSL communication port on page 120

Related references

- Properties related to web server communication including SSL settings (user_httpsd.conf) on page 298

Closing the non-SSL communication port

To close the non-SSL communication port (default: 22015) for HBase 64 Storage Mgmt Web Service when SSL communication is enabled between the management server and management clients, you must change the settings in the `user_httpsd.conf` file and register the server certificate to the management server.

Prerequisites

Before starting the process of closing the non-SSL communication port, complete the following prerequisite tasks:

- Verify the host name
  Verify that the host name set to the CN line of the certificate signing request is the same as the `ServerName` property on the first line of the `user_httpsd.conf` file.
- Change the name resolution setting
  Update your configuration settings so that the system can resolve the IP address from the management server host name that is set as the `ServerName` property on the first line of the `user.httpsd.conf` file.
  To verify that the IP address resolves to the hostname, run the following command:
  `ping` *`management-server-host-name`*
- Enable SSL communication on the management server.

Procedure

1. Open `user_httpsd.conf`:
   - In Windows:
     `HCS-Common-Component-installation-folder``\uCPSB\httpsd\conf\user_httpsd.conf`
   - In Linux:
     `HCS-Common-Component-installation-directory``/uCPSB/httpsd/conf/user_httpsd.conf`
2. In the `user_httpsd.conf` file, specify a hash mark (#) on the lines below to comment the lines out. The example below shows how to edit the `user_httpsd.conf` file. The numbers indicate the default port number.

```
:
#Listen 22015
#Listen [::]:22015
#Listen 127.0.0.1:22015
```

```
#SSLDisable
:
#<VirtualHost *:22016>
# ServerName host-name
:
#</VirtualHost>
```

3. Run the following command to import the server certificate into the truststore (`jssecacerts`):
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64keytool -import -alias *unique-name-in-the-truststore* -file *HCS-Common-Component-installation-folder*\uCPSB\httpsd\conf\ssl\server*server-certificate-file* -keystore *HCS-Common-Component-installation-folder*\uCPSB\jdk\jre\lib\security\jssecacerts -storepass *password-to-access-the-truststore*
   - In Linux:
     HCS-Common-Component-installation-directory/uCPSB/jdk/bin/keytool -import -alias *unique-name-in-the-truststore* -file *HCS-Common-Component-installation-directory*/uCPSB/httpsd/conf/ssl/server/*server-certificate-file* -keystore *HCS-Common-Component-installation-directory*/uCPSB/jdk/jre/lib/security/jssecacerts -storepass *password-to-access-the-truststore*
4. Verify the contents of the imported truststore.
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64ssltool -list -v -keystore *HCS-Common-Component-installation-folder*\uCPSB\jdk\jre\lib\security\jssecacerts -storepass *truststore-password*
   - In Linux:
     HCS-Common-Component-installation-directory/bin/hcmds64ssltool -list -v -keystore *HCS-Common-Component-installation-directory*/uCPSB/jdk/jre/lib/security/jssecacerts -storepass *truststore-password*
5. Restart Compute Systems Manager.
6. Verify that you can log in to the Compute Systems Manager user interface.

Related concepts

- About secure communications for management clients on page 115

Setting up SSL on web-based management clients

To implement secure communications between the management server and management clients, you must set up SSL on all Hitachi Compute Systems Manager management clients that access the Compute Systems Manager web-based user interface. You must have already set up SSL on the

management server and is only required the first time you access the management server from this client.

Prerequisites

If the signature algorithm used is SHA256 with RSA, the Web browser in use must support a server certificate that has an SHA256 with RSA signature.

Procedure

1. From the management web client, access the management server using an SSL connection by typing the following URL:
   `https://`*`HCSM-management-server-name`*`:`*`port-number-for-SSL-communication`*`/ComputeSystemsManager/`
2. Install the SSL certificate.

Result

The SSL certificate is registered on the management client so it can communicate with the management server using SSL.

Related concepts

- About secure communications for management clients on page 115

Related tasks

- Setting up SSL on the server for secure client communication on page 115
- Setting up SSL on management clients running the CLI on page 122

Setting up SSL on management clients running the CLI

To implement secure communication between the management server and management clients, you must set up SSL on all Hitachi Compute Systems Manager management clients that access the server using the CLI. You must have already set up SSL on the management server and is only required the first time you access the management server from this client.

Procedure

1. Save the Compute Systems Manager server certificate that is stored in the following directory to a temporary directory on the Compute Systems Manager CLI host.
   - In Windows:
     `HCS-Common-Component-installation-folder``\uCPSB\httpsd\conf\ssl\server`
   - In Linux:
     `HCS-Common-Component-installation-directory``/uCPSB/httpsd/conf/ssl/server`

2. From a command prompt on the Compute Systems Manager CLI host, import the Compute Systems Manager server certificate to the truststore (`cacerts`) using the following command:
   - In Windows:
     jre-installation-folder`\bin\keytool -importcert -trustcacerts -alias` *unique-name-in-the-truststore* `-file` *server-certificate-file* `-keystore` *jre-installation-folder*`\lib\security\cacerts -storepass changeit`
   - In Linux:
     jre-installation-directory`/bin/keytool -importcert -trustcacerts -alias` *unique-name-in-the-truststore* `–file` *server-certificate-file* `-keystore` *jre-installation-directory*`/lib/security/cacerts -storepass changeit`

   where:
   - *server-certificate-file* is the server certificate that you saved in step 1.
   - `changeit` is the default keystore password for the truststore (`cacerts`). If you receive an invalid password error, confirm the password with an administrator.
3. To set the Compute Systems Manager server location, use the following command:
   - In Windows:
     CLI-installation-folder`\csm configure`
   - In Linux:
     CLI-installation-directory`/csm configure`
4. When prompted, enter the following information:

   `HCSM server host name:` *HCSM-server-name*

   `Use SSL:` `y`

   `HCSM server port number:` *port-number-for-SSL-communication*

Result

The SSL server certificate is registered on the management client so it can communicate with the management server using SSL.

Related concepts

- About secure communications for management clients on page 115

Related tasks

- Setting up SSL on the server for secure client communication on page 115
- Setting up SSL on web-based management clients on page 121

Configuring secure communications for the SMTP server

This module provides information about configuring secure SSL/TLS communication between the management server and the SMTP server, which manages e-mail.

Related concepts

- About secure communications for the SMTP server on page 124
- About secure communications for management clients on page 115

About secure communications for the SMTP server

If the SMTP server uses a server certificate, you can use SSL communication for information sent between the management server and the SMTP server. You implement secure communication between the Hitachi Compute Systems Manager management server and the SMTP server by registering the SMTP server certificate on the management server.

Related concepts

- About Hitachi Compute Systems Manager security settings on page 114
- About Hitachi Compute Systems Manager security settings on page 114

Related tasks

- Setting up SSL for communicating with the SMTP server on page 124

Setting up SSL for communicating with the SMTP server

To implement secure communication between the management server and the SMTP server, you must register the SMTP certificate on the management server.

Procedure

1. Copy the SMTP certificate file to a temporary directory on the management server.
2. On the management server, register the SMTP server certificate by running the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64keytool -import -alias *unique-name-in-the-truststore* -file *SMTP-certificate-file*(PEM-format-or-DER-format) -keystore *HCS-Common-Component-installation-folder*\uCPSB\jdk\jre\lib\security\jssecacerts -storepass *truststore-password*
   - In Linux:
     HCS-Common-Component-installation-directory/uCPSB/jdk/bin/keytool -import -alias *unique-name-in-the-truststore* -file

```
SMTP-certificate-file(PEM-format-or-DER-format) -keystore
HCS-Common-Component-installation-directory/
uCPSB/jdk/jre/lib/security/jssecacerts -storepass
truststore-password
```

3. Restart Compute Systems Manager.
4. From a management client, use a browser to log in to Compute Systems Manager.
5. From the **Administration** tab, select **System Settings > E-mail > Edit Settings > Advanced Settings** and set the **SSL communication port** to the same port number that is set on the SMTP server.

   For details about e-mail notification settings, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Result

The SSL certificate is registered on the management server so that it can communicate with the SMTP server using SSL.

Related concepts

- About secure communications for the SMTP server on page 124
- About secure communications for management clients on page 115

Configuring secure communications for managed servers

This module provides information about improving the security of the secure SSL/TLS communication for managed servers sending alerts to the management server.

About secure communication for managed servers

Secure SSL communication for communication between Hitachi servers (including an LPAR manager on a blade server) and the Hitachi Compute Systems Manager management server is enabled by default.

There are no additional steps required to implement SSL secure communication for servers unless you want to improve communications security for alerts sent by the server. You can strengthen security by creating an additional self-signed certificate or obtaining a new server certificate from a certificate authority. If you choose to use a new certificate, you must update the management server SSL information from the Compute Systems Manager user interface.

Strengthening security for managed server alert communication

To increase the level of security for alert communications sent from a Hitachi Compute Systems Manager server (including an LPAR manager on a blade server), you can create a keystore and import a server certificate or a self-

signed certificate. To further increase security, you can also import the certificate for a Hitachi server to the keystore of the management server.

Prerequisites

Before updating the SSL configuration on the server, verify the following prerequisites:

- If you plan to install a certificate for a Hitachi server, you must first obtain the certificate from the Hitachi server. For details on how to obtain the certificate, see the Hitachi server documentation.

Verify the following information for the certificate authority that you are using:

- The certificate signing request you created by using the hcmds64ssltool command is in PEM format, and the key size of the private key is 2048 bits.
- The server certificate issued by the certificate authority uses X.509 PEM format and supports the signature algorithm.
- The server certificate application process is understood.

Procedure

1. Stop Compute Systems Manager.
2. Create a new keystore using the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64keytool -genkey -keystore *HCSM-installation-folder* \ComputeSystemsManager\conf\ssl*keystore-file-name* -storepass *keystore-password* -keypass *secret-key-password* -keyalg RSA -keysize 2048 -sigalg SHA256withRSA -validity *valid-days-of-certificate* -alias *unique-name-in-keystore*
   - In Linux:
     HCS-Common-Component-installation-directory/uCPSB/jdk/bin/keytool -genkey -keystore *HCSM-installation-directory*/ComputeSystemsManager/conf/ssl/*keystore-file-name* -storepass *keystore-password* -keypass *secret-key-password* -keyalg RSA -keysize 2048 -sigalg SHA256withRSA -validity *valid-days-of-certificate* -alias *unique-name-in-keystore*
3. If you want to use a self-signed certificate, go to step 7. If you want to use a server certificate issued by a certificate authority, use the following command to create a certificate signing request:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64keytool -certreq -file *certificate-signing-request-file-name* -keystore *HCSM-installation-folder*\ComputeSystemsManager \conf\ssl*keystore-file-name* -storepass *keystore-password* -keypass *secret-key-password* -alias *unique-name-in-keystore*

- In Linux:
  HCS-Common-Component-installation-directory/uCPSB/jdk/bin/keytool -certreq -file *certificate-signing-request-file-name* -keystore *HCSM-installation-directory*/ComputeSystemsManager/conf/ssl/*keystore-file-name* -storepass *keystore-password* -keypass *secret-key-password* -alias *unique-name-in-keystore*

  When specifying the alias, use the alias specified in step 2.

4. Send the certificate signing request (httpsd.csr) to the certificate authority to apply for a server certificate.

   The server certificate issued by the certificate authority is usually sent by email. Ensure that you save the email and the server certificate sent by the certificate authority.

5. To import the certificate of the certificate authority to the keystore, use the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64keytool -import -file *certificate-file-of-certificate-authority* -keystore *HCSM-installation-folder*\ComputeSystemsManager\conf\ssl*keystore-file-name* -storepass *keystore-password* -alias *unique-name-in-keystore*
   - In Linux:
     HCS-Common-Component-installation-directory/uCPSB/jdk/bin/keytool -import -file *certificate-file-of-certificate-authority* -keystore *HCSM-installation-directory*/ComputeSystemsManager/conf/ssl/*keystore-file-name* -storepass *keystore-password* -alias *unique-name-in-keystore*

     When specifying the alias, use a name other than the alias specified in step 2.
6. To import the server certificate issues by the certificate authority to the keystore, run the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64keytool -import -file *server-certificate-file* -keystore *HCSM-installation-folder*\ComputeSystemsManager\conf\ssl*keystore-file-name* -storepass *keystore-password* -alias *unique-name-in-keystore*
   - In Linux:
     HCS-Common-Component-installation-directory/uCPSB/jdk/bin/keytool -import -file *server-certificate-file* -keystore *HCSM-installation-directory*/ComputeSystemsManager/conf/ssl/*keystore-file-name* -storepass *keystore-password* -alias *unique-name-in-keystore*

     When specifying the alias, use the alias specified in step 2.
7. To import the certificate for the Hitachi Server to the keystore, run the following command:

- In Windows:
  HCS-Common-Component-installation-folder\bin\hcmds64keytool -import -file *certificate-file-for-Hitachi-server* -keystore *HCSM-installation-folder*\ComputeSystemsManager\conf\ssl*keystore-file-name* -storepass *keystore-password* -alias *unique-name-in-keystore*
- In Linux:
  HCS-Common-Component-installation-directory/uCPSB/jdk/bin/keytool -import -file *certificate-file-for-Hitachi-server* -keystore *HCSM-installation-directory*/ComputeSystemsManager/conf/ssl/*keystore-file-name* -storepass *keystore-password* -alias *unique-name-in-keystore*

  When specifying the file, you must use the path of a PEM-format or DER-format certificate file.

  When specifying the alias, use an alias other than specified in step 2 and step 5.

8. Open the `user.properties` file:
   - In Windows:
     HCSM-installation-folder\ComputeSystemsManager\conf\user.properties
   - In Linux:
     HCSM-installation-directory/ComputeSystemsManager/conf/user.properties
9. For the `hcsm.keystore.filename` property, specify the name of the keystore file that you created.
10. If you import a certificate for a Hitachi server in step 3, locate the `hcsm.certification.verify` property and specify Enable. If you do not see the property in the file, add it.
11. If you migrate LPARs and want to enable encrypted communication only between the management server and the LPAR manager, specify Disable for the `hvm.lpar.migration.allow.plaintext` property. If you do not see the property in the file, add it.
12. Save the file and start Compute Systems Manager.
13. From a management client, log in to Compute Systems Manager and enable the new keystore. For details, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Tip: To obtain the Compute Systems Manager server certificate (used for Hitachi Server communication) from the keystore, run the following command:

In Windows:

HCS-Common-Component-installation-folder\bin\hcmds64keytool -exportcert -file *certificate-file-to-export* -keystore *HCSM-installation-folder*

`\ComputeSystemsManager\conf\ssl\`*`keystore-file-name`* `-storepass` *`keystore-password`* `-alias` *`unique-name-in-keystore`*

In Linux:

`HCS-Common-Component-installation-directory/``uCPSB/jdk/bin/keytool -exportcert -file` *`certificate-file-to-export`* `-keystore` *`HCSM-installation-directory/`*`ComputeSystemsManager/conf/ssl/`*`keystore-file-name`* `-storepass` *`keystore-password`* `-alias` *`unique-name-in-keystore`*

When specifying the variable for the `alias` option, specify the same unique name you specified in step 2.

Result

The management server now uses the new self-signed certificate to increase security for alert transmissions sent by a server.

Related concepts

- About setting up secure communication for an external authentication server on page 131

Configuring secure communications for the Device Manager server

This module describes how to configure secure communications for the Hitachi Device Manager server.

About secure communications for the Device Manager server

When connecting to Hitachi Device Manager, you can use SSL communication for communication between the management server and the Device Manager server. You implement secure communication between the Hitachi Compute Systems Manager management server and the Device Manager server by registering the Device Manager server certificate on the management server.

Related concepts

- About Hitachi Compute Systems Manager security settings on page 114

Related tasks

- Setting up SSL for communicating with the Device Manager server on page 130

Setting up SSL for communicating with the Device Manager server

To implement secure communication between the management server and the Hitachi Device Manager server, you must register the Device Manager certificate on the management server.

Procedure

1. Copy the Device Manager certificate file to a temporary directory on the management server.
2. On the management server, register the Device Manager server certificate by running the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64keytool -import -alias *unique-name-in-the-truststore* -file *Device-Manager-certificate-file*(PEM-format-or-DER-format) -keystore *HCS-Common-Component-installation-folder*\uCPSB\jdk\jre\lib\security\jssecacerts -storepass *truststore-password*
   - In Linux:
     HCS-Common-Component-installation-directory/uCPSB/jdk/bin/keytool -import -alias *unique-name-in-the-truststore* -file *Device-Manager-certificate-file*(PEM-format-or-DER-format) -keystore *HCS-Common-Component-installation-directory*/uCPSB/jdk/jre/lib/security/jssecacerts -storepass *truststore-password*
3. Restart Compute Systems Manager.
4. From a management client, use a browser to log in to Compute Systems Manager.
5. From the **Administration** tab, select **Logical Partitioning > Automatic Registration for Migration WWPNs** and confirm that the communication protocol is set to HTTPS.

   For details about automatic registration for migration WWPNs, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Result

The SSL certificate is registered on the management server so that it can communicate with the Device Manager server using SSL.

Related concepts

- About secure communications for the Device Manager server on page 129
- About secure communications for management clients on page 115

Related tasks

- Starting Hitachi Compute Systems Manager on page 174
- Stopping Hitachi Compute Systems Manager on page 175

About setting up secure communication for an external authentication server

Use the StartTLS protocol to implement secure communication between the Hitachi Compute Systems Manager management server and the LDAP directory server. To implement StartTLS, you must update the properties in the `exauth.properties` file and import the LDAP directory server certificate into the management server.

Related tasks

- Strengthening security for managed server alert communication on page 125

Restricting management client access to Hitachi Compute Systems Manager

This module provides information about restricting management server access from management clients.

Related concepts

- About restricting management client access to Hitachi Compute Systems Manager on page 131

About restricting management client access to Hitachi Compute Systems Manager

You can increase Hitachi Compute Systems Manager security by controlling access to the Compute Systems Manager server. You control access by allowing only specific management clients to log in to the management server. To allow a management client access to the management server, modify the access setting for the client in the `user_httpsd.conf` file. The restriction is enforced for the web user interface and the command line interface (CLI).

Related tasks

- Restricting management server access from a management client on page 131

Restricting management server access from a management client

You can control access to the Hitachi Compute Systems Manager management server by restricting management client access. By default, all clients can access the Compute Systems Manager management server. You can configure the Compute Systems Manager server to allow access only by

specific management clients. The restriction is enforced for the web-based user interface and the CLI.

Note: If you log in to a Hitachi Command Suite product other than Compute Systems Manager on a management client that is not registered in the `user_httpsd.conf` file, you cannot start the Compute Systems Manager GUI from the management client GUI.

To restrict management clients from accessing the management server:

Procedure

1. Stop Compute Systems Manager.
2. Open the following file:
   - In Windows:
     HCS-Common-Component-installation-folder\uCPSB\httpsd\conf\user_httpsd.conf
   - In Linux:
     HCS-Common-Component-installation-directory/uCPSB/httpsd/conf/user_httpsd.conf
3. In the last line of the `user_httpsd.conf` file, add the `<Location /ComputeSystemsManager>` property, which enables you to specify which management clients are allowed to access the management server.
4. Close and save the file.
5. Start Compute Systems Manager.

Result

The management clients that are not explicitly allowed access in the `user_httpsd.conf` file are restricted.

Related concepts

- About restricting management client access to Hitachi Compute Systems Manager on page 131

Related references

- Properties related to web server communication including SSL settings (user_httpsd.conf) on page 298

6

Configuring external authentication

This module describes how to configure a connection with an external LDAP server for authentication.

- ☐ Overview of external authentication and external authorization
- ☐ LDAP directory server data structure models
- ☐ Prerequisites for configuring an LDAP directory server connection
- ☐ Connecting to an LDAP directory server
- ☐ Connecting to a Kerberos server
- ☐ Settings for connecting to an LDAP server
- ☐ Settings for connecting to a Kerberos server
- ☐ Commands for connecting to an external authentication server
- ☐ Using an LDAP search user account when connecting to an LDAP server
- ☐ LDAP certificates for secure communications

Overview of external authentication and external authorization

This module provides conceptual information about using an external authentication and external authorization server with Hitachi Compute Systems Manager.

About using an external authentication server

When using Hitachi Command Suite products, you can authenticate users by connecting to one or more external authentication servers.

If you register the user IDs stored on the external authentication server with Hitachi Compute Systems Manager, you can use the same user IDs to log in to Compute Systems Manager. This means that you do not have to manage login passwords and control accounts in Compute Systems Manager. Compute Systems Manager supports connections with both LDAP directory servers and Kerberos servers.

You can connect directly to an LDAP directory server or use a DNS server to obtain information about the LDAP server. If you use a DNS server, be aware that user logins might take more time. In addition, if you use a DNS server, you cannot set up secure communication with the LDAP server.

Related concepts

- About using an external authorization server on page 134
- Workflow for setting up an LDAP directory server on page 28

Related tasks

- Configuring an LDAP server connection on page 139

About using an external authorization server

If you use both an external authentication server and an external authorization server for your Hitachi Command Suite products, you can control users' access permissions for Hitachi Compute Systems Manager by using the external authorization server.

If you also connect the management server to an external authorization server, you do not need to manage accounts and set permissions for individual users because Compute Systems Manager manages users by authenticating groups on the external authorization server. Set up access to the external authorization server by configuring a connection between Compute Systems Manager and an LDAP directory server.

Related concepts

- About using an external authentication server on page 134

- Workflow for setting up an LDAP directory server on page 28

Related tasks

- Configuring an LDAP server connection on page 139

LDAP directory server data structure models

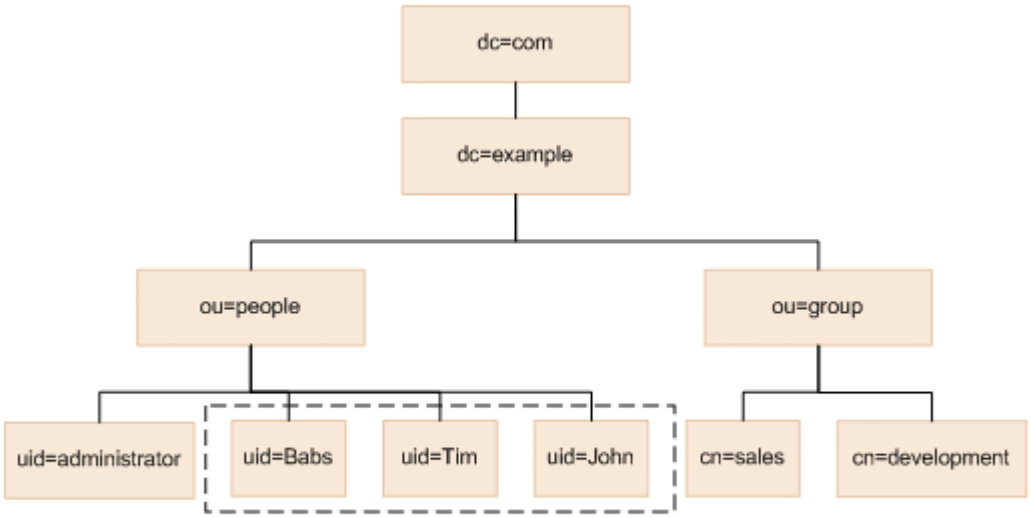
This module provides conceptual information about LDAP directory server data structure models, which determine the Hitachi Compute Systems Manager properties settings that you need to configure by connecting to an LDAP server.

LDAP server flat data structure model

Before you set up a connection to an LDAP directory server, you must determine the LDAP server data structure and associated authentication method. In a flat structure model, the LDAP user data is stored in a structure with a single flat entry below the Base DN.

If the LDAP server uses the flat model, the entries below the Base DN structure are searched for an entry that matches the DN that consists of a combination of the login ID and Base DN. If the user value is found, the user is authenticated.

The following figure shows an example of the flat model. The user entities enclosed within the dotted line can be authenticated. In this example, Base DN is ou=people,dc=example,dc=com because all of the user entries are located just below ou=people.



Legend: The use entities enclosed by the dotted line can be authenticated.

If, however, either of the following conditions exists, you must specify the settings as if a hierarchical structure model exists, regardless of whether the server uses a flat model:

- A user attribute value other than the RDN attribute value is used as the user ID of a Compute Systems Manager user (for example, the Windows logon ID).
- The RDN attribute value of a user ID entry includes a character that is invalid in a Compute Systems Manager user ID. When using the authentication method for the flat model, the RDN attribute value of a user entry functions as the user ID for Compute Systems Manager. Therefore, if the RDN attribute value of a user entry includes an invalid Compute Systems Manager character, you cannot use the authentication method for the flat model. The following is an example of a valid RDN:
  The following is an example of a valid RDN:
  uid=John123S
  cn=John_Smith
  The following is an example of an invalid RDN:
  uid=John:123S (colon required)
  cn=John Smith (a space between John and Smith required)

Related concepts

- LDAP server hierarchical data structure model on page 136
- LDAP data structure Base DN on page 137

Related tasks

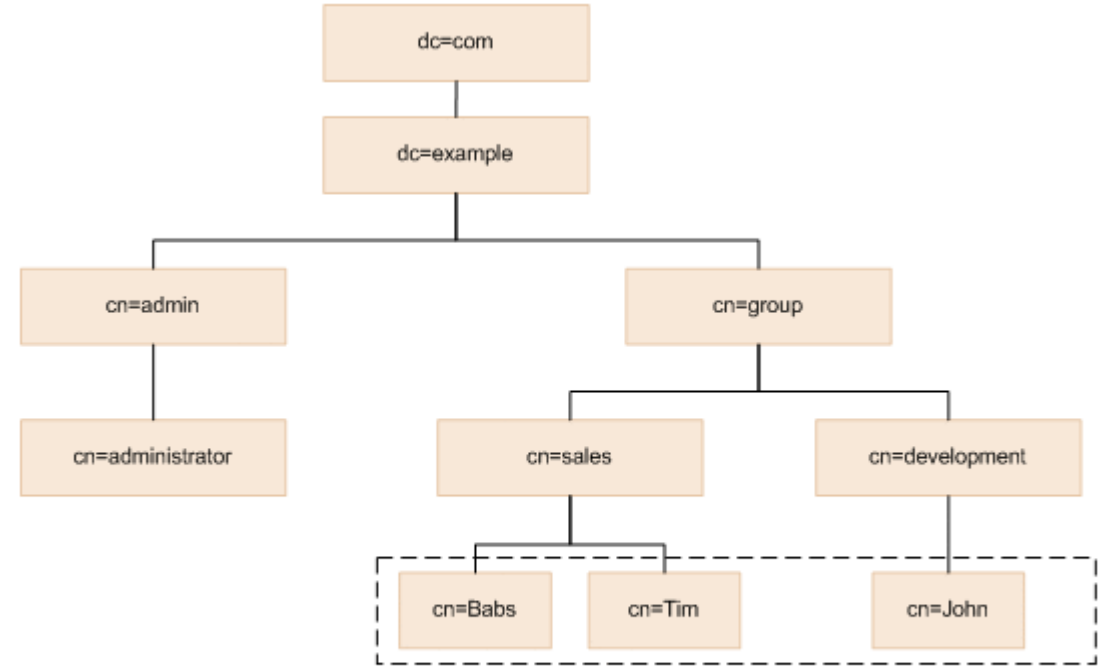
- Prerequisites for determining LDAP server connection properties on page 138

LDAP server hierarchical data structure model

Before you set up a connection to an LDAP directory server, you must determine the LDAP server data structure and associated authentication method. In a hierarchical structure model, the LDAP data is stored in a tree-like structure where user entries are registered in various branches off the root or Base DN.

If the LDAP server uses the hierarchical structure model, the entries below the Base DN in the hierarchy are searched for an entry that matches the login ID and user attribute value specified in the authentication request. If the user is found, the user is authenticated.

The following figure shows an example of the hierarchical structure model. The user entries enclosed within the dotted line can be authenticated. In this example, the Base DN is cn=group,dc=example,dc=com because the target user entries extend across two departments (cn=sales and cn=development).



Legend: The user entities enclosed by the dotted line can be authenticated.

Related concepts

- LDAP server flat data structure model on page 135
- LDAP data structure Base DN on page 137

Related tasks

- Prerequisites for determining LDAP server connection properties on page 138

LDAP data structure Base DN

If you set up a connection to an LDAP directory server, you must specify the LDAP server data structure Base DN, which is the starting point when searching for a user requesting authentication.

Specify the Base DN in the `exauth.properties` file located on the Hitachi Compute Systems Manager management server. Only user entries located below the BaseDN in the hierarchy are searched for authentication purposes. Ensure that all users you want to authenticate for Compute Systems Manager are in this hierarchy.

Related concepts

- LDAP server hierarchical data structure model on page 136
- LDAP server flat data structure model on page 135

Related tasks

- Prerequisites for determining LDAP server connection properties on page 138

Prerequisites for configuring an LDAP directory server connection

This module provides information about the required prerequisites for configuring Hitachi Compute Systems Manager to use an external LDAP directory server for authentication.

Prerequisites for determining LDAP server connection properties

Before you can set up a connection to an external LDAP directory server using the Hitachi Compute Systems Manager connection properties, you must identify the following LDAP server information:

- Data structure type and authentication method.
  The LDAP directory server uses the following two data structure models:
  - Hierarchical structure model
  - Flat model
- Data structure BaseDN
  The BaseDN is the starting point when searching for a user requesting authentication.

Related concepts

- LDAP server hierarchical data structure model on page 136
- LDAP server flat data structure model on page 135
- LDAP data structure Base DN on page 137

Related tasks

- Configuring an LDAP server connection on page 139

Prerequisites for using a DNS server to connect to an LDAP server

If you plan to set up a connection to an LDAP server by using a DNS server to obtain LDAP server information, verify the following:

- DNS Server environment settings are configured on the OS of the LDAP directory server.
- A Service Record (SRV record) is registered on the DNS server for the LDAP directory server. This record contains the host name, port number, and domain name of the LDAP directory server.

Note: If you use a DNS server to look up the LDAP directory server, user logins might take longer.

Related tasks

- Configuring an LDAP server connection on page 139

Related references

- Settings for using DNS to connect to an LDAP server on page 148
- Settings for connecting directly to an LDAP server and an authorization server on page 149

Connecting to an LDAP directory server

This module provides information about configuring Hitachi Compute Systems Manager to use an external LDAP directory server for authentication.

Configuring an LDAP server connection

When using Hitachi Compute Systems Manager, you can connect to an external server for authentication. To configure a connection with an external LDAP directory server for authentication, you must complete tasks on the LDAP server, the management server, and the management clients.

Procedure

1. Identify the LDAP directory server data structure model (hierarchical or flat). The property settings differ depending on the model type.
2. Determine whether to connect directly to an LDAP server or to use a DNS server to obtain LDAP server information. The property settings differ depending on whether you connect directly or use a DNS server.
3. Verify that there is a registered user account on the LDAP server for use with Compute Systems Manager. If not, you must register a Compute Systems Manager user account on the LDAP server by using the instructions in the LDAP server documentation. Be aware of the following user account restrictions:
   - User IDs and passwords must consist of characters that can be used in Compute Systems Manager. Specify a maximum of 256 characters using the following valid characters:
     0 to 9, A to Z, a to z,! # $ % & ' ( ) * + - . = @ \ ^ _ |
   - In Compute Systems Manager, user IDs are not case-sensitive. The combination of character types for passwords must follow the settings on the external authentication server.
4. On the Compute Systems Manager management server, edit the properties in the `exauth.properties` file to set up the LDAP server connection parameters.
5. If the LDAP server uses a hierarchical data structure or Compute Systems Manager connects to an external authorization server (in addition to an external authentication server), register a user account on

the management server for searching LDAP user information by using the following command.

- In Windows:
  HCS-Common-Component-installation-folder\bin\hcmds64ldapuser /set /dn *LDAP-search-user-account* [/pass *LDAP-search-user-account-password*] /name *server-identification-name*
- In Linux:
  HCS-Common-Component-installation-directory/bin/hcmds64ldapuser -set -dn *LDAP-search-user-account* [-pass *LDAP-search-user-account-password*] -name *server-identification-name*

Note: This step is not necessary except in the preceding cases because LDAP user information is not searched during authentication and authorization. If a user account used to search for LDAP user information already exists, delete it.

6. Select one of the following options for configuring user accounts and permissions based on your Compute Systems Manager implementation:
   - If Compute Systems Manager connects to an external authentication server only, use the Compute Systems Manager user interface to create user accounts, specify access control settings for management targets, and optionally, change the user authentication method for existing users.
   - If Compute Systems Manager connects to an external authorization server in addition to an authentication server, use the Compute Systems Manager user interface to register authorization groups and permissions.

   For details and step-by-step procedures for all of these options, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Result

The Compute Systems Manager management server is now connected to an external LDAP directory server for authentication.

Related tasks

- Prerequisites for determining LDAP server connection properties on page 138
- Verifying an LDAP server connection on page 143
- Configuring SSL for a secure LDAP server connection on page 141
- Deleting an LDAP search user on page 161

Related references

- Prerequisites for using a DNS server to connect to an LDAP server on page 138
- Prerequisites for registering a search user on page 158
- Settings for connecting directly to an LDAP server on page 147
- Settings for using DNS to connect to an LDAP server on page 148
- About using commands to connect to an external authentication server on page 155
- Command format for registering a search user on page 159

Configuring SSL for a secure LDAP server connection

After you configure a connection to an external LDAP directory server for authentication, you can increase security by implementing StartTLS secure communication between the LDAP server and the Hitachi Compute Systems Manager management server.

Procedure

1. Verify that you have completed the steps required to set up a connection to the LDAP directory server.
2. On the Compute Systems Manager management server, edit the `exauth.properties` file to specify secure communication in the following parameter fields:
   - `auth.ocsp.enable` (optional)
   - `auth.ocsp.responderURL` (optional)
   - `auth.ldap.ServerName.protocol` (required)
3. If you changed the property value for either `auth.ocsp.enable` or `auth.ocsp.responderURL`, you must restart the Compute Systems Manager services. Other changes do not require restarting the services.
4. To determine whether the LDAP directory server certificate has already been set up for Hitachi Command Suite Common Component, use the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64keytool -list -v keystore *HCS-Common-Component-installation-folder*\uCPSB\jdk\jre\lib\security\cacerts -storepass *password-for accessing-truststore*
   - In Linux:
     HCS-Common-Component-installation-directory/uCPSB/jdk/bin/keytool -list -v keystore *HCS-Common-Component-installation-directory*/uCPSB/jdk/jre/lib/security/cacerts -storepass *password-for accessing-truststore*

   The default password is “changeit”.

5. If the settings are already configured, you are finished. Otherwise, obtain the LDAP directory server certificate from the LDAP server.

   For details, see the LDAP directory server documentation.
6. Verify that the LDAP directory server certificate adheres to the certificate criteria set in the Hitachi Command Suite Common Component truststore.
7. Import the LDAP directory server certificate to the Hitachi Command Suite truststore by using the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64keytool -import -alias *unique-name-in-the-truststore* -file *certificate-file* -keystore *truststore-file-name* -storepass *password-for-accessing-truststore*
   - In Linux:
     HCS-Common-Component-installation-directory/uCPSB/jdk/bin/keytool -import -alias *unique-name-in-the-truststore* -file *certificate-file* -keystore *truststore-file-name* -storepass *password-for-accessing-truststore*

   Note: You can import multiple certificate files by specifying alias names not used in the truststore.
8. Verify the contents of the imported truststore by using the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64keytool -list -v -keystore *truststore-filename* -storepass *password-for-accessing-truststore*
   - In Linux:
     HCS-Common-Component-installation-directory/uCPSB/jdk/bin/keytool -list -v -keystore *truststore-filename* -storepass *password-for-accessing-truststore*
9. Restart Compute Systems Manager.

Result

The Compute Systems Manager management server now connects to an external LDAP directory server using a secure connection.

Related tasks

- Configuring an LDAP server connection on page 139
- Verifying an LDAP server connection on page 143

Related references

- Prerequisites for configuring a secure LDAP server connection on page 161

- Settings for connecting directly to an LDAP server on page 147
- Settings for connecting directly to an LDAP server and an authorization server on page 149
- Command format for registering a search user on page 159
- Command format for importing LDAP server certificates on page 162

Verifying an LDAP server connection

After you complete the required steps for configuring a connection with an LDAP server, you can use the `hcmds64checkauth` command on the management server to verify that the management server can connect to the external authentication server and the external authorization server.

Procedure

1. Verify the connection to the external authentication and authorization servers using the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64checkauth [/user *user-ID*][/pass *password*] [/summary]
   - In Linux:
     HCS-Common-Component-installation-directory/bin/hcmds64checkauth [-user *user-ID*][-pass *password*] [-summary]

   If the user ID or password is omitted, the user is prompted for a user ID and password. Type them as instructed by the message.
2. After you confirm the connection, verify that you can log into Compute Systems Manager.

Related tasks

- Configuring an LDAP server connection on page 139
- Configuring SSL for a secure LDAP server connection on page 141

Related references

- Command format for verifying an external server connection on page 156

Connecting to a Kerberos server

This section explains how to use Kerberos with Hitachi Compute Systems Manager.

Encryption types for Kerberos authentication

When using a Kerberos authentication server with Hitachi Command Suite products, you must ensure that the Kerberos server uses a supported encryption type.

Hitachi Command Suite products support the following Kerberos authentication encryption types:

- AES256-CTS
- AES128-CTS
- RC4-HMAC
- DES3-CBC-SHA1
- DES-CBC-CRC
- DES-CBC-MD5

If the external authentication server is running Windows Server 2008 or Windows Server 2012 and the environment meets both of the following conditions, user authentication might not work properly:

- Authentication server domain functional level is set to Windows Server 2003 or Windows 2000.
- Management server operating system supports AES128-CTS encryption.

For example, if the domain functional level of Active Directory is set to Windows Server 2003 or Windows 2000, the system cannot authenticate the corresponding user using Active Directory in either of the following cases:

- An existing user is migrated to a new Active Directory system with a Windows Server 2003 domain functional level and then the user password is changed.
- A Windows Server 2003 Active Directory system is migrated to an Active Directory system running on Windows Server 2008 or Windows Server 2012 with a domain functional level of Windows Server 2003 and a migrated user password is changed.

To resolve both of these issues, you must change the `default_tkt_enctypes` property setting in the `exauth.properties` file as follows:

```
auth.kerberos.default_tkt_enctypes=rc4-hmac
```

Related references

- Settings for connecting directly to a Kerberos server on page 151
- Settings for using DNS to connect to a Kerberos server and an authorization server on page 154

Configuring a Kerberos server connection

When using Hitachi Compute Systems Manager, you can connect to an external server for authentication. To configure a connection with an external Kerberos server for authentication, you must complete tasks on the Kerberos server, the management server, and the management clients.

Procedure

1. Determine whether to connect directly to a Kerberos server or to use a DNS server to obtain Kerberos server information. The property settings differ depending on whether you connect directly or use a DNS server.
2. Verify that there is a registered user account on the Kerberos server for use with Compute Systems Manager. If not, you must register a Compute Systems Manager user account on the Kerberos server by using the instructions in the Kerberos server documentation. Be aware of the following user account restrictions:
   - User IDs and passwords must consist of characters that can be used in Compute Systems Manager. Specify a maximum of 256 characters using the following valid characters:
     0 to 9, A to Z, a to z,! # $ % & ' ( ) * + - . = @ \ ^ _ |
   - In Compute Systems Manager, user IDs are not case-sensitive. The combination of character types for passwords must follow the settings on the external authentication server.
3. On the Compute Systems Manager management server, edit the properties in the `exauth.properties` file to set up the Kerberos server connection parameters.

   HCS-Common-Component-installation-directory\conf\exauth.properties
4. If Compute Systems Manager connects to an external authorization server (in addition to an external authentication server), register a user account on the management server for searching Kerberos server user information by using the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64ldapuser /set /dn *LDAP-search-user-account* [/pass *LDAP-search-user-account-password*] /name *server-identification-name*
   - In Linux:
     HCS-Common-Component-installation-directory/bin/hcmds64ldapuser -set -dn *LDAP-search-user-account* [-pass *LDAP-search-user-account-password*] -name *server-identification-name*

   Note: If Compute Systems Manager connects only to an external authentication server, user information searches will not be performed for authentication. Therefore, this procedure is not necessary. If you already registered a user account, delete the user account.
5. Select one of the following options for configuring user accounts and permissions based on your Compute Systems Manager implementation:

- If Compute Systems Manager connects to an external authentication server only, use the Compute Systems Manager user interface to create user accounts, specify access control settings for management targets, and optionally, change the user authentication method for existing users.
- If Compute Systems Manager connects to an external authorization server in addition to an authentication server, use the Compute Systems Manager user interface to register authorization groups and permissions.

For details and step-by-step procedures for all of these options, see the *Hitachi Command Suite Compute Systems Manager User Guide*.

Result

The Compute Systems Manager management server is now connected to an external Kerberos server for authentication.

Related concepts

- About using an external authentication server on page 134

Related tasks

- Verifying a Kerberos server connection on page 146
- Deleting an LDAP search user on page 161

Related references

- Command format for verifying an external server connection on page 156
- Prerequisites for registering a search user on page 158
- Command format for registering a search user on page 159

Verifying a Kerberos server connection

After you complete the required steps for configuring a connection with a Kerberos server, you can use the `hcmds64checkauth` command on the management server to verify that the management server can connect to the external authentication server and the external authorization server.

Note: If you plan to use StartTLS communication with the Kerberos server, ensure that you complete the security configuration before verifying the connectivity.

Procedure

1. Verify the connection to the external authentication and authorization servers using the following command:
   - In Windows:

HCS-Common-Component-installation-folder\bin\hcmds64checkauth [/user *user-ID*][/pass *password*] [/summary]

- In Linux:
  HCS-Common-Component-installation-directory/bin/hcmds64checkauth [-user *user-ID*] [-pass *password*] [-summary]

If the user ID or password is omitted, the user is prompted for a user ID and password. Type them as instructed by the message.

2. After you confirm the connection, verify that you can log into Compute Systems Manager.

Related tasks

- Configuring a Kerberos server connection on page 144
- Configuring SSL for a secure LDAP server connection on page 141

Related references

- Properties related to Kerberos server connections (exauth.properties) on page 313

Settings for connecting to an LDAP server

This module provides information about the properties that you specify when configuring a connection to an external LDAP directory server.

Settings for connecting directly to an LDAP server

To configure a direct connection with an external LDAP directory server for authentication, edit the properties in the `exauth.properties` file on the Hitachi Compute Systems Manager management server. The following table lists the property values required for an implementation where you connect the Compute Systems Manager management server directly to an LDAP directory server (connecting only to an external authentication server).

Property	Setting Details
`auth.server.type`	ldap
`auth.server.name`	Server identification name of the LDAP server
`auth.group.mapping`	false
`auth.ocsp.enable`	false To use StartTLS communication, change the setting as required.
`auth.ocsp.responderURL`	By default, this entry is blank. To use StartTLS communication, change the setting as required.

Property	Setting Details
auth.ldap.*ServerName*.protocol	ldap To use StartTLS communication, change the setting to tls.
auth.ldap.*ServerName*.host	Host name or IP address of the LDAP server
auth.ldap.*ServerName*.port	Port number of the LDAP server
auth.ldap.*ServerName*.timeout	Amount of time to wait before an LDAP directory server connection time-out
auth.ldap.*ServerName*.attr	Name of the attribute that defines the user ID value included in the certificate
auth.ldap.*ServerName*.basedn	DN (Base DN)
auth.ldap.*ServerName*.retry.interval	Retry interval when LDAP server communication fails
auth.ldap.*ServerName*.retry.times	Number of times to retry a connection when LDAP server communication fails
auth.ldap.*ServerName*.dns_lookup	false

Related tasks

- Configuring an LDAP server connection on page 139

Related references

- Properties related to LDAP directory server connections (exauth.properties) on page 306
- Example properties file for external LDAP directory server connections (exauth.properties) on page 310

Settings for using DNS to connect to an LDAP server

To configure a connection with an external LDAP directory server for authentication, edit the properties in the `exauth.properties` file on the Hitachi Compute Systems Manager management server. The following table lists the property values required for an implementation where you connect the Compute Systems Manager management server to an LDAP directory server using DNS (connecting only to an external authentication server).

Property	Setting Details
auth.server.type	ldap
auth.server.name	Server identification name of the LDAP server
auth.group.mapping	false
auth.ldap.*ServerName*.protocol	ldap

Property	Setting Details
auth.ldap.*ServerName*.timeout	Amount of time to wait before an LDAP directory server connection time-out
auth.ldap.*ServerName*.attr	Name of the attribute that defines the user ID value included in the certificate
auth.ldap.*ServerName*.basedn	DN (Base DN)
auth.ldap.*ServerName*.retry.interval	Retry interval when LDAP server communication fails
auth.ldap.*ServerName*.retry.times	Number of times to retry a connection when LDAP server communication fails
auth.ldap.*ServerName*.domain.name	Name of the domain managed by the LDAP server
auth.ldap.*ServerName*.dns_lookup	true

Related tasks

- Configuring an LDAP server connection on page 139

Related references

- Prerequisites for using a DNS server to connect to an LDAP server on page 138
- Properties related to LDAP directory server connections (exauth.properties) on page 306
- Example properties file for external LDAP directory server connections (exauth.properties) on page 310

Settings for connecting directly to an LDAP server and an authorization server

To configure a direct connection with an external LDAP directory server for authentication and with an external authorization server, edit the properties in the `exauth.properties` file on the Hitachi Compute Systems Manager management server. The following table lists the property values required for an implementation where you connect the Compute Systems Manager management server directly to an LDAP directory server and to an external authorization server.

Property	Setting Details
auth.server.type	ldap
auth.server.name	Server identification name of the LDAP server
auth.group.mapping	true
auth.ocsp.enable	false To use StartTLS communication, change the setting as required.

Property	Setting Details
auth.ocsp.responderURL	By default, this entry is blank. To use StartTLS communication, change the setting as required.
auth.ldap.*ServerName*.protocol	ldap To use StartTLS communication, change the setting to tls.
auth.ldap.*ServerName*.host	Host name or IP address of the LDAP server
auth.ldap.*ServerName*.port	Port number of the LDAP server
auth.ldap.*ServerName*.timeout	Amount of time to wait before an LDAP directory server connection time-out
auth.ldap.*ServerName*.attr	Name of the attribute that defines the user ID value included in the certificate
auth.ldap.*ServerName*.basedn	DN (Base DN)
auth.ldap.*ServerName*.retry.interval	Time interval for retries when LDAP server communication fails
auth.ldap.*ServerName*.retry.times	Number of times to retry a connection when LDAP server communication fails
auth.ldap.*ServerName*.domain.name	Name of the domain managed by the LDAP server
auth.ldap.*ServerName*.dns_lookup	false

Related tasks

- Configuring an LDAP server connection on page 139

Related references

- Properties related to LDAP directory server connections (exauth.properties) on page 306
- Example properties file for external LDAP directory server connections (exauth.properties) on page 310

Settings for using DNS to connect to an LDAP server and an authorization server

To configure a connection with an external LDAP directory server for authentication and an external authorization server, edit the properties in the exauth.properties file on the Hitachi Compute Systems Manager management server. The following table lists example settings for an implementation where you connect the Compute Systems Manager management server to an LDAP directory server using DNS and to an external authorization server.

Property	Setting Details
auth.server.type	ldap
auth.server.name	Server identification name of the LDAP server
auth.group.mapping	true
auth.ldap.*ServerName*.protocol	ldap
auth.ldap.*ServerName*.timeout	Amount of time to wait before an LDAP directory server connection time-out.
auth.ldap.*ServerName*.attr	Name of the attribute that defines the user ID value included in the certificate.
auth.ldap.*ServerName*.basedn	DN (Base DN)
auth.ldap.*ServerName*.retry.interval	Retry interval when LDAP server communication fails
auth.ldap.*ServerName*.retry.times	Number of times to retry a connection when LDAP server communication fails
auth.ldap.*ServerName*.domain.name	Name of the domain managed by the LDAP server
auth.ldap.*ServerName*.dns_lookup	true

Related tasks

- Configuring an LDAP server connection on page 139

Related references

- Prerequisites for using a DNS server to connect to an LDAP server on page 138
- Properties related to LDAP directory server connections (exauth.properties) on page 306
- Example properties file for external LDAP directory server connections (exauth.properties) on page 310

Settings for connecting to a Kerberos server

This module provides information about the properties that you specify when configuring a connection to a Kerberos server.

Settings for connecting directly to a Kerberos server

To configure a direct connection with an external Kerberos server for authentication, edit the properties in the `exauth.properties` file on the Hitachi Compute Systems Manager management server. The following table lists the property values required for an implementation where you connect the Compute Systems Manager management server directly to a Kerberos server (connecting only to an external authentication server).

Property	Setting Details
auth.server.type	kerberos
auth.group.mapping	false
auth.ocsp.enable	false To use StartTLS communication, change the setting as required.
auth.ocsp.responderURL	By default, this entry is blank. To use StartTLS communication, change the setting as required.
auth.kerberos.default_realm	Realm name
auth.kerberos.dns_lookup_kdc	false
auth.kerberos.default_tkt_enctypes	Encryption type used for Kerberos authentication
auth.kerberos.clockskew	Acceptable time difference range between the management server and the Kerberos server
auth.kerberos.timeout	Amount of time to wait before a Kerberos server connection time-out
auth.kerberos.realm_name	Realm identifier
auth.kerberos.*auth.kerberos.realm_name-property-value*.realm	Realm name
auth.kerberos.*auth.kerberos.realm_name-property-value*.kdc	Host name or IP address[:port-number] of the Kerberos server

Related tasks

- Configuring a Kerberos server connection on page 144

Related references

- Encryption types for Kerberos authentication on page 143
- Properties related to Kerberos server connections (exauth.properties) on page 313

Settings for using DNS to connect to a Kerberos server

To configure a connection with an external Kerberos server for authentication, edit the properties in the `exauth.properties` file on the Hitachi Compute Systems Manager management server. The following table lists the property values required for an implementation where you connect the Compute Systems Manager management server to a Kerberos server using DNS (connecting only to an external authentication server).

Property	Setting Details
auth.server.type	kerberos

Property	Setting Details
auth.group.mapping	false
auth.kerberos.default_realm	Realm name
auth.kerberos.dns_lookup_kdc	true
auth.kerberos.default_tkt_enctypes	Encryption type used for Kerberos authentication
auth.kerberos.clockskew	Acceptable time difference range between the management server and the Kerberos server
auth.kerberos.timeout	Amount of time to wait before a Kerberos server connection time-out

Related tasks

- Configuring a Kerberos server connection on page 144

Related references

- Encryption types for Kerberos authentication on page 143
- Properties related to Kerberos server connections (exauth.properties) on page 313

Settings for connecting directly to a Kerberos server and an authorization server

To configure a direct connection with an external Kerberos server for authentication and with an external authorization server, edit the properties in the exauth.properties file on the Hitachi Compute Systems Manager management server. The following table lists the property values required for an implementation where you connect the Compute Systems Manager management server directly to a Kerberos server and to an external authorization server.

Property	Setting Details
auth.server.type	kerberos
auth.group.mapping	true
auth.kerberos.default.realm	Realm name
auth.kerberos.dns_lookup_kdc	false
auth.kerberos.clockskew	Acceptable range for the time difference between the management server and the Kerberos server.
auth.kerberos.timeout	Amount of time to wait before the Kerberos server connection times out.
auth.ocsp.enable	false To use StartTLS communication, change the setting as required.

Property	Setting Details
auth.ocsp.responderURL	By default, this entry is blank. To use StartTLS communication, change the setting as required.
auth.kerberos.realm_name	Realm identifier
auth.kerberos.*auth.kerberos.realm_name-property-value*.realm	Realm name
auth.kerberos.*auth.kerberos.realm_name-property-value*.kdc	Host name or IP address[:port-number] for the Kerberos server
auth.group.*realm-name*.protocol	ldap When using a StartTLS connection, change the value to tls.
auth.group.*realm-name*.port	Port number for the Kerberos server
auth.group.*realm-name*.basedn	DN (BaseDN)
auth.group.*realm-name*.timeout	Waiting time to connect to the LDAP directory server
auth.group.*realm-name*.retry.interval	Time interval for retries when LDAP directory server communication fails
auth.group.*realm-name*.retry.times	Number of retries for failed connections with the LDAP directory server

Related tasks

- Configuring a Kerberos server connection on page 144

Related references

- Properties related to Kerberos server connections (exauth.properties) on page 313

Settings for using DNS to connect to a Kerberos server and an authorization server

To configure a connection with an external Kerberos server for authentication and an external authorization server, edit the properties in the exauth.properties file on the Hitachi Compute Systems Manager management server. The following table lists example settings for an implementation where you connect the Compute Systems Manager management server to a Kerberos server using DNS and to an external authorization server.

Property	Setting Details
auth.server.type	kerberos
auth.group.mapping	true

Property	Setting Details
auth.kerberos.default_realm	Realm name
auth.kerberos.dns_lookup_kdc	true
auth.kerberos.clockskew	Acceptable time difference range between the management server and the Kerberos server
auth.kerberos.timeout	Amount of time to wait before a Kerberos server connection timeout

Related tasks

- Configuring a Kerberos server connection on page 144

Related references

- Properties related to Kerberos server connections (exauth.properties) on page 313

Commands for connecting to an external authentication server

This module provides guidelines, rules, and syntax for the commands you use to connect to an external authentication server.

About using commands to connect to an external authentication server

If using command line arguments for specifying an external authentication server, you must follow specific guidelines.

If you include command-line control characters in the arguments of commands that specify the settings for connecting to an external authentication server, you must escape the characters correctly according to the command line specifications. If using command-line control characters, be aware of the following restrictions:

In Windows:

- If you include the following characters in an argument, enclose the argument in double quotation marks (") or use a caret (^) to escape each character:
  Spaces & | ^ < > ( )
- Backslashes (\) included in the arguments are treated specially in the command line.
  - A backslash might be treated as an escape character depending on the character that follows it.

Therefore, if a backslash *and* any of the characters are included in an argument, use a caret to escape each character rather than enclose the argument in double quotation marks.
    - If there is a backslash at the end of an argument, escape it using another backslash.

In Linux:

- If you include the following characters in an argument, enclose the argument in double quotation marks (") or use a backslash (\) to escape each character:
  Spaces # & ' ( ) ~ \ ` < > ; |
  Note that a backslash in an argument is treated as an escape character even if the argument is enclosed in double quotation marks. If a backslash is included in an argument, escape it by using another backslash.

Related tasks

- Configuring an LDAP server connection on page 139
- Configuring a Kerberos server connection on page 144

Related references

- Command format for verifying an external server connection on page 156

Command format for verifying an external server connection

You can use the `hcmds64checkauth` command on the management server to verify that the management server can connect to the external authentication server and the external authorization server as follows:

- In Windows:
  HCS-Common-Component-installation-folder\bin\hcmds64checkauth [/user *user-ID*][/pass *password*] [/summary]
- In Linux:
  HCS-Common-Component-installation-directory/bin/hcmds64checkauth [-user *user-ID*][-pass *password*] [-summary]

If the user ID or password is omitted, the user is prompted for a user ID and password. Type them as instructed by the message.

When typing the user ID or password, ensure that you adhere to the following rules:

- Both must match the ID and password of the user account that you registered for checking connections with the external authentication and external authorization servers.
  When using LDAP authentication, specify the same *user-ID* that is listed in the `auth.ldap.`*auth.server.name-property-value*`.attr` in the `exauth.properties` file.

When using Kerberos authentication and connecting to an external authentication server only, specify a user account that is registered in a Hitachi Command Suite product for use with Kerberos authentication. When using Kerberos authentication and also connecting to an external authorization server, specify a user account that is not registered in a Hitachi Command Suite product for use with Kerberos authentication.
- You cannot specify a user account with a user-ID or password that begins with a forward slash (/).

Important: If you are using Kerberos authentication and the realm name is specified multiple times in the `exauth.properties` file, check the user account for each realm. In addition, specify the user ID using the following format:
- When specifying a user who does not belong to the realm specified for `default_realm` in the `exauth.properties` file, specify the realm name in addition to the user ID.
- When specifying a user who belongs to the realm specified as the `default_realm` in the `exauth.properties` file, specify the user ID only (you can omit the realm name).

If you run the command with the summary option specified, the confirmation message is displayed in summary format.

The results from the `hcmds64checkauth` command are divided into the following four phases:
- Phase 1: The command verifies that common properties are correctly specified in the `exauth.properties` file.
- Phase 2: The command verifies that the properties for the external authentication server and the external authorization server are correctly specified in the `exauth.properties` file.
- Phase 3: The command verifies that the management server can connect to the external authentication server.
- Phase 4: If the management server is also linked to an external authorization server, the command verifies that the management server can connect to the external authorization server and can search authorization groups.

Related references

- About using commands to connect to an external authentication server on page 155
- Settings for connecting directly to an LDAP server on page 147
- Settings for connecting directly to a Kerberos server on page 151
- Settings for connecting directly to an LDAP server and an authorization server on page 149
- Settings for connecting directly to a Kerberos server and an authorization server on page 153

- Settings for using DNS to connect to an LDAP server and an authorization server on page 150
- Settings for using DNS to connect to a Kerberos server and an authorization server on page 154

Using an LDAP search user account when connecting to an LDAP server

This module provides information about registering and managing an LDAP search user account.

Prerequisites for registering a search user

When setting up a connection to an LDAP directory server, you must configure a user account for searching LDAP information on the LDAP directory server. The user account requirements are as follows:

Note: Property settings that include "DN" differ depending on the authentication method as follows:

- For LDAP authentication, the DN specified in `auth.ldap.`*`auth.server.name-property-value`*`.basedn`.
- For Kerberos authentication, the DN specified in `auth.group.`*`realm-name`*`.basedn`.

- Account can bind to the DN.
- Account can reference the DN.
- Account can reference authorized groups under the DN (when also linking with an external authorization server)
- Account can search the attributes for all entries below the DN as well as attributes for nested groups of authorized groups (when also linking with an external authorization server).
- Account ID does not include double quotation marks. This is supported on the LDAP server, but not on the Hitachi Compute Systems Manager management server.

Note: If you are using Active Directory, you can use the `dsquery` command provided by Active Directory to check the DN of a user with administrative rights:

```
dsquery user -name administrator
```

Related tasks

- Checking the registration status of an LDAP search user on page 160
- Configuring an LDAP server connection on page 139
- Configuring a Kerberos server connection on page 144

Related references

- Command format for registering a search user on page 159

Command format for registering a search user

Before registering a user account for searching user information using the `hcmds64ldapuser` command, review the command format guidelines for creating the user account.

The format of the `hcmds64ldapuser` command is as follows:

- In Windows:
  HCS-Common-Component-installation-folder\bin\hcmds64ldapuser /set /dn *LDAP-search-user-account* [/pass *LDAP-search-user-account-password*] /name *server-identification-name*
- In Linux:
  HCS-Common-Component-installation-directory/bin/hcmds64ldapuser -set -dn *LDAP-search-user-account* [-pass *LDAP-search-user-account-password*] -name *server-identification-name*

The command parameters are as follows:

- *DN*—specifies the DN of the user by following the standards described in RFC4514.

  Note: If the DN contains one or more commas, such as in cn=administrator,cn=admin,dc=example,com, specify the DN as follows: `hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example\,com" /pass administrator_pass /name Server-Name`

- *Password*—specifies the password for the user account that must exactly match the password registered on the authentication server, including case. If the password is omitted, the user is prompted for a password. Type the password as instructed by the prompt message.
- *Server identification name*—the name differs depending on the authentication method.
  For LDAP authentication use the server identifier for the LDAP directory server:
  - Specify the server identifier that has been specified for the `auth.server.name` property in the `exauth.properties` file.

  For Kerberos authentication, use the realm name of the server:
  - If you directly specify the Kerberos server information in the `exauth.properties` file, specify the value of `auth.kerberos.default_realm` or the value of `auth.kerberos.`*`auth.kerberos.realm_name-property-value`*`.realm`

- If you set the configuration to refer to the DNS server for the Kerberos server information in the `exauth.properties` file, specify the realm name that has been registered in the DNS server.

The following example command, based on a hierarchical structure model, assumes that the user account is "administrator" (with permissions for searching all users under the Base DN), the DN is "cn=administrator,cn=admin,dc=example,dc=com", and the password is "administrator_pass":

- In Windows:
  ```
  hcmds64ldapuser /set /dn
  "cn=administrator,cn=admin,dc=example,dc=com" /pass
  administrator_pass /name Server-Name
  ```
- In Linux:
  ```
  hcmds64ldapuser -set -dn
  "cn=administrator,cn=admin,dc=example,dc=com" -pass
  administrator_pass -name Server-Name
  ```

In Windows, if a comma is included in the DN, for example "`cn=administrator,cn=admin,dc=example,com`", add "\" before each comma when specifying the DN, as follows:

```
hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example
\,com" /pass administrator_pass /name ServerName
```

In Linux, one backslash (\) is processed as an escape character. To specify one backslash as a character, two backslashes must be specified, as follows:

```
hcmds64ldapuser -set -dn "cn=administrator,cn=admin,dc=example\
\,com" -pass administrator_pass -name ServerName
```

Related tasks

- Configuring an LDAP server connection on page 139
- Configuring a Kerberos server connection on page 144
- Deleting an LDAP search user on page 161

Related references

- Prerequisites for registering a search user on page 158

Checking the registration status of an LDAP search user

To determine the names of LDAP directory servers for which the LDAP search user is registered, use the following command on the management server:

- In Windows:
  ```
  HCS-Common-Component-installation-folder\bin\hcmds64ldapuser /
  list
  ```
- In Linux:

HCS-Common-Component-installation-directory/bin/hcmds64ldapuser -list

Related tasks

- Configuring an LDAP server connection on page 139
- Configuring a Kerberos server connection on page 144
- Deleting an LDAP search user on page 161

Related references

- Prerequisites for registering a search user on page 158
- Command format for registering a search user on page 159

Deleting an LDAP search user

To delete an LDAP search user account, use the following command on the management server:

- In Windows:
  HCS-Common-Component-installation-folder\bin\hcmds64ldapuser /delete /name *server-identification-name*
- In Linux:
  HCS-Common-Component-installation-directory/bin/hcmds64ldapuser -delete -name *server-identification-name*

Related tasks

- Configuring SSL for a secure LDAP server connection on page 141

Related references

- Command format for registering a search user on page 159

LDAP certificates for secure communications

This module provides rules and command syntax for importing LDAP server certificates.

Prerequisites for configuring a secure LDAP server connection

Configuring a secure connection to an LDAP or Kerberos server requires that you import a server certificate to the management server. Before importing a server certificate for secure communication, verify that the certificate adheres to the following rules:

The CN (CS in the Subject column) of the authentication server certificate must match the value set in the `exauth.properties` file:

For LDAP directory servers, the CN must match:

`auth.ldap.`*`auth.server.name-property-value`*`.host` in the `exauth.properties` file.

For Kerberos servers, the CN must match:

`auth.kerberos.`*`auth.kerberos.realm_name-property-values`*`.kdc` in the `exauth.properties` file.

Related tasks

- Configuring an LDAP server connection on page 139

Rules for importing LDAP directory server certificates

When importing an LDAP directory server certificate on the management server, adhere to the following rules:

- Do not import and use your own certificate into the truststore cacerts because that truststore is updated when you upgrade Hitachi Command Suite Common Component.
- Note the following when you use the `hcmds64keytool` command (in Windows) or the `keytool` command (in Linux) to specify a unique name in the truststore, the truststore file name, and the password:
  - Specify the file name as a character string of no more than 255 characters.
  - Do not use the following symbols in the file name: : , ; * ? " < > |.
  - Do not include double quotation marks (") in the unique name in the truststore or the password.

Related tasks

- Configuring SSL for a secure LDAP server connection on page 141

Related references

- Prerequisites for configuring a secure LDAP server connection on page 161
- Command format for importing LDAP server certificates on page 162

Command format for importing LDAP server certificates

When you use the `hcmds64keytool` command (in Windows) or the `keytool` command (in Linux) to import an LDAP directory server certificate to implement secure communication, use the following command format:

- In Windows:
  `HCS-Common-Component-installation-folder``\bin\hcmds64keytool -import -alias `*`unique-name-in-the-truststore`*` -file `*`certificate_file`*` -keystore `*`truststore-filename`*` -storepass `*`password-for-accessing-truststore`*
- In Linux:
  `HCS-Common-Component-installation-directory``/uCPSB/jdk/bin/keytool -import -alias `*`unique-name-in-the-truststore`*` -file`

certificate_file -keystore *truststore-filename* -storepass *password-for-accessing-truststore*

Unique-name-in-the-truststore specifies the name used to identify the certificate in the truststore.

For *truststore-file-name*, specify the name of the truststore file to create and register in the specified destination. Specify one of the following:

- In Windows:
  HCS-Common-Component-installation-folder\conf\sec\ldapcerts
  HCS-Common-Component-installation-folder\uCPSB\jdk\jre\lib\security\jssecacerts
- In Linux:
  HCS-Common-Component-installation-directory/conf/sec/ldapcacerts
  HCS-Common-Component-installation-directory/uCPSB/jdk/jre/lib/security/jssecacerts

Hitachi Data Systems recommends that you import the LDAP directory server certificate to `ldapcacerts`. If the certificate is shared by other programs, you can import the certificate to `jssecacerts`.

Related tasks

- Configuring SSL for a secure LDAP server connection on page 141

Related references

- Prerequisites for configuring a secure LDAP server connection on page 161
- Rules for importing LDAP directory server certificates on page 162

7

Installing and configuring Deployment Manager

Deployment Manager enables you to back up and restore disk data of managed resources, as well as deploy a master image to create new resources.

About Deployment Manager environment settings

Deployment Manager enables you to restore disk data of managed resources to a previous state in the event that a failure occurs, and create multiple copies of managed resources in the same environment. Deployment Manager requires that you configure settings on the management server as well as on managed resources.

Note: Deployment Manager is supported on Windows only.

To configure the environment settings for Deployment Manager:

- Install the Deployment Manager prerequisites (IIS, and .NET Framework).
- Install Deployment Manager from the Hitachi Compute Systems Manager installation wizard.
- Change the port used by Deployment Manager (if necessary).
- Change the boot settings for the managed resources.

If Deployment Manager is already installed, you can use the Compute Systems Manager installation wizard to upgrade, overwrite, or remove Deployment Manager.

Related tasks

- Installing Deployment Manager on page 169
- Configuring managed resources for use with Deployment Manager on page 170
- Changing the Deployment Manager port number on page 171
- Verifying the system prerequisites on page 38

Related references

- Prerequisites for installing Deployment Manager on page 166

Prerequisites for installing Deployment Manager

Before installing Deployment Manager, ensure that the management server meets the following requirements:

- Prerequisite software (IIS 7.5 or later and .NET Framework 3.5 SP1 (3.5.1) and 4.*x*) is installed.
- Deployment Manager port is not being used by another product.
  Certain ports cannot be used for Deployment Manager. If the port is already in use and you do not change it, Deployment Manager and the other products might not run properly.
- SQL Server instances with different languages do not coexist.

When you install Deployment Manager, SQL Server is automatically installed. If another SQL Server instance with a different language setting is already installed, the Deployment Manager installation fails.

Caution: If you remove an SQL Server instance being used by a product other than Deployment Manager, do not delete the DPMDBI instance.

Related tasks

- Installing Internet Information Server on page 167
- Installing .NET Framework for Deployment Manager on page 168

Installing Internet Information Server

You must install Internet Information Server (IIS) before installing Deployment Manager. Before installing IIS, ensure that the management server meets the required IIS prerequisites.

Note: If the management server is already running IIS, you do not need to install it again.

Procedure

1. Install IIS by using the standard steps provided with the operating system documentation and then depending on the IIS version, specify and install the following role services:

   For IIS 7.*x*, set the following:
   - Static Content
   - ASP.NET
   - Metabase Compatibility
   - IIS Management Console

   For IIS 8.0 or later, set the following:
   - Static Content
   - ASP.NET 4.5
   - Metabase Compatibility
   - IIS Management Console
2. For IIS 7.*x*, set the IIS default website:
   a. If the default website has been deleted, re-create it.
   b. Set the default website so that it is accessible through the loopback address (127.0.0.1) using the HTTP protocol. The port number of the default website is used during communication with Deployment Manager.

Related concepts

- About Deployment Manager environment settings on page 166

Related references

- Prerequisites for installing Deployment Manager on page 166

Installing .NET Framework for Deployment Manager

You must install .NET Framework before installing Deployment Manager. Deployment Manager requires both .NET Framework 3.5.1 (including 3.5 SP1) and .NET Framework 4.*x*.

Before installing .NET Framework, verify that the prerequisite version of IIS is installed on the server.

Note: If the management server is already running .NET Framework 3.5.1 or .NET Framework 4.*x*, you do not need to install it again.

Procedure

1. Determine which versions of .NET Framework are running on the server.
   - If both versions are running, you do not need to reinstall and you are done with this procedure.
   - If there are no versions of .NET Framework running or only .NET Framework 4.*x* is running, go to the next step.
   - If the server is running .NET Framework 3.5.1, but not .NET Framework 4.*x*, go to step 3.
2. To install .NET Framework 3.5.1 use the procedure for the operating system running on the management server.
   - To install .NET Framework 3.5.1 on Windows Server 2008 R2, open the Windows **Server Manager > Features > Add Features**, and then follow the instructions in the wizard to install **.NET Framework 3.5.1 Features**.
   - To install .NET Framework 3.5.1 on Windows Server 2012, open the Windows **Server Manager > Manage > Add Roles and Features**, and then follow the instructions in the wizard to select a server on which to install .NET Framework, and then install **.NET Framework 3.5 Features**.
3. To install .NET Framework 4.*x*, use the procedure for the operating system running on the management server.
   - When using Windows Serer 2008 R2, run the following command to install the software:
     DVD-drive:\HCSM_SERVER\HCSM\DPMMEDIA\dotNet Framework40\dotNetFx40_Full_x86_x64.exe
   - When using Windows Server 2012, open the Windows **Server Manager**, select **Manage > Add Roles and Features**, and then

follow the instructions in the wizard to select a server and install **.NET Framework 4.5 Features**.

Installing Deployment Manager

Before installing Deployment Manager, verify the following management server prerequisites:

- IIS 7.5 or later is installed.
- .NET Framework 3.5 SP1 (3.5.1) is installed.
- .NET Framework 4.*x* is installed.

Procedure

1. Run the Hitachi Compute Systems Manager installation program to install Deployment Manager.
   The Deployment Manager installation is included within the main Hitachi Compute Systems Manager installation.

   Note: If Deployment Manager is already installed, the removal option is available.

2. Follow the online prompts to install Deployment Manager. Record the user name you use to install the software because you must use the same user to complete and overwrite installation, an upgrade, or a removal.
3. If you are prompted to restart the operating system during the Deployment Manager installation, restart the machine and then run the Hitachi Compute Systems Manager installation wizard again.

   Note: If you install Deployment Manager after installing Hitachi Compute Systems Manager, the installation program runs an overwrite installation of Hitachi Compute Systems Manager.

   When you finish the Deployment Manager installation, you are returned to the main Hitachi Compute Systems Manager installation program.

   Note: You can change the port number the system uses for internal communication between Deployment Manager and IIS after installation by accessing the **Administration** tab.

Related tasks

- Changing the Deployment Manager port number on page 171

Related references

- Prerequisites for installing Deployment Manager on page 166

Prerequisites for using Deployment Manager

Before you can use Deployment Manager after installation, you must verify that the management server environment meets the following requirements:

- Managed resources meet the system requirements.
- The hardware models of the master and destination resources are the same.
  For details about hardware conditions, see the documentation for your hardware model.
- If you want to deploy the environment of the managed resource, you must disable LAN redundancy.
  However, if a duplex LAN is configured by using the `bonding` or `hbonding` driver, you do not need to disable LAN redundancy.
- DHCP server configuration status meets the following conditions:
  - When the DHCP server is configured on the management server, only one DHCP server is configured on the network.
  - When the DHCP server is not configured on the management server, all DHCP servers are set up in the same network.
    You can set up multiple DHCP servers.

Related tasks

- Installing Deployment Manager on page 169

Configuring managed resources for use with Deployment Manager

Before you can use a managed resource with Deployment Manager, you must change the boot settings for the managed resource.

To set up a PXE boot (network boot) on a managed resource that you want to use with Deployment Manager, you must change the BIOS start sequence for the managed resource as follows:

- Place the network boot entry above (before) the hard disk drive (HDD) entry.
- If there are multiple LAN boards, place the LAN board managed by Deployment Manager above (before) the HDD, and then disable the PXE boot settings for all other LAN boards. If you cannot disable these settings, place the LAN board below (after) the HDD.

Related concepts

- About Deployment Manager environment settings on page 166

Changing the Deployment Manager port number

If the default Deployment Manager port is assigned to another product on the management server, you must change the Deployment Manager port.

Note: Certain ports cannot be used for Deployment Manager.

The procedure for changing the port number depends on which port number you want to change.

- To change the port number used for internal communication with IIS (default 80/tcp):
  1. In the IIS settings, change the port number for the default website.
  2. Log in to Compute Systems Manager, access the Administration tab, and select Deployment > Settings.
  3. Change the port number to the same value as you set in the first step.
- To change all other port numbers:
  1. Stop Compute Systems Manager.
  2. In the properties file, change the Deployment Manager port number.
  3. Start Compute Systems Manager.

Related concepts

- About Deployment Manager environment settings on page 166

Related references

- Editing Deployment Manager properties and settings files when changing ports on page 171

Editing Deployment Manager properties and settings files when changing ports

If you change the Deployment Manager port number, you must edit the `port.ini` properties file and the `MgrServerList.xml` file.

The `port.ini` file is located in the following folder:

HCSM-installation-folder`\ComputeSystemsManager\DeploymentManager\PXE\Images`

The Deployment Manager `port.ini` file includes the port and function-related parameters listed in the following table:

Property	Description
BackupRestoreUnicast	This port is used for managed resource disk backup and restoration. The default value is 26501. If an attempt to change this port number fails, the system uses the default value 56020/tcp.
BOOTNIC	This port is used for managed resource PXE booting. The default value is 26502. If an attempt to change this port number fails, the system uses the default value 56022/tcp.
FSC	This port is used for managed resource PXE booting. The default value is 26503. If an attempt to change this port number fails, the system uses the default value 56030/tcp.
FTUnicast	This port is used for operating managed resource disks. The default value is 26508. If an attempt to change this port number fails, the system uses the default value 56023/tcp.

The `MgrServerList.xml` file is located in the following folder:

HCSM-installation-folder`\ComputeSystemsManager\DeploymentManager\WebServer\App_Data\Config\`

The Deployment Manager `MgrServerList.xml` file includes the port listed in the following table:

Port number	Location to edit
26500/tcp	<Port>*port-number-to-change*</Port> For example: <Port>26500</Port>

Related tasks

- Changing the Deployment Manager port number on page 171

Related references

- Properties related to Deployment Manager ports (port.ini) on page 321

8

Administering the management server

This module describes tasks related to administering the Hitachi Compute Systems Manager (HCSM) management server.

- Starting and Stopping Hitachi Compute Systems Manager
- Managing the database

Starting and Stopping Hitachi Compute Systems Manager

This module provides information about starting and stopping Hitachi Compute Systems Manager, which is required for many administrative tasks.

About starting and stopping Hitachi Compute Systems Manager

When you start a machine where you installed Hitachi Compute Systems Manager, Compute Systems Manager starts automatically. At the same time, other Hitachi Command Suite products are also started.

To change the Compute Systems Manager settings, you must manually stop and start Compute Systems Manager. You can choose whether to stop and start Hitachi Command Suite only, or stop and start Compute Systems Manager in addition to all other Hitachi Command Suite products.

Related tasks

- Starting Hitachi Compute Systems Manager on page 174
- Stopping Hitachi Compute Systems Manager on page 175
- Checking the status of Hitachi Compute Systems Manager services on page 178

Related references

- Hitachi Compute Systems Manager services and processes on page 176

Starting Hitachi Compute Systems Manager

You can start Hitachi Compute Systems Manager from the Windows desktop or from the command line.

To start Compute Systems Manager from the Windows desktop:

- For Windows Server 2008 R2, select Start > All Programs > Hitachi Command Suite > Compute Systems Manager > Start - HCSM.
- For Windows Server 2012, select Start > All Apps > Hitachi Command Suite > Start - HCSM.
- To start Compute Systems Manager from the command line, use the following command:
  HCS-Common-Component-installation-folder\bin\hcmds64srv /start

To start Compute Systems Manager from the Linux command line, enter the following command:

HCS-Common-Component-installation-directory/bin/hcmds64srv -start

The Compute Systems Manager services start. Other Hitachi Command Suite products installed on the same machine, including Hitachi Command Suite common component, also start.

Related concepts

- About starting and stopping Hitachi Compute Systems Manager on page 174

Related tasks

- Stopping Hitachi Compute Systems Manager on page 175
- Checking the status of Hitachi Compute Systems Manager services on page 178

Related references

- Hitachi Compute Systems Manager services and processes on page 176

Stopping Hitachi Compute Systems Manager

You can stop Hitachi Compute Systems Manager from the Windows desktop or from the command line.

Note: You must stop all Hitachi Command Suite services before making configuration changes. Therefore, do not stop only the Compute Systems Manager service unless there is a specific reason to do so (for example, when troubleshooting an issue).

In Windows:

To stop Compute Systems Manager from the Windows desktop:

- For Windows Server 2008 R2, select Start > All Programs > Hitachi Command Suite > Compute Systems Manager > Stop - HCSM.
- For Windows Server 2012, select Start > All Apps > Hitachi Command Suite > Stop - HCSM.
- To stop Compute Systems Manager from the command line, use the following command:
  HCS-Common-Component-installation-folder\bin\hcmds64srv /stop /server ComputeSystemsManagerWebService

In Linux:

To stop Compute Systems Manager from the command line, use the following command:

HCS-Common-Component-installation-directory/bin/hcmds64srv -stop

To stop only Compute Systems Manager but not other Hitachi Command Suite products, use the following command:

HCS-Common-Component-installation-directory/bin/hcmds64srv -stop -server ComputeSystemsManagerWebService

Only the Compute Systems Manager service stops.

Related concepts

- About starting and stopping Hitachi Compute Systems Manager on page 174

Related tasks

- Starting Hitachi Compute Systems Manager on page 174
- Checking the status of Hitachi Compute Systems Manager services on page 178

Related references

- Hitachi Compute Systems Manager services and processes on page 176

Hitachi Compute Systems Manager services and processes

When viewing Hitachi Compute Systems Manager status or messages, the system displays information for the Windows Compute Systems Manager services and processes listed in the following table:

Process name	Service Name	Description
`cjstartweb.exe` `hcmdssvctl.exe`	HCS Compute Systems Manager Web Service	Hitachi Compute Systems Manager servlet service. When other products in the Hitachi Command Suite are installed on the same machine, processes for those products might start with the name `cjstartweb.exe` or `hcmdssvctl.exe`
`cjstartweb.exe` `hcmdssvctl.exe`	HBase 64 Storage Mgmt SSO Service	Hitachi Command Suite servlet service for single sign-on. When other products in the Hitachi Command Suite are installed on the same machine, processes for those products might start with the name `cjstartweb.exe` or `hcmdssvctl.exe`
`httpsd.exe` `rotatelogs.exe`	HBase 64 Storage Mgmt Web Service	Hitachi Command Suite common web service. Multiple instances of this process might be running.
`httpsd.exe` `rotatelogs.exe`	HBase 64 Storage Mgmt Web SSO Service	Hitachi Command Suite common web service for single sign-on. Multiple instances of this process might be running.
`hntr2mon.exe`	Hitachi Network Objectplaza Trace Monitor 2 Hitachi Network Objectplaza Trace Monitor 2 (x64)	Hitachi Command Suite common trace information collection. (Integrated trace information is collected.)
`hntr2srv.exe`		Hitachi Command Suite common trace service.

Process name	Service Name	Description
		(This service processes events from the Services window.)
pdservice.exe	HiRDB/EmbeddedEdition _HD1	Database management-related processes.
pdprcd.exe		

When viewing Compute Systems Manager Deployment Manager status or messages, the system displays information for the services and processes listed in the following table:

Process name	Service Name	Description
apiserv.exe	DeploymentManager APIService	Deployment Manager Common Component service
bkressvc.exe	DeploymentManager Backup/ Restore Management	Backup/restore task execution service
depssvc.exe	DeploymentManager Get Client Information	Deployment Manager service for collecting information from the target server
pxesvc.exe	DeploymentManager PXE Management	Network (PXE) boot control service
pxemtftp.exe	DeploymentManager PXE Mtftp	TFTP server functionality
rupdssvc.exe	DeploymentManager Remote Update Service	Deployment Manager service for executing remote updates for the target server
schwatch.exe	DeploymentManager Schedule Management	Schedule management service
ftsvc.exe	DeploymentManager Transfer Management	File transfer service
sqlservr.exe	SQL Server (DPMDBI)	Database service
sqlagent.exe	SQL Server Agent (DPMDBI) **Note:** This service is registered during the Deployment Manager installation, but it does not run as a resident process.	Database job management service

When viewing Compute Systems Manager status or messages, the system displays information for the Linux Compute Systems Manager processes listed in the following table:

Process name	Description
cjstartweb	Hitachi Compute Systems Manager servlet service.
hcs_csm	
cjstartweb	Hitachi Command Suite servlet services for single sign-on.

Process name	Description
hcs_hsso	
httpsd	Hitachi Command Suite common web service. Multiple instances of this process might be running.
httpsd	Hitachi Command Suite common web service for single sign-on. Multiple instances of this process might be running.
rotatelogs	Log partitioning utility for web services. Multiple instances of this process might be running.
hntr2mon	Hitachi Command Suite common trace information collection. (Integrated trace information is collected.)
pdprcd	Database process server process.

Related concepts

- About starting and stopping Hitachi Compute Systems Manager on page 174

Related tasks

- Checking the status of Hitachi Compute Systems Manager services on page 178

Checking the status of Hitachi Compute Systems Manager services

You can check Hitachi Compute Systems Manager status from the desktop or from the command line.

In Windows:

To check Compute Systems Manager status from the Windows desktop:

- For Windows Server 2008 R2, select Start > All Programs > Hitachi Command Suite > Compute Systems Manager > Status - HCSM.
- For Windows Server 2012, select Start > All Apps > Hitachi Command Suite > Status - HCSM.
- To check Compute Systems Manager from the command line, use the following command:
  HCS-Common-Component-installation-folder\bin\hcmds64srv /statusall

In Linux:

To check Compute Systems Manager from the command line, use the following command:

HCS-Common-Component-installation-directory/bin/hcmds64srv -statusall

The system displays the operation status information for each of the Compute Systems Manager services.

Related concepts

- About starting and stopping Hitachi Compute Systems Manager on page 174

Related references

- Hitachi Compute Systems Manager services and processes on page 176

Managing the database

This module provides information about managing the Hitachi Compute Systems Manager database.

About database management

Managing the Hitachi Compute Systems Manager database includes maintaining a backup copy of the database. If a database-related failure occurs on the Compute Systems Manager management server, the system uses the backup to restore the database.

- To back up and restore the Compute Systems Manager database, use either of the following methods:
  - Use the `hcmds64backups` command to back up the database and then use the `hcmds64db` command to restore the database (recommended).
  - Use the `hcmds64dbtrans` command to export the database, and then use the `hcmds64dbtrans` command to import the database.
    Use this method if the environment where you want to restore the database does not satisfy the conditions for using the `hcmds64db` command for restoration.

Tip: To protect against failure, make sure that you regularly back up the database using the `hcmds64backups` command and also export the database using the `hcmds64dbtrans` command.

- Database migration—migrate Compute Systems Manager to another server by exporting the current database and importing it to a new server. When you use Compute Systems Manager over a long time period, Compute Systems Manager software upgrades and increases in managed resources might require you to implement servers with higher performance. In this case, you can migrate Compute Systems Manager to another server. You migrate a database by using the `hcmds64dbtrans` command on the source server to export the database and then using the same command to import the database to the target server. You can migrate a database to a computer in a different environment, such as the following:

- Migrate to servers on a different platform (such as migrating to a different version of Windows Server or from a Windows server to a Linux server).
- Migrate to servers with a different Compute Systems Manager installation directory.
- Migrate to servers with a more recent Compute Systems Manager version.

  If you are running more than one Hitachi Command Suite product on the same management server as Compute Systems Manager, you can back up, restore, and migrate all databases at the same time.

Note: To use backup software to back up a disk area that includes the Compute Systems Manager installation directory or the database directory, stop all services of Hitachi Command Suite products in advance.

If you back up the disk area without stopping services, a failure might occur because of delayed I/O operations, file exclusion, or other causes.

Related tasks

- Backing up the database on page 181
- Restoring the database on page 182
- Exporting the database on page 184
- Importing the database on page 185
- Stopping Hitachi Compute Systems Manager on page 175

Related references

- Prerequisites for database backup on page 180
- Prerequisites for restoring the database on page 182
- Prerequisites for database migration on page 183
- Troubleshooting example: database corruption on page 255

Prerequisites for database backup

Before you back up the Hitachi Compute Systems Manager database, you must create a directory for storing the backup files. When you create the directory, ensure that you follow the Compute Systems Manager path naming conventions. Also ensure that the directory size is equal to or greater than the required space specified by the following formula:

Database directory required space: `(`*`total-size-of-all-Hitachi-Command-Suite-product-databases-to-back-up`* `+4.6GB) x 2`

where the size of the Compute Systems Manager and Hitachi Command Suite Common Component databases is determined by the size of the directory containing the database files. For details on the database sizes of other Hitachi Command Suite products, see the documentation for those products.

Related concepts

- About database management on page 179

Related tasks

- Backing up the database on page 181

Backing up the database

You must maintain a backup copy of the database so that the Hitachi Compute Systems Manager management server can restore the database if there is a failure.

Procedure

1. Verify the path name of the database backup directory that you created, and then verify that the directory is empty (does not contain any subdirectories or files).
2. Back up the database by using the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64backups /dir *local-disk-folder-for-data-storage-backup* /auto
   - In Linux:
     HCS-Common-Component-installation-directory/bin/hcmds64backups -dir *local-disk-directory-for-data-storage-backup* -auto

   When specifying the command options, use the following descriptions:
   - `dir`
     Specify the absolute path on the local disk where the database backup files are stored. Do not specify a subdirectory or a specific file. Make sure the directory specified for `dir` is empty.
   - `auto`
     Use this option to automatically change the status of Hitachi Command Suite products and the database services to the status required for backing up the database. After the command finishes, the Hitachi Command Suite products and the database services are changed to `start` status.

   The system creates the database backup files and saves the database backup to the storage directory in a file named `backup.hdb`.

Result

You now have a backup copy of the latest Compute Systems Manager database.

Postrequisites

Note: The system backs up the Hitachi Command Suite setting files in a different location than the database backup directory. If an error occurs in the management server and you must reinstall the Hitachi Command Suite products, use the backup setting files to obtain the previous settings.

Related concepts

- About database management on page 179

Related tasks

- Restoring the database on page 182

Related references

- Prerequisites for database backup on page 180

Prerequisites for restoring the database

Before you restore the Hitachi Compute Systems Manager database, ensure that the following settings are the same on the management server from which you created the database backup and the management server where you plan to restore the database:

- Hitachi Command Suite products versions and revisions, including the installed Compute Systems Manager
- Installation locations for Hitachi Command Suite products including Compute Systems Manager, Common Component and the associated databases
- IP address and host name of the host

Caution: The `hcmds64db` command, that you use to restore the database, creates temporary files while restoring the database. Ensure that you have write permission for the database directory and that the directory has enough free space.

Related concepts

- About database management on page 179

Related tasks

- Backing up the database on page 181
- Restoring the database on page 182

Restoring the database

If you encounter a failure situation, you can restore the existing database using the database backup. Use the following procedure if you backed up your database using the `hcmds64backups` command.

Procedure

1. Restore the database by using the following command:
   - In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64db /restore *backup-file*(backup.hdb) /type ALL /auto
   - In Linux:
     HCS-Common-Component-installation-directory/bin/hcmds64db -restore *backup-file*(backup.hdb) -type ALL -auto

   When specifying the command options, use the following descriptions:
   - `restore`
     Specify the absolute path to the database backup file (`backup.hdb`) created by the `hcmds64backups` command.
   - `auto`
     Use this option to automatically change the status of Hitachi Command Suite products and the database services to the status required for restoring the database. After the command finishes, the Hitachi Command Suite products and the database services are changed to stop status.
2. Start Compute Systems Manager.

Result

The Compute Systems Manager database is now restored.

If other Hitachi Command Suite products run on the same host, those products are also restored. If the command restores other Hitachi Command Suite products, you might need to complete additional tasks for those products. For details, see the Hitachi Command Suite product documentation.

Related concepts

- About database management on page 179

Related tasks

- Backing up the database on page 181

Related references

- Prerequisites for restoring the database on page 182

Prerequisites for database migration

To migrate the Hitachi Compute Systems Manager database to another server, export the existing database from the source Compute Systems Manager server and import it to the target Compute Systems Manager server.

Before you start the migration process, complete the following prerequisite tasks:

- Verify that the Compute Systems Manager software version running on the target server is the same or later than the version running on the source server.
- Create a directory for temporarily storing the database data and a directory for storing archive files. For each directory, verify that the available space is equal to the total size of the following directories:
  - Database storage directory for each Hitachi Command Suite product
  - Database storage directory for the Hitachi Command Suite Common Component database (excluding the SYS directory and SYS subdirectories)

Note: Compute Systems Manager exports databases as archive files. If the capacity of the archive storage directory is insufficient, the archive file creation fails. In this case, ensure that there is enough capacity in the archive directory, and then try exporting again.

Related concepts

- About database management on page 179

Related tasks

- Exporting the database on page 184
- Importing the database on page 185

Exporting the database

To migrate the Hitachi Compute Systems Manager database to another server, you export the existing database. You can also use the exported database to restore a database after a failure.

Procedure

1. Verify that the working directory that you plan to use for exports is empty (does not contain any subdirectories or files).
2. To export the databases, run the following command:
   - In Windows:
     `HCS-Common-Component-installation-folder\bin\hcmds64dbtrans /export /workpath working-folder /file archive-file /auto`
   - In Linux:
     `HCS-Common-Component-installation-directory/bin/hcmds64dbtrans -export -workpath working-directory -file archive-file -auto`

   When specifying the command options, use the following descriptions:

   - `workpath`

Specify an absolute path on the local disk where you want to temporarily store the database data. Ensure that the directory you specify is empty and does not contain any subdirectories or files.

- `file`

  Specify the absolute path of the archive file that you want the export command to generate.

- `auto`

  Use this option to automatically change the status of Hitachi Command Suite products and the database services to the status required for exporting the database. After the command finishes, the Hitachi Command Suite products and the database services are changed to start status.

3. For migrations, transfer the exported files to the migration target server.

Result

The database is exported. For migration, the exported database is ready for you to import to the target Compute Systems Manager server.

Related concepts

- About database management on page 179

Related tasks

- Importing the database on page 185

Related references

- Prerequisites for database migration on page 183

Importing the database

After you export the Hitachi Compute Systems Manager database from an existing server, you can import it to another Compute Systems Manager server. You can also use an exported database to restore an existing database after a failure.

Procedure

1. If you specified a value other than the default for a property on the migration source management server, check and review the property value set on the migration destination server. These values must match for the property file migration to succeed. The property files are not migrated during a database migration.
2. To import the database without an archive file (database files transferred manually), go to step 3. To import the database using an archive file, use the following command.
   - In Windows:

HCS-Common-Component-installation-folder\bin
\hcmds64dbtrans /import /workpath *working-folder* /file
archive-file /type {ALL|*product-name*} /auto

- In Linux:
  HCS-Common-Component-installation-directory/bin/
  hcmds64dbtrans -import -workpath *working-directory* -file
  archive-file -type {ALL|*product-name*} -auto

When specifying the command options, use the following descriptions:

- workpath
  Specify an absolute path on the local disk where you want to temporarily store the database information. Ensure that the directory you specify is empty and does not contain any subdirectories or files.
- file
  Specify the absolute path of the database archive file that you transferred from the original server.
- type
  To import all Hitachi Command Suite product databases, specify the type as ALL. To import the Compute Systems Manager database only, specify HCSM. To import other Hitachi Command Suite product databases individually, see the documentation for the applicable Hitachi Command Suite product.
- auto
  Use this option to automatically change the status of Hitachi Command Suite products and the database services to the status required for importing the database. After the command finishes, the Hitachi Command Suite products and the database services are changed to stop status.

3. To import the database without an archive file (database files transferred manually), use one of the following commands:

- In Windows:
  HCS-Common-Component-installation-folder\bin
  \hcmds64dbtrans /import /workpath *working-folder* /type
  {ALL|*product-name*} /auto
- In Linux:
  HCS-Common-Component-installation-directory/bin/
  hcmds64dbtrans -import -workpath *working-directory* -type
  {ALL|*product-name*} -auto

When specifying the command options, use the following descriptions:

- workpath
  Specify an absolute path on the local disk where you want to temporarily store the database information. Ensure that the directory you specify is empty and does not contain any subdirectories or files.
- type

To import all Hitachi Command Suite product databases, specify the type as ALL. To import the Compute Systems Manager database only, specify HCSM. To import other Hitachi Command Suite product databases individually, see the documentation for the applicable Hitachi Command Suite product.

- `auto`

  Use this option to automatically change the status of Hitachi Command Suite products and the database services to the status required for importing the database. After the command finishes, the Hitachi Command Suite products and the database services are changed to stop status.

4. Start Compute Systems Manager on the new server.
5. Back up the database.

   Make sure that you back up the database immediately after the import so that it is available in case of a failure.

Result

The Compute Systems Manager database is now running on the new server.

Related concepts

- About database management on page 179

Related tasks

- Exporting the database on page 184

Related references

- Prerequisites for database migration on page 183

9

Implementing Hitachi Compute Systems Manager in a cluster environment

This module describes tasks related to configuring and using Hitachi Compute Systems Manager (HCSM) in a cluster environment.

About implementing Hitachi Compute Systems Manager in a cluster environment

When using Hitachi Compute Systems Manager, you can increase reliability by setting up a failover management server using clustering services.

When you use Compute Systems Manager in a cluster environment, you designate one Compute Systems Manager server as the active node and another as the standby node as follows:

- Active node
  The active node is the host that is running services in a system that uses a cluster.
  If a failure occurs, cluster services implements a failover and the standby node takes over operation of the system resources so that there is no interruption.
- Standby node
  The standby node is the host that waits "on standby" to take over operation of system resources from the active node if a failure occurs.

Note: If an active node encounters a failure and fails over to the standby node, any tasks that are running fail. This means that you must run the tasks again on the standby node.

The cluster management software instructions in this manual apply to the following:

- Windows: Windows Server Failover Clustering
- Linux: Red Hat High Availability
  This manual includes procedures for implementing Compute Systems Manager by using Conga, which is provided with Red Hat High Availability. To use Conga, you must install the luci package.
  The examples used in the manual assume that the following luci package version is installed:
  Version: 0.26.0
  Release: 48.el6
  For details about the luci package, see the Red Hat High Availability documentation.

Related concepts

- Hitachi Compute Systems Manager services used in a cluster environment on page 191

Related tasks

- Installing or Upgrading Hitachi Compute Systems Manager in a Windows cluster on page 201

- Installing a new Hitachi Compute Systems Manager instance on a Linux active node on page 205
- Installing a new Hitachi Compute Systems Manager instance on a Linux standby node on page 209
- Upgrading or overwriting Hitachi Compute Systems Manager on a Linux active node on page 212
- Upgrading or overwriting Hitachi Compute Systems Manager on a Linux standby node on page 214
- Migrating Hitachi Compute Systems Manager to a cluster environment (Windows) on page 216
- Migrating Hitachi Compute Systems Manager to a cluster environment (Linux) on page 220
- Removing the software in a cluster environment (Windows) on page 249
- Removing the software in a cluster environment (Linux) on page 251
- Upgrading the software from v7.x in a cluster environment on page 327

Related references

- Determining which method to use when implementing in a cluster environment on page 192
- Verifying management server free disk space in a cluster environment on page 198
- Checking the cluster configuration using the cluster management software on page 199

Hitachi Compute Systems Manager services used in a cluster environment

The following list identifies the Hitachi Compute Systems Manager services and Hitachi Command Suite Common Component services that are used within a cluster environment:

- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt Web SSO Service
- HCS Compute Systems Manager Web Service
- HiRDB/ClusterService _HD1 (Windows)
- HiRDB (Linux)

When using Deployment Manager on a Windows management server, you use the following additional services:

- DeploymentManager PXE Management
- DeploymentManager PXE Mtftp
- DeploymentManager Transfer Management

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Registering services to a cluster environment (Windows) on page 224
- Registering services to a cluster environment (Linux) on page 226
- Deleting services from the cluster management software (Windows) on page 227
- Deleting services from the cluster management software (Linux) on page 229
- Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Windows) on page 232
- Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Linux) on page 233
- Starting Hitachi Compute Systems Manager in a cluster environment (Windows) on page 234
- Starting Hitachi Compute Systems Manager in a cluster environment (Linux) on page 234

Related references

- Hitachi Compute Systems Manager services and processes on page 176

Prerequisites for implementing in a cluster environment

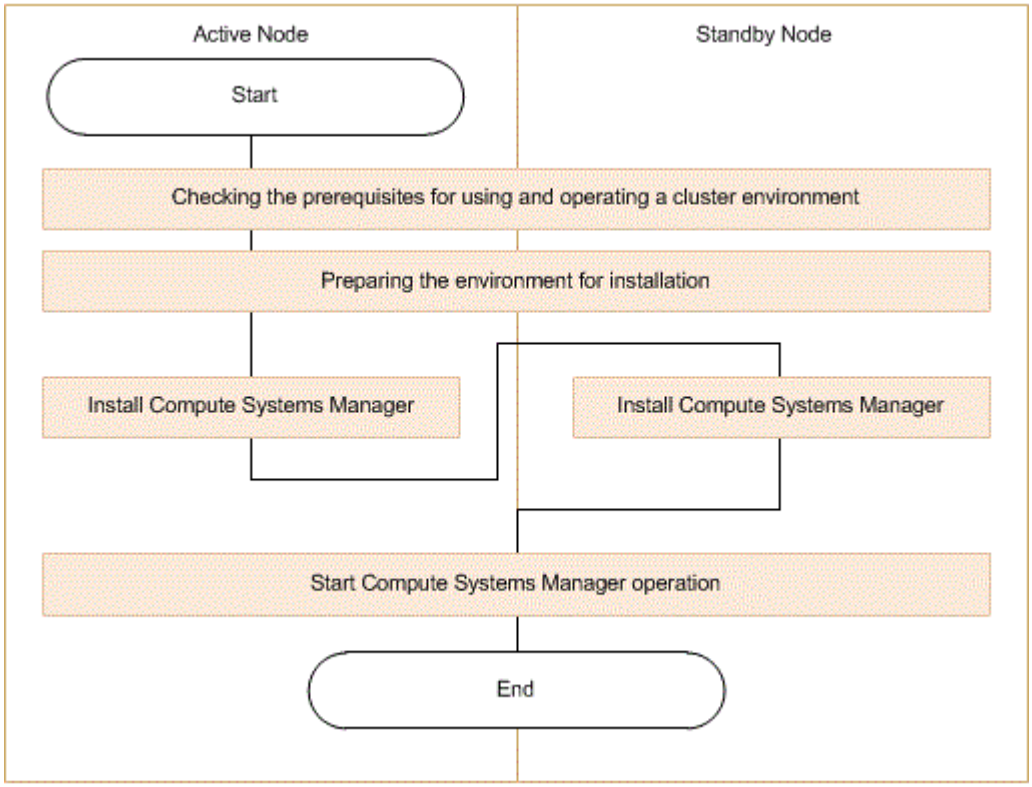
Before installing or configuring Hitachi Compute Systems Manager in a cluster environment, you must verify that your environment meets all prerequisites. This includes verifying your existing Compute Systems Manager installation status, verifying required free disk space, and verifying the installation of your other Hitachi Command Suite products.

Determining which method to use when implementing in a cluster environment

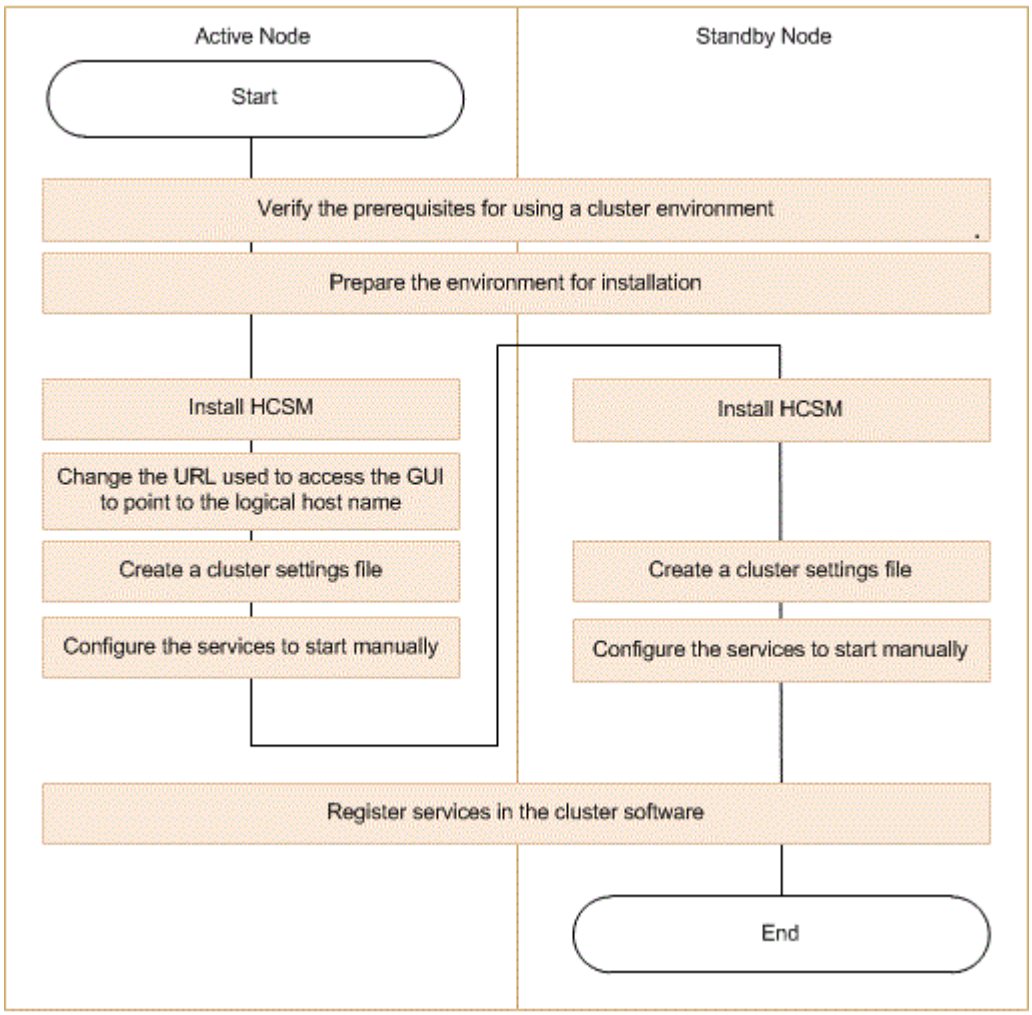
The setup process for installing and configuring Hitachi Compute Systems Manager in a cluster environment, differs depending on the management server status and your environment. Before you set up Compute Systems Manager, you must determine which installation method to use for your environment.

The following shows the workflow for setting a up cluster environment, depending on the state of the management server.

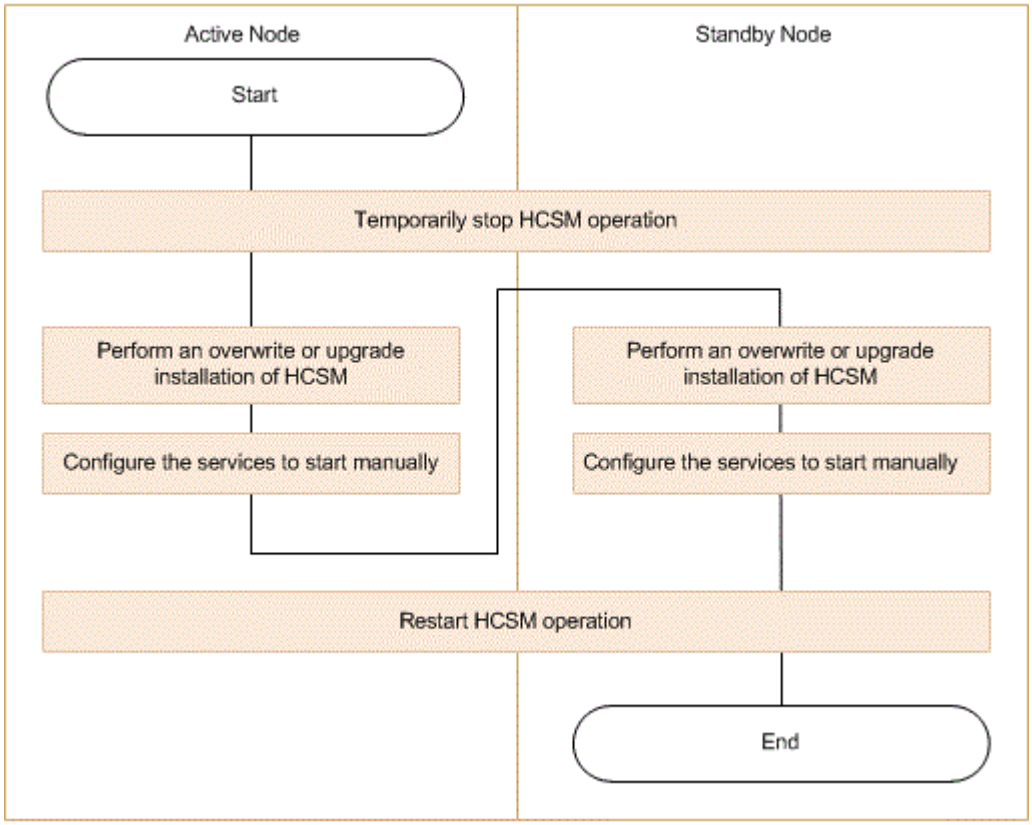
- If the management server is in a cluster environment (Windows):



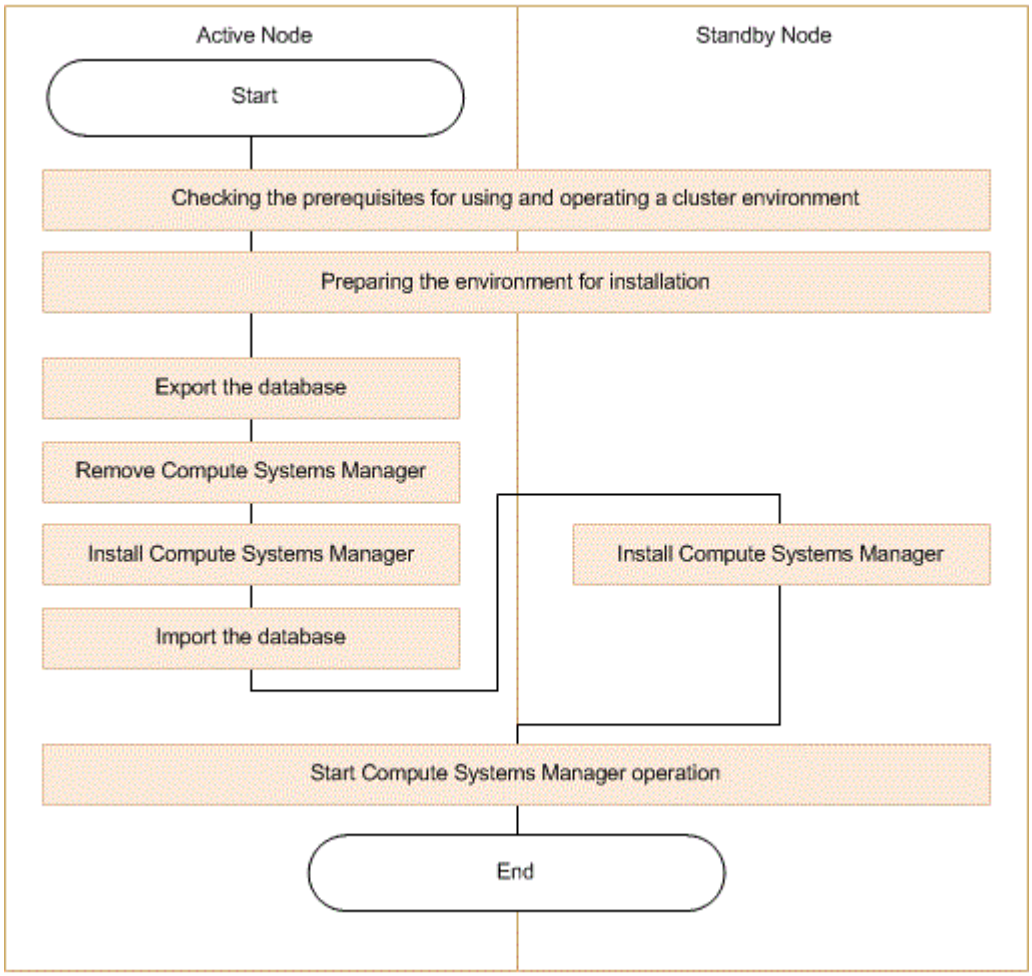
- If the management server is in a cluster environment and Compute Systems Manager has not been installed (Linux):



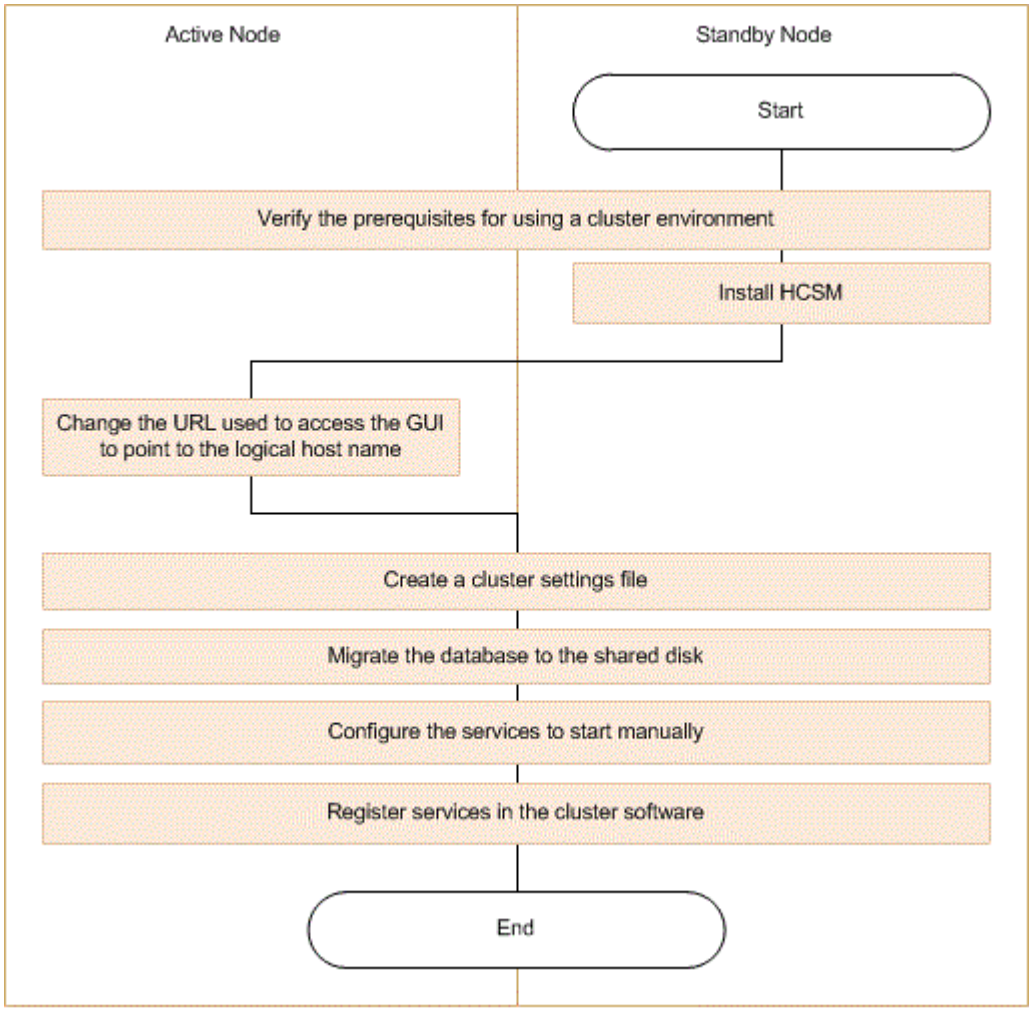
- If the management server is in a cluster environment and Compute Systems Manager is already installed (Linux):



- If the management server is not in a cluster environment (Windows):



- If the management server is not in a cluster environment (Linux):



Note:

- When installing Compute Systems Manager to a cluster environment for the first time or when migrating from a non-cluster environment to a cluster environment, make sure that every node in the cluster has the same disk configuration, and all Hitachi Command Suite products are installed in the same location (including drive letter, path, etc.) on each node.
- In Windows, the user must log in as a domain user with Administrator permission to perform an installation in a cluster environment.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Installing a new Hitachi Compute Systems Manager instance on a Linux active node on page 205
- Installing or Upgrading Hitachi Compute Systems Manager in a Windows cluster on page 201
- Installing a new Hitachi Compute Systems Manager instance on a Linux standby node on page 209
- Upgrading or overwriting Hitachi Compute Systems Manager on a Linux active node on page 212
- Upgrading or overwriting Hitachi Compute Systems Manager on a Linux standby node on page 214
- Starting Hitachi Compute Systems Manager in a cluster environment (Windows) on page 234
- Migrating Hitachi Compute Systems Manager to a cluster environment (Windows) on page 216
- Migrating Hitachi Compute Systems Manager to a cluster environment (Linux) on page 220
- Registering services to a cluster environment (Linux) on page 226

Related references

- Verifying management server free disk space in a cluster environment on page 198
- Checking the cluster configuration using the cluster management software on page 199

Verifying management server free disk space in a cluster environment

When setting up Hitachi Compute Systems Manager in a cluster environment, you must migrate or back up the database to a shared disk.

Before you set up Compute Systems Manager in a cluster environment, verify that the management server has the following free disk space available:

- Free space required for the database backup (For details about the required free space, see *Prerequisites for database backup*.)
- Free space required on the shared disk:
  - Free space required at the specified location for re-creating a migrated database:
    *Hitachi-Command-Suite-Common-Component-database-size** + *total-size-of-all-Hitachi-Command-Suite-products-installed-on-same-host-as-HCSM* (including Compute Systems Manager)*
  - If you are using Deployment Manager on a Windows management server, free space required to migrate image files
  - Free space required to store the work folder used by Compute Systems Manager

For details about the Compute Systems Manager work folder, see the description of the `hcsm.shared.directory` located in the following properties file:
In Windows:
HCSM-installation-folder`\ComputeSystemsManager\conf\user.properties`
In Linux:
HCSM-installation-directory`/ComputeSystemsManager/conf/user.properties`
*The size of the Compute Systems Manager and Hitachi Command Suite Common Component databases can be determined from the size of the directory containing the database files. For details on the database sizes of other Hitachi Command Suite products, see the documentation for those products.

Related tasks

- Installing or Upgrading Hitachi Compute Systems Manager in a Windows cluster on page 201
- Installing a new Hitachi Compute Systems Manager instance on a Linux active node on page 205
- Upgrading or overwriting Hitachi Compute Systems Manager on a Linux active node on page 212
- Migrating Hitachi Compute Systems Manager to a cluster environment (Windows) on page 216
- Migrating Hitachi Compute Systems Manager to a cluster environment (Linux) on page 220
- Upgrading the software from v7.x in a cluster environment on page 327

Related references

- Determining which method to use when implementing in a cluster environment on page 192
- Checking the cluster configuration using the cluster management software on page 199
- Prerequisites for database backup on page 180

Checking the cluster configuration using the cluster management software

When setting up Hitachi Compute Systems Manager in a cluster environment, you must use the cluster management software to verify the current environment settings and to configure additional settings.

Log in as a domain user with Administrative permissions and then use the cluster management software to check the following items before setting up Compute Systems Manager in a cluster environment:

- Check whether a group exists in which other Hitachi Command Suite product services are registered.
  If a group in which Hitachi Command Suite services are registered already exists, use that group. Verify that the group consists only of resources related to Hitachi Command Suite products.
  If no group in which Hitachi Command Suite services are registered exists, use the cluster management software to create a group in which you plan to register the Compute Systems Manager services.

  Note: Group names on a Windows management server cannot contain the following characters: ! " &) * ^ | < >

- Verify that the group in which you plan to register services includes the shared disk and client access point that can be inherited between the active and standby nodes. The client access point is the cluster management IP address and the logical host name.
- Verify that you can allocate, delete, and monitor resources by using the cluster management software without any issues.

Services that are used in a cluster environment can be failed over together by registering them as a group in the cluster management software. These groups might be referred to by different names, such as "resource groups" or "roles", depending on the versions of the cluster management software and the OS.

Related tasks

- Installing or Upgrading Hitachi Compute Systems Manager in a Windows cluster on page 201
- Installing a new Hitachi Compute Systems Manager instance on a Linux active node on page 205
- Upgrading or overwriting Hitachi Compute Systems Manager on a Linux active node on page 212
- Migrating Hitachi Compute Systems Manager to a cluster environment (Windows) on page 216
- Migrating Hitachi Compute Systems Manager to a cluster environment (Linux) on page 220
- Upgrading the software from v7.x in a cluster environment on page 327

Related references

- Determining which method to use when implementing in a cluster environment on page 192
- Verifying management server free disk space in a cluster environment on page 198

Installing Hitachi Compute Systems Manager in a cluster environment

This module provides information about installing and configuring Hitachi Compute Systems Manager in a cluster environment.

Installing or Upgrading Hitachi Compute Systems Manager in a Windows cluster

You can complete a new installation, an overwrite installation, or an upgrade of Hitachi Compute Systems Manager on the Windows management server in a cluster configuration.

Prerequisites

Note: This topic explains procedures for new installations, overwrite installations, and upgrades from v8.0 or later. You must follow a different procedure if you are upgrading from version 7.*x*. For details, see information about upgrading from version 7.*x*.

Before installing or upgrading, complete the following tasks:

- Complete the pre-installation checklist.
- Verify that the management server has the required free space for installing in a cluster environment.
- Use the cluster management software to check the cluster settings.
- If Windows Firewall is enabled, verify that the Firewall Service is running.
- Verify that the Windows Services and Event Viewer dialog boxes are closed.
- If you are installing a new instance of Deployment Manager, verify all Deployment Manager prerequisites.
- If you plan to install other products using the integrated media, verify that your system meets the prerequisites for all the products.
- If another Hitachi Command Suite product is installed, check the port number that is used by the database.
  During new installations, the database port number is set to the default (22032/tcp).
  If you changed the port number from the default, record the port number you are using.
- If you are upgrading Deployment Manager v8.1.4 or earlier, and the user who is running the upgrade differs from the user that completed the initial installation, you must remove Deployment Manager before the upgrade. Log in as the user who installed Deployment Manager and remove the software. Then, log in as the user running the upgrade and select Deployment Manager to complete the upgrade process.

- If other Hitachi Command Suite product services are already registered to the cluster management application group used by the installation wizard, note the following:
  When you run an installation on an active node, all registered services are removed and then re-registered by default when you complete the installation on the standby node. If you changed the service resource names, record the resource names in advance, and then manually change the names after the installation is finished.

Note: This step does not apply to Hitachi File Services Manager resources because they are not removed during the installation.

Procedure

1. Using the cluster management software, do the following:
   a. Move the owner of the group in which Hitachi Command Suite services are registered to the active node.
   b. Bring the cluster management IP address and shared disks online.
2. Install or upgrade Compute Systems Manager on the active node by running the installation wizard, selecting the cluster configuration option, and specifying the required information.
   If another Hitachi Command Suite product already exists in the cluster environment, you do not need to specify any settings because the installation program automatically uses the existing configuration settings.

Note: You cannot install Deployment Manager by using the All-in-One Installer.

3. After completing the installation or upgrade on the active node, use the cluster management software to move the owner of the group in which Hitachi Command Suite services are registered to the standby node.
4. Install or upgrade Compute Systems Manager on the standby node by running the installation wizard.
   During the installation or upgrade, ensure you follow these requirements:
   - Install Compute Systems Manager in the same location as on the active node.
   - If you installed Deployment Manager on the active node, install it on the standby node.

Note: When completing a new installation of multiple Hitachi Command Suite products on a standby node, install the products in the order that they were installed on the active node.

5. If you changed the database port number to a port number other than the default, specify the port number that you recorded earlier.

   Note: If a product that uses the 32-bit version of Hitachi Command Suite Common Component is installed (Hitachi File Services Manager or Hitachi Storage Navigator Modular 2), make sure that the port numbers you set do not conflict with the port number used by these products.

6. To manage a Hitachi server, change the settings as needed so that the management server IP address registered on the Hitachi server can be used as the cluster management IP address.

   Specify the cluster management IP address for the `svp.bind.address` property of the following file:

   HCSM-installation-folder`\ComputeSystemsManager\conf\user.properties`

   Tip:
   - If the `svp.bind.address` property is not specified, the IP address of the active and standby nodes is registered on the Hitachi server.
   - The management server IP address, with which the Hitachi server is communicating, is registered on the Hitachi server. If you specify the `svp.bind.address` property, the IP address specified for the property is also registered. You can check the management server IP addresses registered on the Hitachi servers by using the Web console. If you find management server IP addresses that are no longer in use, delete them.

7. To start Compute Systems Manager in the cluster, run the following command :

   HCS-Common-Component-installation-folder`\Clustersetup\hcmds64clustersrvstate /son /r` *group-name*

8. To register a plug-in license, enter the license key on the standby node.
9. Using the cluster management software, move the owner of the group in which you registered the Compute Systems Manager services to the active node.
10. If you registered a plug-in license on the standby node, enter the same license key on the active node.
11. If you installed Deployment Manager, set up the cluster environment so that you can enable and use Deployment Manager.

Related concepts

- About verifying system prerequisites on page 38

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191
- About verifying the installation environment on page 41

Related tasks

- Installing the software (Windows) on page 47
- Installing from the integrated media by using the all-in-one installer (Windows) on page 49
- Installing Deployment Manager on page 169
- Setting up Deployment Manager in a cluster environment on page 231
- Starting Hitachi Compute Systems Manager in a cluster environment (Windows) on page 234
- Upgrading the software from v7.x in a cluster environment on page 327
- Backing up the database in a cluster environment (Windows) on page 235
- Starting Hitachi Compute Systems Manager in a cluster environment (Windows) on page 234
- Changing Hitachi Compute Systems Manager ports on page 74

Related references

- Hitachi Compute Systems Manager properties requiring updates for port number changes on page 73
- Prerequisites for installing Deployment Manager on page 166
- Determining which method to use when implementing in a cluster environment on page 192
- Verifying management server free disk space in a cluster environment on page 198
- Checking the cluster configuration using the cluster management software on page 199
- Settings requirements for virus scanning programs in a cluster environment on page 230
- Synchronizing settings in a cluster environment on page 230
- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 291
- Hitachi Command Suite properties requiring updates for port number changes on page 71
- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 291

Installing a new instance of Hitachi Compute Systems Manager in a Linux cluster

This module provides information about installing and configuring a new instance of Hitachi Compute Systems Manager in a cluster environment. Instructions for upgrading in a Linux cluster are provided in a different topic.

Installing a new Hitachi Compute Systems Manager instance on a Linux active node

You can complete a new installation of Hitachi Compute Systems Manager on the Linux management server on an active node in a cluster configuration.

Prerequisites

Before installing on an active node, complete the following tasks:

- Complete the pre-installation checklist.
- Verify that the management server has the required free space for installing in a cluster environment.
- Use the cluster management software to check the cluster settings.
- If you plan to install other products using the integrated media, verify that your system meets the prerequisites for all the products.
- If the cluster environment is created by using other Hitachi Command Suite products, delete all the Hitachi Command Suite services of each product that are registered in the cluster management software group. However, do not delete the shared disk and cluster management IP address from the group.
  For details about how to delete a service, see the manual for that specific product.
- If another Hitachi Command Suite product is installed, check the port number that is used by the database.
  If you run the `hcmds64dbclustersetup` command during the installation procedure, the database port number is set to the default (22032/tcp). If changed the port number from the default, record the port number you are using.

Procedure

1. In the cluster management software, select the active node and start the group.

   Confirm that the group is moved to the active node and only the shared disk and cluster management IP address are enabled.
2. Complete a new installation of Compute Systems Manager on the active node.

   If another Hitachi Command Suite product already exists in the cluster environment, verify the following before installing Compute Systems Manager:
   - Access the shared disk and specify a path as the storage location for the database.
   - Use the IP address of the management server when specifying the logical host name (the virtual host name allocated to the cluster management IP address).

If no other Hitachi Command Suite products exist in the cluster environment, verify the following before installing Compute Systems Manager:

- Access the local disk and specify a path as the storage location for the database.
- Specify the IP address of the active node as the IP address of the management server.

3. Using the Compute Systems Manager user interface, complete the following tasks:
   a. Register the licenses for the products you plan to use. Access the IP address of the active node.
   b. Check whether the URL points to the logical host name by using the following command:

      ```
      HCS-Common-Component-installation-directory/bin/
      hcmds64chgurl -list
      ```

      If the URL does not point to the logical host name, change the URL by using the following command. As the host name, specify the host name you entered during the installation process.

      ```
      HCS-Common-Component-installation-directory/bin/
      hcmds64chgurl -change http://IP-address-or-host-name-of-
      active-node:port-number http://logical-host-name:port-
      number
      ```

4. If you already have a Hitachi Command Suite product configured within the cluster, skip to the next step. If Compute Systems Manager is the first Hitachi Command Suite product in the cluster, create a cluster configuration file as follows:
   a. Add the following information to a blank text file:

      ```
      mode=online
      virtualhost=logical-host-name
      onlinehost=active-node-host-name
      standbyhost=standby-node-host-name
      ```

      Note: On an active node, you must specify `online` for `mode`.

      Save the file as `cluster.conf` in *HCS-Common-Component-installation-directory*`/conf`.
   b. Back up the Compute Systems Manager database by using the following command:

      ```
      HCS-Common-Component-installation-directory/bin/
      hcmds64backups -dir local-disk-directory-for-data-storage-
      backup -auto
      ```

Note: We recommend that you back up the database in case an error occurs.

c. Migrate the database to the shared disk by using the following command:

HCS-Common-Component-installation-directory/bin/hcmds64dbclustersetup -createcluster -databasepath *directory-on-shared-disk-for-database-recreation* -exportpath *local-disk-directory-for-data-storage-backup* -auto

Caution: When you run the `hcmds64dbclustersetup` command, the remote connection settings between Hitachi Device Manager and Hitachi Tuning Manager revert to the default values. If necessary, specify these settings again.

If you created databases on the shared disk for products using the 32-bit Hitachi Command Suite Common Component (Hitachi File Services Manager and Hitachi Storage Navigator Modular 2), you must specify a different directory for the databasepath option.

d. If you recorded a database port number as part of the prerequisites, set that port number.

Note: If a product that uses the 32-bit version of Hitachi Command Suite Common Component is installed (Hitachi File Services Manager or Hitachi Storage Navigator Modular 2), make sure that the port numbers you set do not conflict with the port number used by these products.

5. Use the following command to ensure that the Hitachi Command Suite product services are stopped:

HCS-Common-Component-installation-directory/bin/hcmds64srv -status

6. Use the following command to ensure that the Hitachi Command Suite services do not start automatically when the machine starts:

HCS-Common-Component-installation-directory/bin/hcmds64srv -starttype manual -all

7. To ensure that the Compute Systems Manager services do not start automatically when the machine starts do one of the following:

- Move the files below to another directory.
- 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/S99hicommand64-hcs_csm
- /etc/rc5.d/S99hicommand64-hcs_csm

If any other Hitachi Command Suite product is installed, also prevent that product from automatically starting. To obtain the files to use, refer to the manual for that specific product.

8. Create a work directory on the shared disk.
   a. Create a directory on the shared disk to use as the Compute Systems Manager work directory.
   b. Access the following properties file and enter the work directory path as the value for the `hcsm.shared.directory` property:

      HCSM-installation-directory/ComputeSystemsManager/conf/user.properties

9. To manage a Hitachi server, change the settings as needed so that the management server IP address registered on the Hitachi server can be used as the cluster management IP address.

   Specify the cluster management IP address for the `svp.bind.address` property of the following file:

   HCSM-installation-directory/ComputeSystemsManager/conf/user.properties

   Tip:
   - If the `svp.bind.address` property is not specified, the IP address of the active and standby nodes is registered on the Hitachi server.
   - The management server IP address, with which the Hitachi server is communicating, is registered on the Hitachi server. If you specify the `svp.bind.address` property, the IP address specified for the property is also registered. You can check the management server IP addresses registered on the Hitachi servers by using the Web console. If you find management server IP addresses that are no longer in use, delete them.

10. In the cluster management software, move the group in which you registered the Compute Systems Manager services to the standby node.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191
- About verifying the installation environment on page 41

Related tasks

- Installing the software (Linux) on page 50

- Backing up the database in a cluster environment (Linux) on page 236

Related references

- Determining which method to use when implementing in a cluster environment on page 192
- Verifying management server free disk space in a cluster environment on page 198
- Checking the cluster configuration using the cluster management software on page 199
- Command format for migrating to a Linux cluster environment on page 247
- Settings requirements for virus scanning programs in a cluster environment on page 230
- Hitachi Command Suite properties requiring updates for port number changes on page 71
- Hitachi Compute Systems Manager properties requiring updates for port number changes on page 73
- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 291
- Properties related to clustering (cluster.conf) on page 321

Installing a new Hitachi Compute Systems Manager instance on a Linux standby node

You can complete a new installation of Hitachi Compute Systems Manager on the Linux management server on a standby node in a cluster configuration.

Before you install on the standby node, you must complete the installation on the active node.

Procedure

1. Complete a new installation of Compute Systems Manager on the standby node.

   Before installing Compute Systems Manager on the standby node, be aware of the following requirements:
   - You must install Compute Systems Manager in the same location as on the active node.
   - If other Hitachi Command Suite products already exist and are active in the cluster environment, specify the logical host name (the virtual host name allocated to the cluster management IP address) as the IP address of the management server. If there are no other Hitachi Command Suite products in the cluster environment, specify the IP address or the host name of the standby node.
2. Register the licenses for the products you plan to use.

3. If you already have a Hitachi Command Suite product configured within the cluster, skip to the next step. If Compute Systems Manager is the first Hitachi Command Suite product in the cluster, do the following:

   a. Add the following information to a blank text file:

   ```
   mode=standby
   virtualhost=logical-host-name
   onlinehost=active-node-host-name
   standbyhost=standby-node-host-name
   ```

   Save the file as `cluster.conf` in *HCS-Common-Component-installation-directory*`/conf`.

   Note: On a standby node, you must specify `standby` for `mode`.

   b. Migrate the database to the shared disk by using the following command:

   HCS-Common-Component-installation-directory`/bin/hcmds64dbclustersetup -createcluster -databasepath` *shared-disk-directory-for-database-recreation* `-exportpath` *local-disk-directory-for-data-storage-backup* `-auto`

   For the `databasepath` option, specify the same directory as the one used by the active node to re-create the database.

   Caution: When you run the `hcmds64dbclustersetup` command, the remote connection settings between Hitachi Device Manager and Hitachi Tuning Manager revert to the default values. If necessary, specify these settings again.

4. If you changed the database port number on the active node, specify the same port number on the standby node.
5. Use the following command to ensure that the Hitachi Command Suite product services are stopped:

   HCS-Common-Component-installation-directory`/bin/hcmds64srv -status`
6. Use the following command to ensure that the Hitachi Command Suite product services do not start automatically when the machine starts:

   HCS-Common-Component-installation-directory`/bin/hcmds64srv -starttype manual -all`
7. To ensure that the Compute Systems Manager services do not start automatically when the machine starts do one of the following:
   - Move the files below to another directory.
   - 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/S99hicommand64-hcs_csm`

- /etc/rc5.d/S99hicommand64-hcs_csm

If any other Hitachi Command Suite product is installed, also prevent that product from automatically starting. To obtain the files to use, refer to the manual for that specific product.

8. Access the following properties file and verify that the work directory path created on the active node is specified as the value for the `hcsm.shared.directory` property:

   HCSM-installation-directory`/ComputeSystemsManager/conf/user.properties`

   If not, modify the value to match the value specified on the active node.
9. If, on the active node, you specified the cluster management IP address for the `svp.bind.address` property in the following file, specify the IP address for the standby node as well.

   HCSM-installation-directory`/ComputeSystemsManager/conf/user.properties`
10. Register the Compute Systems Manager services in the cluster management software group.

    If you removed any other Hitachi Command Suite product services before installing Compute Systems Manager, also register the services for those products.
11. In the cluster management software, select the active node to start operation in the cluster environment.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191
- About verifying the installation environment on page 41

Related tasks

- Installing the software (Linux) on page 50
- Starting Hitachi Compute Systems Manager in a cluster environment (Linux) on page 234
- Changing Hitachi Compute Systems Manager ports on page 74

Related references

- Determining which method to use when implementing in a cluster environment on page 192
- Verifying management server free disk space in a cluster environment on page 198
- Synchronizing settings in a cluster environment on page 230
- Command format for migrating to a Linux cluster environment on page 247

- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 291
- Properties related to clustering (cluster.conf) on page 321

Upgrading Hitachi Compute Systems Manager in a Linux cluster environment

This module provides information about upgrading or completing an overwrite installation of Hitachi Compute Systems Manager in a Linux cluster environment.

Upgrading or overwriting Hitachi Compute Systems Manager on a Linux active node

You can complete an upgrade or overwrite installation of Hitachi Compute Systems Manager on a Linux management server that is an active node in a cluster environment.

Prerequisites

Before installing on an active node, complete the following tasks:

- Complete the pre-installation checklist.
- Verify that the management server has the required free space for installing in a cluster environment.
- If you plan to install other products using the integrated media, verify that your system meets the prerequisites for all the products.
- If the cluster environment is created by using other Hitachi Command Suite products, delete all the Hitachi Command Suite services of each product that are registered in the cluster management software group.

Procedure

1. In the cluster management software, move the group in which Compute Systems Manager are registered from the standby node to the active node.
2. If a Hitachi Command Suite product is running, stop it by using the following command:

   ```
   HCS-Common-Component-installation-directory/bin/hcmds64srv -stop
   ```
3. Complete an overwrite or upgrade installation of Compute Systems Manager on the active node.

   Back up the database before the overwrite or upgrade installation by following the installer instructions.
4. If a Hitachi Command Suite product is running, stop it by using the following command:

HCS-Common-Component-installation-directory/bin/hcmds64srv -stop

5. Use the following command to ensure that the Hitachi Command Suite services do not start automatically when the machine starts:

   HCS-Common-Component-installation-directory/bin/hcmds64srv -starttype manual -all

6. To ensure that the Compute Systems Manager services do not start automatically when the machine starts do one of the following:
   - Move the files below to another directory.
   - 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/S99hicommand64-hcs_csm
     - /etc/rc5.d/S99hicommand64-hcs_csm

     If any other Hitachi Command Suite product is installed, also prevent that product from automatically starting. To obtain the files to use, refer to the manual for that specific product.
7. Access the following properties file and verify that `hcsm.shared.directory` property specifies the Compute Systems Manager work directory path:

   HCSM-installation-directory/ComputeSystemsManager/conf/user.properties

   If there is no work directory specified, create a directory on the shared disk, and then specify the path of that directory.
8. To manage a Hitachi server, change the settings as needed so that the management server IP address registered on the Hitachi server can be used as the cluster management IP address.

   Specify the cluster management IP address for the `svp.bind.address` property of the following file:

   HCSM-installation-directory/ComputeSystemsManager/conf/user.properties

Tip:

- If the `svp.bind.address` property is not specified, the IP address of the active and standby nodes is registered on the Hitachi server.
- The management server IP address, with which the Hitachi server is communicating, is registered on the Hitachi server. If you specify the `svp.bind.address` property, the IP address specified for the property is also registered. You can check the management server IP addresses registered on the Hitachi servers by using the Web console. If you find management server IP addresses that are no longer in use, delete them.

9. In the cluster management software, move the group in which you registered the Compute Systems Manager services to the standby node.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191

Related tasks

- Installing the software (Linux) on page 50
- Backing up the database in a cluster environment (Linux) on page 236
- Deleting services from the cluster management software (Linux) on page 229

Related references

- Determining which method to use when implementing in a cluster environment on page 192
- Verifying management server free disk space in a cluster environment on page 198
- Checking the cluster configuration using the cluster management software on page 199

Upgrading or overwriting Hitachi Compute Systems Manager on a Linux standby node

You can complete an upgrade or overwrite installation of Hitachi Compute Systems Manager on a Linux management server that is a standby node in a cluster environment.

Before you overwrite or upgrade on the standby node, you must complete the installation on the active node.

Prerequisites

Before you start the overwrite or upgrade installation, make a note of the file path of the script you used to register the services in the cluster when you installed the first time. You must have this information to register the services after you complete this installation.

Procedure

1. Stop all Hitachi Command Suite product services the following command:

   ```
   HCS-Common-Component-installation-directory/bin/hcmds64srv -stop
   ```

2. Complete an overwrite or upgrade installation of Compute Systems Manager on the standby node.

3. If a Hitachi Command Suite product is running, stop it by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64srv -stop
4. Use the following command to ensure that the Hitachi Command Suite product services do not start automatically when the machine starts:

   HCS-Common-Component-installation-directory/bin/hcmds64srv -starttype manual -all
5. To ensure that the Compute Systems Manager services do not start automatically when the machine starts do one of the following:
   - Move the files below to another directory.
   - 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/S99hicommand64-hcs_csm
     - /etc/rc5.d/S99hicommand64-hcs_csm

     If any other Hitachi Command Suite product is installed, also prevent that product from automatically starting. To obtain the files to use, refer to the manual for that specific product.
6. Access the following properties file and verify that `hcsm.shared.directory` property specifies the same Compute Systems Manager work directory path specified on the active node:

   HCSM-installation-directory/ComputeSystemsManager/conf/user.properties

   If not, change the property to reflect the correct work directory path.
7. If you specified the cluster management IP address for the `svp.bind.address` property on the active node, do the same on the standby node within the following file:

   HCSM-installation-directory/ComputeSystemsManager/conf/user.properties
8. Re-register the services that you deleted from the cluster management software group.
9. In the cluster management software, select the active node to start operations in the cluster environment.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Installing the software (Linux) on page 50
- Starting Hitachi Compute Systems Manager in a cluster environment (Linux) on page 234
- Registering services to a cluster environment (Linux) on page 226

Related references

- Determining which method to use when implementing in a cluster environment on page 192
- Verifying management server free disk space in a cluster environment on page 198

Migrating Hitachi Compute Systems Manager to a cluster environment

This module provides information about migrating an installation of Hitachi Compute Systems Manager to a cluster environment.

Migrating Hitachi Compute Systems Manager to a cluster environment (Windows)

You can migrate a Hitachi Compute Systems Manager Windows management server to a cluster environment.

Prerequisites

Before migrating to a cluster environment, complete the following tasks:

- Complete the pre-installation checklist.
- Verify that the management server has the required free space for installing in a cluster environment.
- Use the cluster management software to check the cluster settings.
- If Windows Firewall is enabled, verify that the Firewall Service is running.
- Verify that the Windows Services and Event Viewer dialog boxes are closed.
- If you are installing a new instance of Deployment Manager, verify all Deployment Manager prerequisites.
- If you plan to install other products using the integrated media, verify that your system meets the prerequisites for all the products.
- If you are using Deployment Manager and plan to migrate Compute Systems Manager to a cluster environment, you must move the Deployment Manager image file to the shared disk.
- Check whether the work folder used by Compute Systems Manager contains any subfolders or files. If it does, move the Compute Systems Manager work folder to the shared disk.
  For details about the Compute Systems Manager work folder, see the description of the `hcsm.shared.directory` property defined in the following file:
  HCSM-installation-folder`\ComputeSystemsManager\conf\user.properties`
- Check the port number used for the database

If you are migrating to a cluster environment, the database port number is set to the default (22032/tcp).
If you have changed the port number from the default, record the port number that you are using.

- As part of the migration process, you must uninstall all Hitachi Command Suite products including Compute Systems Manager. If you changed any of the default values in your initial installation, record those settings because the migration processes resets all settings to the default value.

You can change the environment of a Compute Systems Manager system from a non-cluster to a cluster configuration.

Procedure

1. Export the database by using the following command:
   HCS-Common-Component-installation-folder\bin\hcmds64dbtrans /export /workpath *working-directory* /file *archive-file* /auto
   If other Hitachi Command Suite products are installed, the associated databases are also exported.
2. Remove Compute Systems Manager.
   You must also remove any other Hitachi Command Suite products that are installed.
3. Using the cluster management software, do the following:
   a. Move the owner of the group in which Hitachi Command Suite services are registered to the active node.
   b. Bring the cluster management IP address and shared disks online.
4. Install a new instance of Compute Systems Manager on the active node by running the installation wizard, selecting the cluster configuration option, and specifying the required information.
   If another Hitachi Command Suite product already exists in the cluster environment, you do not need to specify any settings because the installation program automatically uses the existing configuration settings.

   Note: You cannot install Deployment Manager by using the All-in-One Installer.

5. Import the database you exported by using the following command:
   HCS-Common-Component-installation-folder\bin\hcmds64dbtrans /import /workpath *working-directory* /file *archive-file* /type ALL /auto
6. After importing the database to the active node, use the cluster management software to move the owner of the group in which Hitachi Command Suite services are registered to the standby node.

7. Install Compute Systems Manager on the standby node by running the installation wizard.

   During the installation or upgrade, ensure you follow these requirements:
   - Install Compute Systems Manager in the same location as on the active node.
   - If you installed Deployment Manager on the active node, install it on the standby node.
8. If you changed the database port number to a port number other than the default, specify the port number that you recorded earlier.

   Note: If a product that uses the 32-bit version of Hitachi Command Suite Common Component is installed (Hitachi File Services Manager or Hitachi Storage Navigator Modular 2), make sure that the port numbers you set do not conflict with the port number used by these products.

9. To manage a Hitachi server, change the settings as needed so that the management server IP address registered on the Hitachi server can be used as the cluster management IP address.

   Specify the cluster management IP address for the `svp.bind.address` property of the following file:

   HCSM-installation-folder`\ComputeSystemsManager\conf\user.properties`

   Tip:
   - If the `svp.bind.address` property is not specified, the IP address of the active and standby nodes is registered on the Hitachi server.
   - The management server IP address, with which the Hitachi server is communicating, is registered on the Hitachi server. If you specify the `svp.bind.address` property, the IP address specified for the property is also registered. You can check the management server IP addresses registered on the Hitachi servers by using the Web console. If you find management server IP addresses that are no longer in use, delete them.

10. Run the following command to start Compute Systems Manager in the cluster:

    HCS-Common-Component-installation-folder`\Clustersetup\hcmds64clustersrvstate /son /r` *group-name*
11. To register a plug-in license, enter the license key on the standby node.
12. Using the cluster management software, move the owner of the group in which you registered the Compute Systems Manager services to the active node.

13. If you registered a plug-in license on the standby node, enter the same license key on the active node.
14. If you installed Deployment Manager:
    a. Set up the cluster environment so that you can enable and use Deployment Manager.
    b. If you moved the Deployment Manager image files to the shared disk, import the image files.

    For details about managing image files of Deployment Manager, such as importing image files, see the *Hitachi Command Suite Compute Systems Manager User Guide*.
15. If Tuning Manager was remotely connected while you were using Device Manager in a non-cluster environment, you may need to start Tuning Manager and then reconfigure the setting for linking with Tuning Manager.

Related concepts

- About verifying system prerequisites on page 38
- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191
- About verifying the installation environment on page 41

Related tasks

- Installing the software (Windows) on page 47
- Installing from the integrated media by using the all-in-one installer (Windows) on page 49
- Registering services to a cluster environment (Windows) on page 224
- Starting Hitachi Compute Systems Manager in a cluster environment (Windows) on page 234
- Changing Hitachi Compute Systems Manager ports on page 74
- Importing the database on page 185
- Exporting the database on page 184

Related references

- Determining which method to use when implementing in a cluster environment on page 192
- Verifying management server free disk space in a cluster environment on page 198
- Checking the cluster configuration using the cluster management software on page 199
- Settings requirements for virus scanning programs in a cluster environment on page 230
- Hitachi Command Suite properties requiring updates for port number changes on page 71

- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 291

Migrating Hitachi Compute Systems Manager to a cluster environment (Linux)

You can migrate a Hitachi Compute Systems Manager (Linux) management server to a cluster environment.

Prerequisites

Before migrating to a cluster environment, complete the following tasks:

- Complete the pre-installation checklist.
- Verify that the management server has the required free space for installing in a cluster environment.
- Use the cluster management software to check the cluster settings.
- If you plan to install other products using the integrated media, verify that your system meets the prerequisites for all the products.
- Check the port number that is used by the database.
  If you run the `hcmds64dbclustersetup` command during the installation procedure, the database port number is set to the default (22032/tcp).
  If you changed the port number from the default, record the port number you are using.
- Check whether the work directory used by Compute Systems Manager contains any subdirectories or files. If it does, move the Compute Systems Manager work directory to the shared disk.
  For details about the Compute Systems Manager work directory, see the description of the `hcsm.shared.directory` property defined in the following file:
  HCSM-installation-directory`/ComputeSystemsManager/conf/user.properties`

You can change the environment of a Compute Systems Manager system from a non-cluster to a cluster configuration. Before you can migrate to a Linux cluster configuration, you must ensure that Compute Systems Manager is installed and operational on the active node in the new cluster.

Procedure

1. Install Compute Systems Manager on a server that you plan to use as the standby node.
2. Register the licenses for the products you plan to use.
   Access the IP address of the standby node.
3. On the active node, use the following command to change the URL used to access the Compute Systems Manager user interface to point to the logical host name:

HCS-Common-Component-installation-directory/bin/hcmds64chgurl -change http://*active-node-IP-address-or-host-name*:*port-number* http://*logical-host-name*:*port-number*

4. On the active and standby nodes, create a cluster configuration file.

   This procedure is not necessary if the cluster environment was created by using a different Hitachi Command Suite product.

   For active nodes, specify the following in the cluster configuration file:

   Note: You must specify `online` for `mode`.

   ```
   mode=online
   virtualhost=logical-host-name
   onlinehost=active-node-host-name
   standbyhost=standby-node-host-name
   ```

   For standby nodes, specify the following in the cluster configuration file:

   Note: You must specify `standby` for `mode`.

   ```
   mode=standby
   virtualhost=logical-host-name
   onlinehost=active-node-host-name
   standbyhost=standby-node-host-name
   ```

   Save the file as `cluster.conf` in *HCS-Common-Component-installation-directory*/conf.

5. On the active node, use the following command to back up the database:

   HCS-Common-Component-installation-directory/bin/hcmds64backups -dir *local-disk-directory-for-data-storage-backup* -auto

6. On the active node, use the following command to migrate the database to the shared disk:

   HCS-Common-Component-installation-directory/bin/hcmds64dbclustersetup -createcluster -databasepath *directory-on-shared-disk-for-database-recreation* -exportpath *local-disk-directory-for-backup-storage* -auto

7. On the standby node, use the following command to provide access to the database on the shared disk:

   HCS-Common-Component-installation-directory/bin/hcmds64dbclustersetup -createcluster -databasepath *directory-on-shared-disk-for-database-recreation* -exportpath *local-disk-directory-for-backup-storage* -auto

For the *databasepath* option, specify the same directory as the one used by the active node to re-create the database.

Caution: When you run the `hcmds64dbclustersetup` command, the remote connection settings between Hitachi Device Manager and Hitachi Tuning Manager revert to the default values. If necessary, specify these settings again.

If you created databases on the shared disk for products using the 32-bit Hitachi Command Suite Common Component (Hitachi File Services Manager and Hitachi Storage Navigator Modular 2), you must specify a different directory for the databasepath option.

8. If you changed the default database port number, specify the port number you are using on both the active and standby nodes.

Note: If a product that uses the 32-bit version of Hitachi Command Suite Common Component is installed (Hitachi File Services Manager or Hitachi Storage Navigator Modular 2), make sure that the port numbers you set do not conflict with the port number used by these products.

9. On the active and standby nodes, use the following command to ensure that the Hitachi Command Suite product services are stopped:

   HCS-Common-Component-installation-directory`/bin/hcmds64srv -status`

10. On the active and standby nodes, use the following command to ensure that the Hitachi Command Suite product services do not start automatically when the machine starts:

    HCS-Common-Component-installation-directory`/bin/hcmds64srv -starttype manual -all`

11. On the active and standby nodes, ensure that the Compute Systems Manager services do not start automatically when the machine starts by doing one of the following:
    - Move the files below to another directory.
    - 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/S99hicommand64-hcs_csm`
      - `/etc/rc5.d/S99hicommand64-hcs_csm`

      If any other Hitachi Command Suite product is installed, also prevent that product from automatically starting. To obtain the files to use, refer to the manual for that specific product.
12. On both the active and standby nodes, set up the Compute Systems Manager work directory.

a. If you moved the Compute Systems Manager work directory to the shared disk, specify the path of that directory. If you did not move the directory, create a directory on the shared disk, and then specify the path of that directory.

b. Access the following properties file and enter the work directory path as the value for the `hcsm.shared.directory` property:

HCSM-installation-directory`/ComputeSystemsManager/conf/user.properties`

13. To manage a Hitachi server, change the settings as needed so that the management server IP address registered on the Hitachi server can be used as the cluster management IP address.

On both the active and standby nodes, specify the cluster management IP address for the `svp.bind.address` property of the following file:

HCSM-installation-directory`/ComputeSystemsManager/conf/user.properties`

Tip:

- If the `svp.bind.address` property is not specified, the IP address of the active and standby nodes is registered on the Hitachi server.
- The management server IP address, with which the Hitachi server is communicating, is registered on the Hitachi server. If you specify the `svp.bind.address` property, the IP address specified for the property is also registered. You can check the management server IP addresses registered on the Hitachi servers by using the Web console. If you find management server IP addresses that are no longer in use, delete them.

14. Register the Compute Systems Manager services in the cluster management software group.

15. In the cluster management software, select the active node to start operations in the cluster environment.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191
- About verifying the installation environment on page 41

Related tasks

- Installing the software (Linux) on page 50
- Registering services to a cluster environment (Linux) on page 226
- Backing up the database in a cluster environment (Linux) on page 236

- Starting Hitachi Compute Systems Manager in a cluster environment (Linux) on page 234
- Changing Hitachi Compute Systems Manager ports on page 74

Related references

- Determining which method to use when implementing in a cluster environment on page 192
- Verifying management server free disk space in a cluster environment on page 198
- Checking the cluster configuration using the cluster management software on page 199
- Settings requirements for virus scanning programs in a cluster environment on page 230
- Synchronizing settings in a cluster environment on page 230
- Command format for migrating to a Linux cluster environment on page 247
- Hitachi Command Suite properties requiring updates for port number changes on page 71
- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 291
- Properties related to clustering (cluster.conf) on page 321

Registering and deleting services in the cluster management software

This module explains how to register and delete services in the cluster management software.

Registering services to a cluster environment (Windows)

You can manually register Hitachi Command Suite services including Compute Systems Manager in the Windows cluster management software group.

Note: In most cases, you do not need to use this command because all Hitachi Command Suite services register automatically when you install the product.

Therefore, you should only use this comment if you need to re-register services (for example, if you removed services inadvertently).

Prerequisites

Before you register services, ensure you are logged in as a domain user with Administrative permissions. Also ensure that a resource group exists in the cluster in which you can register the Hitachi Command Suite services. If for

some reason the group no longer exists, use the cluster management software to create a group.

Register the Compute Systems Manager services in the cluster management software group by using the following command:

HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvupdate /sreg /r *HCS-cluster-group-name* /sd *drive-letter-of-shared-disk* /ap *resource-name-for-client-access-point*

where

`r` - specifies the name of the group in which the Hitachi Command Suite product services including Compute Systems Manager will be registered. If the group name contains spaces, commas (,), semicolons (;), or equal signs (=), you must enclose the group name in quotation marks ("); for example, if the group name is HCS cluster, you would specify "HCS cluster".

`sd` - specifies the drive letter of the shared disk that is registered to the cluster management software. You cannot specify multiple drive letters for this option. If the database of Hitachi Command Suite products is divided into multiple shared disks, run the `hcmds64clustersrvupdate` command for each shared disk.

`ap` - specifies the name of the resource for the client access point that is registered to the cluster management software.

Tip:

- If you installed the deployment manager, the Deployment Manager services are automatically registered.
- If another Hitachi Command Suite product is installed on the management server, also register the services for that product. For details about other Hitachi Command Suite services, see the documentation for those products.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191

Related references

- Checking the cluster configuration using the cluster management software on page 199

Registering services to a cluster environment (Linux)

Before you can use Compute Systems Manager in the Linux cluster environment, you must register the Hitachi Command Suite services including Compute Systems Manager in the Linux cluster management software group.

Create scripts for registering Linux services by using the sample scripts provided with the software.

Procedure

1. Access the following location on the installation media:

   DVD-Drive/SAMPLE/CLUSTER_TOOL
2. Copy the following zip files to location in which you want to store the sample scripts:
   - HCS_LinuxCluster_SampleScripts_Common.zip

     This script controls the Hitachi Command Suite Common Component services.
   - HCS_LinuxCluster_SampleScripts_HCSM.zip

     This script controls the Compute Systems Manager services.
3. Decompress the zip files to any location. The zip files contain the following scripts:
   - sc_hbase64_hirdb
   - sc_hbase64_hsso
   - sc_hbase64_hweb
   - sc_hbase64_web
   - sc_hbase64_csm
4. Edit the property defined for each script as follows:
   - HCMDS_HOME

     Specify the path of the Hitachi Command Suite Common Component installation directory.
   - PDHOST (required only when the sc_hbase64_hirdb file is used.)

     Specify the logical host name.
5. Store the edited scripts in the following directory on both the active and standby nodes:

   /etc/init.d
6. Assign execution permission to the scripts on both the active and standby nodes by using the following command:

   chmod u+x *script-file-name*
7. In the cluster management software, temporarily stop the cluster operation of Compute Systems Manager.
8. In the cluster management software, click **Add Resource**, and then from **Add Resource to Service**, select **Script** to register the service.

Display the services in the order of registration and specify the following values:

Sequence number	Service Name	Script name (optional)	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 Compute Systems Manager Web Service	sc_hbase64_csm	/etc/init.d/sc_hbase64_csm

If the cluster environment is configured by using another Hitachi Command Suite product, also register the services for that product.

For details about how to register a service, see the manual for that product.

9. Click **Submit**.
   The services are registered in the cluster group.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191

Related tasks

- Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Linux) on page 233

Related references

- Checking the cluster configuration using the cluster management software on page 199

Deleting services from the cluster management software (Windows)

You can manually delete services for Hitachi Command Suite products including Compute Systems Manager from the Windows cluster group.

Note: In most cases, you do not need to use this command because all Hitachi Command Suite services are deleted automatically when you remove the product.

Therefore, you should only use this comment if you need to delete services (for example, if you inadvertently changed the service settings).

Prerequisites

Before you delete services, ensure you are logged in as a domain user with Administrative permissions.

Delete the Compute Systems Manager services in the cluster management software group by using the following command:

- From stand-alone installation media:
  HCSM-installation-media\ClusterSetup\hcmds64clustersrvupdate /sdel /r *HCS-cluster-group-name*
- From integrated installation media:
  integrated-installation-media\HCS\ClusterSetup\hcmds64clustersrvupdate /sdel /r *HCS-cluster-group-name*
- From the installation directory of a Hitachi Command Suite product with v8.1.2 or later:
  HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvupdate /sdel /r *HCS-cluster-group-name*
  where
  `sdel` - deletes the Hitachi Command Suite product services that include Compute Systems Manager from the cluster management software group.
  `r` - specifies the name of the group in which the Hitachi Command Suite product services are registered. If the group name contains spaces, commas (,), semicolons (;), or equal signs (=), you must enclose the group name in quotation marks ("); for example, if the group name is HCS cluster, you would specify "HCS cluster".

Note:

- All the Compute Systems Manager and Hitachi Command Suite product services registered in the group specified by the `r` option are deleted. However, the Hitachi File Services Manager services are not deleted.
  For details about the services of other Hitachi Command Suite products, see the documentation for those products.
- If the resource name of a service has changed, all of the resource names are initialized when you delete the service and then re-register it. Record the resource names for the services that you are deleting so that you can change the names after re-registering those services.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191

Deleting services from the cluster management software (Linux)

You can delete services for Hitachi Command Suite products including Compute Systems Manager from the Linux cluster group.

Delete the Compute Systems Manager services in the cluster management software group as follows:

Procedure

1. In the cluster management software, temporarily stop the cluster operation of Compute Systems Manager.
2. In the cluster management software, click **Remove** for each of the following services:
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
   - HCS Compute Systems Manager Web Service
   - HiRDB

   If the cluster environment is created by using another Hitachi Command Suite product, also delete the services of that product.

   For details about how to delete a service, see the manual of the product.
3. Click **Submit**.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191

Related tasks

- Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Linux) on page 233

Configuring Hitachi Compute Systems Manager within a cluster environment

This module provides information about configuring Hitachi Compute Systems Manager within a cluster by verifying environment settings and adding resources.

Related references

- Synchronizing settings in a cluster environment on page 230

Settings requirements for virus scanning programs in a cluster environment

To use a virus scanning program on a machine that manages a shared disk, exclude the directory on the shared disk that was specified when the database was migrated from the scanning parameters.

If a virus scanning program accesses database files on the shared disk, a failure might occur because of delayed I/O operations, file exclusion, or other causes.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Installing or Upgrading Hitachi Compute Systems Manager in a Windows cluster on page 201
- Migrating Hitachi Compute Systems Manager to a cluster environment (Linux) on page 220
- Migrating Hitachi Compute Systems Manager to a cluster environment (Windows) on page 216
- Installing a new Hitachi Compute Systems Manager instance on a Linux standby node on page 209
- Upgrading the software from v7.x in a cluster environment on page 327

Synchronizing settings in a cluster environment

When you use Hitachi Compute Systems Manager in a cluster environment, you must ensure that the settings for the following options are synchronized on the active and standby nodes:

- Warning banner message settings
- Password policy settings
- Number of login attempts permitted before automatic account lockout

Additionally, after installing Compute Systems Manager in a cluster environment, you must ensure that when you change the Compute Systems Manager software configuration, you use the same settings on all nodes.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Installing or Upgrading Hitachi Compute Systems Manager in a Windows cluster on page 201
- Migrating Hitachi Compute Systems Manager to a cluster environment (Linux) on page 220
- Migrating Hitachi Compute Systems Manager to a cluster environment (Windows) on page 216
- Installing a new Hitachi Compute Systems Manager instance on a Linux standby node on page 209

Setting up Deployment Manager in a cluster environment

You must set up Deployment Manager to run in a cluster environment by using the Compute Systems Manager interface.

Prerequisites

Ensure that you installed Deployment Manager when you installed Hitachi Compute Systems Manager in the cluster environment.

Procedure

1. Log in to Compute Systems Manager, access the **Administration** tab and select **Deployment > Settings**.
2. Specify the following settings:
   - **Default Path**: Specify the directory on the shared disk.
   - **Cluster Setting**: Select **Cluster Environment**.
   - For the following settings, specify the content that matches your environment:
     If you use the same IP address for the DHCP server and Deployment Manager, specify the following:
     - **DHCP Server Installed on the HCSM Server**: Yes.
     - **Cluster IP Address**: Specify the same IP address as the DHCP server.

     If you use a different IP address for the DHCP server and Deployment Manager, specify the following:
     - **DHCP Server Installed on the HCSM Server**: No.

- **Cluster IP Address**: Specify a different IP address for the DHCP server.

3. Temporarily stop the Compute Systems Manager operation by using the following command:

   HCS-Common-Component-installation-directory\ClusterSetup\hcmds64clustersrvstate /soff /r *HCS-cluster-group-name*

4. Start cluster operation for Compute Systems Manager by using the following command:

   HCS-Common-Component-installation-directory\ClusterSetup\hcmds64clustersrvstate /son /r *HCS-cluster-group-name*

Related concepts

- Hitachi Compute Systems Manager services used in a cluster environment on page 191
- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- About upgrading from Hitachi Compute Systems Manager v7.x on page 324

Related tasks

- Migrating Hitachi Compute Systems Manager to a cluster environment (Windows) on page 216
- Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Windows) on page 232
- Starting Hitachi Compute Systems Manager in a cluster environment (Windows) on page 234
- Installing or Upgrading Hitachi Compute Systems Manager in a Windows cluster on page 201
- Upgrading the software from v7.x in a cluster environment on page 327

Starting and stopping services in a cluster environment

This module provides information about starting and stopping Hitachi Compute Systems Manager in a cluster environment, which is required for many administrative tasks.

Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Windows)

If you are using Hitachi Compute Systems Manager in a Windows cluster environment and you must temporarily stop Compute Systems Manager, use the following command:

- From stand-alone installation media:
  HCSM-installation-media/ClusterSetup/hcmds64clustersrvstate /soff /r *HCS-cluster-group-name*

- From integrated installation media:
  integrated-installation-media\HCS\ClusterSetup\hcmds64clustersrvstate /soff /r *HCS-cluster-group-name*
- From the installation directory of a Hitachi Command Suite product with v8.1.2 or later:
  HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvstate /soff /r *HCS-cluster-group-name*
  where
  `soff` - takes the Hitachi Command Suite product services that include Compute Systems Manager that are registered to the cluster management software group offline and disables failover.
  `r` - specifies the name of the group in which the Hitachi Command Suite product services are registered. If the group name contains spaces, commas (,), semicolons (;), or equal signs (=), you must enclose the group name in quotation marks ("); for example, if the group name is HCS cluster, you would specify "HCS cluster".

The groups are taken offline and failover is disabled.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191

Related tasks

- Starting Hitachi Compute Systems Manager in a cluster environment (Windows) on page 234

Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Linux)

If you are using Hitachi Compute Systems Manager in a Linux cluster environment, you must temporarily stop Compute Systems Manager when setting up the cluster configuration.

To temporarily stop operation in a cluster environment:

Procedure

1. In the cluster management software, open the **Service Groups** window, and select the group in which Hitachi Command Suite product services, including Compute Systems Manager services, are registered.
2. Click **stop (disable)** to stop and disable the group.
   The groups are taken offline and failover is disabled.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191

Related tasks

- Starting Hitachi Compute Systems Manager in a cluster environment (Linux) on page 234

Starting Hitachi Compute Systems Manager in a cluster environment (Windows)

Before Hitachi Compute Systems Manager can run in a cluster environment, you must start the services.

To start Compute Systems Manager services in a Windows cluster environment, use the following command:

```
HCS-Common-Component-installation-directory\ClusterSetup
\hcmds64clustersrvstate /son /r HCS-cluster-group-name
```

where

`son` - brings online and enables failover for the Hitachi Command Suite product services that include Compute Systems Manager and are registered to the cluster management software group.

`r` - specifies the name of the group in which the Hitachi Command Suite product services including Compute Systems Manager are registered. If the group name contains spaces, commas (,), semicolons (;), or equal signs (=), you must enclose the group name in quotation marks ("); for example, if the group name is HCS cluster, you would specify "HCS cluster".

The groups are registered are brought online and failover is enabled.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191

Starting Hitachi Compute Systems Manager in a cluster environment (Linux)

Before Hitachi Compute Systems Manager can run in a cluster environment, you must start the services.

To start Compute Systems Manager services in a Linux cluster environment:

Procedure

1. In the cluster management software, open the **Service Groups** window, and select the group in which Hitachi Command Suite product services, including Compute Systems Manager services, are registered.
2. From the drop-down list, select the active or standby node and click **start** to start the services.
   The system brings the group services online and failover is enabled.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191

Managing the database in a cluster environment

This module provides information about managing the Hitachi Compute Systems Manager database in a cluster environment.

Backing up the database in a cluster environment (Windows)

In a cluster environment, you must maintain a backup copy of the database on the active node so that the Hitachi Compute Systems Manager Windows management server can restore the database if there is a failure. You complete all database management tasks on the active node.

Caution: When Hitachi Device Manager is installed on the same management server as Compute Systems Manager, and is remotely connected to Hitachi Tuning Manager, you must temporarily stop it on the computer on which the Tuning Manager server is installed. You can start Tuning Manager again after backing up the database. For details on how to stop and restart Tuning Manager, see the documentation for the version of Tuning Manager installed in your system.

Procedure

1. Temporarily stop Compute Systems Manager operations within the cluster by using the following command:

   ```
   HCS-Common-Component-installation-folder\ClusterSetup
   \hcmds64srvstate /soff /r HCS-cluster-group-name
   ```

2. Back up the database by using the following command:

   ```
   HCS-Common-Component-installation-folder\bin
   \hcmds64backups /dir local-disk-folder-for-backup-storage /
   auto
   ```

To specify the folder for the `dir` option, use the absolute path on the shared disk where the database backup files are stored. Do not specify a subfolder or a specific file.

3. Stop the Hitachi Command Suite product services by using the following command:

   HCS-Common-Component-installation-folder\bin\hcmds64srv /stop

4. Confirm that the Hitachi Command Suite product services are stopped or that the return value is 0 by using the following command:

   HCS-Common-Component-installation-folder\bin\hcmds64srv /statusall

5. Start the Compute Systems Manager cluster operations by using the following command:

   HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvstate /son /r *HCS-cluster-group-name*

Result

You now have a backup copy of the latest Compute Systems Manager database.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Restoring the database in a cluster environment (Windows) on page 238
- Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Windows) on page 232
- Starting Hitachi Compute Systems Manager in a cluster environment (Windows) on page 234
- Stopping Hitachi Compute Systems Manager on page 175
- Backing up the database on page 181

Related references

- Prerequisites for database backup on page 180

Backing up the database in a cluster environment (Linux)

In a cluster environment, you must maintain a backup copy of the database on the active node so that the Hitachi Compute Systems Manager Linux management server can restore the database if there is a failure. You complete all database management tasks on the active node.

Prerequisites

Before you back up the database, complete the following tasks:

- Record the file path of the script you used to register the services to the cluster management software when you first installed the product. This information is used for registering services to the cluster management software after the database backup.
- Delete the Hitachi Command Suite product services that are registered in the cluster management software group, including the Hitachi Compute Systems Manager services.

Procedure

1. Verify that the cluster management software group was moved to the active node. If the group was moved to the standby node, move it to the active node.
2. Confirm that the Hitachi Command Suite product services are stopped or that the return value is 0 by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64srv -statusall
3. Back up the database by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64backups -dir *local-disk-directory-for-backup-storage* -auto

   To specify the directory for the `dir` option, use the absolute path on the shared disk where the database backup files are stored. Do not specify a subdirectory or a specific file.
4. Stop the Hitachi Command Suite product services by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64srv -stop
5. Confirm that the Hitachi Command Suite product services are stopped or that the return value is 0 by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64srv -statusall
6. Re-register the services that were deleted from the cluster management software group.
7. In the cluster management software, select the active node to start operation in a cluster environment.

Result

You now have a backup copy of the latest Compute Systems Manager database.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Registering services to a cluster environment (Linux) on page 226
- Deleting services from the cluster management software (Linux) on page 229
- Starting Hitachi Compute Systems Manager in a cluster environment (Linux) on page 234
- Stopping Hitachi Compute Systems Manager on page 175
- Backing up the database on page 181

Related references

- Prerequisites for database backup on page 180

Restoring the database in a cluster environment (Windows)

If you encounter a failure situation, you can restore the existing database on the Windows management server active node using the database backup. You complete all database management tasks on the active node.

Caution:

- When Hitachi Device Manager is installed on the same management server as Hitachi Compute Systems Manager, and is remotely connected to Hitachi Tuning Manager, you must temporarily stop it on the computer where the Tuning Manager server is installed. You can start Tuning Manager again after the database has been restored. For details on how to stop and restart Tuning Manager, see the documentation for the version of Tuning Manager installed in your system.
- The `hcmds64db` command, which you use to restore the database, creates temporary files while restoring the database. Ensure that you have write permission for the database directory and that the directory has enough free space.

Procedure

1. Temporarily stop Compute Systems Manager within the cluster by using the following command:

   ```
   HCS-Common-Component-installation-folder\ClusterSetup
   \hcmds64clustersrvstate /soff /r HCS-resource-group-name
   ```

2. On the active node, restore the database by using the following command:

   ```
   HCS-Common-Component-installation-folder\bin\hcmds64db /
   restore backup-file /type ALL
   ```

   where

   backup-file is the absolute path to the backup file (`backup.hdb`) saved on the shared disk.

3. Start Compute Systems Manager operations within the cluster by using the following command:

   ```
   HCS-Common-Component-installation-folder\ClusterSetup
   \hcmds64clustersrvstate /son /r HCS-resource-group-name
   ```
4. Use the Compute Systems Manager user interface to check the status of the Compute Systems Manager tasks. If a task is incomplete or failed, recreate the task or reschedule it.
5. If Hitachi Device Manager is remotely connected to Tuning Manager , the settings are reset when you restore the database. You must set up your Tuning Manager connection again.

Related tasks

- Backing up the database in a cluster environment (Windows) on page 235
- Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Windows) on page 232
- Starting Hitachi Compute Systems Manager in a cluster environment (Windows) on page 234
- Restoring the database on page 182

Related references

- Prerequisites for restoring the database on page 182

Restoring the database in a cluster environment (Linux)

If you encounter a failure situation, you can restore the existing database on the Linux management server active node using the database backup. You complete all database management tasks on the active node.

Prerequisites

Before you restore the database, complete the following tasks:

- Record the file path of the script you used to register the services to the cluster management software when you first installed the product. This information is used for registering services to the cluster management software after the database restore.
- Delete the Hitachi Command Suite product services that are registered in the cluster management software group, including the Hitachi Compute Systems Manager services.

Procedure

1. Verify that the cluster management software group was moved to the active node. If the group was moved to the standby node, move it to the active node.
2. Restore the database by using the following command:

   ```
   HCS-Common-Component-installation-directory/bin/hcmds64db -
   restore backup-file -type ALL
   ```

To specify the directory for the `dir` option, use the absolute path on the shared disk where the database backup files are stored. Do not specify a subdirectory or a specific file.

3. Stop Hitachi Command Suite products within the cluster by using the following command:

   HCS-Common-Component-installation-directory`/bin/hcmds64srv -stop`

4. Re-register the services that were deleted from the cluster management software group.
5. In the cluster management software, select the active node to start operation in a cluster environment.
6. Use the Compute Systems Manager user interface to check the status of the Compute Systems Manager tasks. If a task is incomplete or failed, recreate the task or reschedule it.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Registering services to a cluster environment (Linux) on page 226
- Deleting services from the cluster management software (Linux) on page 229
- Starting Hitachi Compute Systems Manager in a cluster environment (Linux) on page 234
- Restoring the database on page 182
- Starting Hitachi Compute Systems Manager on page 174

Related references

- Prerequisites for restoring the database on page 182

Exporting the database in a cluster environment (Windows)

To migrate the Hitachi Compute Systems Manager database from a Windows server to another server in a cluster environment, you export the existing database. You can also use the exported database to restore a database after a failure. You complete all database management tasks on the active node.

Caution: When Hitachi Device Manager is installed on the same management server as Compute Systems Manager, and is remotely connected to Hitachi Tuning Manager, you must temporarily stop it on the computer on which the Tuning Manager server is installed. You can start Tuning Manager again after exporting the database. For details on how to stop and restart Tuning Manager, see the documentation for the version of Tuning Manager installed on your system.

Procedure

1. Temporarily stop Compute Systems Manager within the cluster by using the following command:

   HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvstate /soff /r *HCS-cluster-group-name*
2. Export the databases by using the following command:

   HCS-Common-Component-installation-folder\bin\hcmds64dbtrans /export /workpath *working-folder* /file *archive-file* /auto

   When specifying the folder for the `workpath` option, use an absolute path on the local disk where you want to temporarily store the database data. Ensure that the folder you specify is empty and does not contain any subfolders or files.

   When specifying the file name for the `file` option, specify the absolute path of the archive file that you want the export command to generate.

   If the system cannot create an archive file, verify that there is enough capacity on the migration destination server and try exporting again.
3. For migrations, transfer the exported files to the migration target server.
4. Stop the Hitachi Command Suite product services by using the following command:

   HCS-Common-Component-installation-folder\bin\hcmds64srv /stop
5. Start Compute Systems Manager within the cluster by using the following command:

   HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvstate /son /r *HCS-cluster-group-name*

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Windows) on page 232
- Starting Hitachi Compute Systems Manager in a cluster environment (Windows) on page 234
- Stopping Hitachi Compute Systems Manager on page 175
- Exporting the database on page 184

Related references

- Prerequisites for database migration on page 183

Exporting the database in a cluster environment (Linux)

To migrate the Hitachi Compute Systems Manager database from a Linux server to another server in a cluster environment, you export the existing database. You can also use the exported database to restore a database after a failure. You complete all database management tasks on the active node.

Prerequisites

Before you export the database, complete the following tasks:

- Record the file path of the script you used to register the services to the cluster management software when you first installed the product. This information is used for registering services to the cluster management software after the database export.
- Delete the Hitachi Command Suite product services that are registered in the cluster management software group, including the Hitachi Compute Systems Manager services.

Procedure

1. Verify that the cluster management software group was moved to the active node. If the group was moved to the standby node, move it to the active node.
2. Export the databases by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64dbtrans -export -workpath *working-directory* -file *archive-file* -auto

   When specifying the directory for the `workpath` option, use an absolute path on the local disk where you want to temporarily store the database data. Ensure that the directory you specify is empty and does not contain any subdirectories or files.

   When specifying the file name for the `file` option, specify the absolute path of the archive file that you want the export command to generate.

   If the system cannot create an archive file, verify that there is enough capacity on the migration destination server and try exporting again.
3. For migrations, transfer the exported files to the migration target server.
4. Stop the Hitachi Command Suite product services by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64srv -stop
5. Re-register the services that were deleted from the cluster management software group.
6. In the cluster management software, select the active node to start operation in a cluster environment.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Registering services to a cluster environment (Linux) on page 226
- Deleting services from the cluster management software (Linux) on page 229
- Starting Hitachi Compute Systems Manager in a cluster environment (Linux) on page 234
- Stopping Hitachi Compute Systems Manager on page 175
- Exporting the database on page 184

Related references

- Prerequisites for database migration on page 183

Importing the database in a cluster environment (Windows)

After you export the Hitachi Compute Systems Manager database from an existing server in the cluster, you can import it to another Windows Compute Systems Manager server. You can also use an exported database to restore an existing database after a failure. All database management in a cluster environment is completed on the active node.

Prerequisites

If you are using a value other than the default for a property on the migration source management server, review the relevant settings in the properties files on the active and standby nodes of the migration destination. The properties file is not migrated to the migration destination server even if you import the database. This means you must update the property values in the destination servers if you need to maintain the settings.

Caution: When Hitachi Device Manager is installed on the same management server as Compute Systems Manager, and is remotely connected to Hitachi Tuning Manager, you must temporarily stop it on the computer on which the Tuning Manager server is installed. You can start Tuning Manager again after importing the database. For details on how to stop and restart Tuning Manager, see the documentation for the version of Tuning Manager installed on your system.

Procedure

1. Temporarily stop Compute Systems Manager within the cluster by using the following command:

   ```
   HCS-Common-Component-installation-folder\ClusterSetup
   \hcmds64clustersrvstate /soff /r HCS-cluster-group-name
   ```

2. On the active node, import the database by using the following command:

   HCS-Common-Component-installation-folder\bin\hcmds64dbtrans /import /workpath *working-folder* /file *archive-file* /type {ALL|*Hitachi-Command-Suite-product-names*} /auto

   When specifying the command options, use the following descriptions:

   - workpath

     When importing a database using archive files:

     Specify the *working-folder* using the absolute path of the folder in which to unpack the archive file. Specify a folder on a local disk. The file option is mandatory when importing a database from an archive file. Ensure that the folder you specify is empty and does not contain any subfolders or files.

     When importing a database without using archive files:

     Specify the *working-folder* that contains the database data files transferred from the migration source. Do not change the file structure in the transferred folder or any of the subfolders. In this case, do not specify the file option.

   - file

     Specify the *archive-file* using the absolute path of the database archive file that you transferred from the original server. You can omit this option if the database data transferred from the migration source is stored in the directory specified in workpath.

   - type

     To import all Hitachi Command Suite product databases, specify the type as ALL. To import the Compute Systems Manager database only, specify HCSM. To import other Hitachi Command Suite product databases individually, see the documentation for the applicable Hitachi Command Suite product.

3. Start the Compute Systems Manager services by using the following command:

   HCS-Common-Component-installation-folder\bin\hcmds64srv /start

4. Start Compute Systems Manager cluster operations by using the following command:

   HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvstate /son /r *HCS-cluster-group-name*

5. Back up the databases by using the following command:

   As a precaution, we recommend that you immediately back up the databases you imported.

   HCS-Common-Component-installation-folder/bin/hcmds64backups /dir *local-disk-folder-for-backup-storage* /auto

To specify the folder for the `dir` option, use the absolute path on the shared disk where the database backup files are stored. Do not specify a subfolder or a specific file.

6. If Hitachi Device Manager is remotely connected to Tuning Manager, the settings are reset when you restore the database. You must set up your Tuning Manager connection again.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Windows) on page 232
- Starting Hitachi Compute Systems Manager in a cluster environment (Windows) on page 234
- Backing up the database in a cluster environment (Windows) on page 235
- Starting Hitachi Compute Systems Manager on page 174
- Importing the database on page 185

Related references

- Prerequisites for database migration on page 183

Importing the database in a cluster environment (Linux)

After you export the Hitachi Compute Systems Manager database from an existing server in the cluster, you can import it to another Linux Compute Systems Manager server. You can also use an exported database to restore an existing database after a failure. All database management in a cluster environment is completed on the active node.

Prerequisites

Before you import the database, complete the following tasks:

- If you are using a value other than the default for a property on the migration source management server, review the relevant settings in the properties files on the active and standby nodes of the migration destination. The properties file is not migrated to the migration destination server even if you import the database. This means you must update the property values in the destination servers if you need to maintain the settings.
- Record the file path of the script you used to register the services to the cluster management software when you first installed the product. This information is used for registering services to the cluster management software after the database import.

- Delete the Hitachi Command Suite product services that are registered in the cluster management software group, including the Hitachi Compute Systems Manager services.

Procedure

1. Verify that the cluster management software group was moved to the active node. If the group was moved to the standby node, move it to the active node.
2. Import the database by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64dbtrans -import -workpath *working-directory* -file *archive-file* -type {ALL|*Hitachi-Command-Suite-product-names*} -auto

   When specifying the command options, use the following descriptions:

   - `workpath`

     When importing a database using archive files:
     Specify the *working-directory* using the absolute path of the directory in which to unpack the archive file. Specify a directory on a local disk. The file option is mandatory when importing a database from an archive file. Ensure that the directory you specify is empty and does not contain any subdirectories or files.
     When importing a database without using archive files:
     Specify the *working-directory* that contains the database data files transferred from the migration source. Do not change the file structure in the transferred directory or any of the subdirectories. In this case, do not specify the file option.
   - `file`

     Specify the *archive-file* using the absolute path of the database archive file that you transferred from the original server. You can omit this option if the database data transferred from the migration source is stored in the directory specified in `workpath`.
   - `type`

     To import all Hitachi Command Suite product databases, specify the type as ALL. To import the Compute Systems Manager database only, specify HCSM. To import other Hitachi Command Suite product databases individually, see the documentation for the applicable Hitachi Command Suite product.
3. Stop the Hitachi Command Suite product services by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64srv -stop
4. Re-register the services that were deleted from the cluster management software group.

5. In the cluster management software, select the active node to start operation in a cluster environment.
6. Back up the database, as a precaution, by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64backups -dir *local-disk-directory-for-backup-storage* -auto

   To specify the directory for the `dir` option, use the absolute path on the shared disk where the database backup files are stored. Do not specify a subdirectory or a specific file.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Registering services to a cluster environment (Linux) on page 226
- Deleting services from the cluster management software (Linux) on page 229
- Starting Hitachi Compute Systems Manager in a cluster environment (Linux) on page 234
- Backing up the database in a cluster environment (Linux) on page 236
- Starting Hitachi Compute Systems Manager on page 174
- Importing the database on page 185

Related references

- Prerequisites for database migration on page 183

Command format for migrating to a Linux cluster environment

You can use the `hcmds64dbclustersetup` command to migrate Hitachi Compute Systems Manager to a Linux cluster environment. This command backs up the pre-migration database to the local disk and re-creates (on the shared disk) a database for use in a cluster environment.

Note: You do not need this command in Windows clusters because the database is automatically migrated during the installation process.

You use the Linux cluster setup migration command as follows:

HCS-Common-Component-installation-directory/bin/hcmds64dbclustersetup -createcluster -databasepath *directory-on-shared-disk-for-database-recreation* -exportpath *local-disk-directory-for-data-storage-backup* -auto

where

- `createcluster` migrates a Hitachi Command Suite product from a non-cluster configuration to a cluster configuration

- `databasepath` specifies the directory in which to recreate the database for use in a cluster environment. Specify an absolute path that is 63 characters or less for a directory on the shared disk. You can use the following characters A~Z a~z 0~9 and the forward slash (/).
- `exportpath` specifies the directory in which to store the pre-migration database that you are backing up. Specify an absolute path that is 63 characters or less for a directory on the local disk. The valid path characters are the same as for the `databasepath` option.
- `auto` is an optional parameter that specifies whether to automatically change the status of Hitachi Command Suite products and the database services to the status required for backing up the database. After the command runs, the Hitachi Command Suite products and the database services are changed to the stop status.

Caution: When using this command, be aware of the following:

- When you execute the `hcmds64dbclustersetup` command, the port number used for the database and the remote connection settings between Hitachi Device Manager and Hitachi Tuning Manager revert to the default settings.
- The port number used for the database is initialized to the default value, `22032/tcp`.
- If the *`local-disk-directory-for-data-storage-backup`* already exists, delete the entire content of the directory, or delete the directory.
- Do not disconnect the shared disk from the active node until the command completes successfully.
- If you restart the server after the command ends with an error, the shared disk might connect to the standby node.
- If you created databases on the shared disk for products using the 32-bit Hitachi Command Suite Common Component (Hitachi File Services Manager and Hitachi Storage Navigator Modular 2), you must specify a different directory for the databasepath option.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Installing a new Hitachi Compute Systems Manager instance on a Linux active node on page 205
- Installing a new Hitachi Compute Systems Manager instance on a Linux standby node on page 209
- Migrating Hitachi Compute Systems Manager to a cluster environment (Linux) on page 220

Removing software from a cluster environment

This module provides information about removing software components from a cluster environment.

Removing Deployment Manager from a cluster environment

You can remove Deployment Manager from a cluster environment without removing Hitachi Compute Systems Manager from the environment.

Procedure

1. In the cluster management software, move the owner of the group in which the Compute Systems Manager services are registered to the active node.
2. Remove Deployment Manager from the active node.
3. On the active node, delete any files and folders that are no longer required.
4. In the cluster management software, move the owner of the group in which the Compute Systems Manager services are registered to the standby node.
5. Remove Deployment Manager from the standby node.
6. On the standby node, delete any files and folders that are no longer required.
7. Start cluster operations by using the following command:

   HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvstate /son /r *HCS-cluster-group-name*
8. Using the cluster management software, move the owner of the group containing the Compute Systems Manager resources to the active node.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Removing the software (Windows) on page 61

Removing the software in a cluster environment (Windows)

You can remove the Hitachi Compute Systems Manager software from a Windows server in a cluster environment if you want to migrate to a different server or stop Compute Systems Manager operation.

Note: If you remove Compute Systems Manager, the properties files, database files, log files, and other product-related files are deleted.

If you plan to continue using other Hitachi Command Suite products, note the following:

When you remove the software from an active node, all registered services are removed and then re-registered by default when you complete the removal on the standby node. If you changed the service resource names, record the resource names in advance, and then manually change the names after the removal is finished.

This step does not apply to Hitachi File Services Manager resources because they are not removed.

Procedure

1. In the cluster management software, move the owner of the group in which the Compute Systems Manager services are registered to the active node.
2. Remove Compute Systems Manager from the active node. If you used the All-in-One Installer for installation, use the All-in-One Uninstaller to remove the software.
3. On the active node, delete any files and folders that are no longer required (such as those files and folders created during installation in the cluster environment).
4. In the cluster management software, move the owner of the Compute Systems Manager services group to the standby node.
5. Remove Compute Systems Manager from the standby node.
6. On the standby node, delete any files and folders that are no longer required (such as those files and folders created during installation in the cluster environment).
7. If the following resources are not in use by other applications, use the cluster management software to take them offline, and then delete them.
8. If the Compute Systems Manager services group is no longer needed, delete it.
9. If you want to continue using other Hitachi Command Suite products, do the following:
   a. Start cluster operations by using the following command:

      ```
      HCS-Common-Component-installation-folder\ClusterSetup
      \hcmds64clustersrvstate /son /r HCS-cluster-group-name
      ```

   b. Using the cluster management software, move the owner of the group containing the Hitachi Command Suite resources to the active node.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190

Related tasks

- Starting Hitachi Compute Systems Manager in a cluster environment (Windows) on page 234
- Backing up the database in a cluster environment (Windows) on page 235
- Removing the software (Windows) on page 61

Related references

- Prerequisites for removing the software on page 60

Removing the software in a cluster environment (Linux)

You can remove the Hitachi Compute Systems Manager software from a Linux server in a cluster environment if you want to migrate to a different server or stop Compute Systems Manager operation.

Note: If you remove Compute Systems Manager, the properties files, database files, log files, and other product-related files are deleted.

Prerequisites

Before you remove the software, delete the Hitachi Command Suite product services that are registered in the cluster management software group, including the Hitachi Compute Systems Manager services.

Procedure

1. In the cluster management software, move the group in which Compute Systems Manager services are registered from the standby node to the active node.
2. Stop the Hitachi Command Suite product services by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64srv -stop
3. Back up the database by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64backups -dir *local-disk-directory-for-backup-storage* -auto
4. Stop the Hitachi Command Suite product services by using the following command:

   HCS-Common-Component-installation-directory/bin/hcmds64srv -stop
5. Remove Compute Systems Manager from the active node.
6. On the active node, delete any files and directories that are no longer required (such as those files and directories created during installation in the cluster environment).

7. In the cluster management software, move the Compute Systems Manager services group to the standby node.
8. Remove Compute Systems Manager from the standby node.
9. On the standby node, delete any files and directories that are no longer required (such as those files and directories created during installation in the cluster environment).
10. If the following resources are not in use by other applications, use the cluster management software to take them offline, and then delete them:
    - cluster management IP address
    - shared disk
11. If the Compute Systems Manager services group is no longer needed, delete it.
12. If you want to continue using other Hitachi Command Suite products, register the Hitachi Command Suite services you want to use in the cluster management software group.

    For details about how to register services, see the documentation for that product.
13. To being using another Hitachi Command Suite product In the cluster, use the cluster management software to select the active node to start operation in a cluster environment.

Related concepts

- About implementing Hitachi Compute Systems Manager in a cluster environment on page 190
- Hitachi Compute Systems Manager services used in a cluster environment on page 191

Related tasks

- Deleting services from the cluster management software (Linux) on page 229
- Starting Hitachi Compute Systems Manager in a cluster environment (Linux) on page 234
- Backing up the database in a cluster environment (Linux) on page 236
- Removing the software (Linux) on page 62
- Installing from the integrated media by using the all-in-one installer (Windows) on page 49
- Stopping Hitachi Compute Systems Manager on page 175

Related references

- Prerequisites for removing the software on page 60

10

Troubleshooting

This module describes troubleshooting Hitachi Compute Systems Manager (HCSM).

- ☐ Troubleshooting overview
- ☐ Troubleshooting examples
- ☐ Collecting maintenance information
- ☐ Reviewing audit log information
- ☐ Log file settings

Troubleshooting overview

If problems occur when you are running Hitachi Compute Systems Manager, follow the instructions that appear in the error messages generated by Compute Systems Manager.

In some cases, no messages display or following the instructions does not resolve the problem. In this situation, contact your system administrator and collect additional maintenance information so that you can continue to investigate the failure.

Related references

- Troubleshooting example: no login window displayed on page 254
- Troubleshooting example: management server does not start on page 255
- Troubleshooting example: database corruption on page 255
- Troubleshooting example: database corruption in a Windows cluster environment on page 256
- Troubleshooting example: database corruption in a Linux cluster environment on page 257

Troubleshooting examples

This module provides troubleshooting examples to help you better understand the troubleshooting process.

Troubleshooting example: no login window displayed

If an error occurs while trying to access the management client from a browser, Hitachi Compute Systems Manager generates an error message. The following is an example of the troubleshooting information Compute Systems Manager might generate when no login window opens even though the user specified the correct URL.

Possible cause

Compute Systems Manager is not running or is in the process of starting on the management server.

Countermeasure

Check the Compute Systems Manager operating status to see if the service is starting. If yes, wait until the service starts. If the service is not starting, start it.

Related concepts

- Troubleshooting overview on page 254

Troubleshooting example: management server does not start

If Hitachi Compute Systems Manager does not start as expected, Compute Systems Manager generates an error message. The following is an example of the troubleshooting information Compute Systems Manager might generate when the Compute Systems Manager service or the Hitachi Command Suite Common Component does not start.

Possible cause

The desktop heap might be insufficient.

Countermeasure

Verify that the desktop heap is set to the required size. For details, see the Microsoft support website.

Related concepts

- Troubleshooting overview on page 254

Troubleshooting example: database corruption

If you cannot restore a database using the `hcmds64db` or `hcmds64dbtrans` command, Hitachi Compute Systems Manager generates an error message. If you receive this type of error, you can use the `hcmds64dbrepair` command to restore the database.

Possible cause

The database might be corrupted.

Countermeasure

1. Verify that the available capacity in the following directory is greater than the size of the database:
   In Windows:
   HCS-Common-Component-installation-folder\tmp
   In Linux:
   HCS-Common-Component-installation-directory/tmp
   When restoring the database, the archived database files are extracted to this directory.
2. Stop Compute Systems Manager.
3. To restore the database, use the following command:
   In Windows:
   HCS-Common-Component-installation-folder\bin\hcmds64dbrepair /trans *exported-database-archive-files-folder*
   In Linux:

HCS-Common-Component-installation-directory/bin/hcmds64dbrepair -trans *exported-database-archive-files-directory*

You must use the absolute path to the location of the database archive files.

4. Start Compute Systems Manager.
5. Change the Compute Systems Manager System account password.
   This step is required because the `hcmds64dbrepair` command resets the System account back to the default password.

Related concepts

- Troubleshooting overview on page 254

Related tasks

- Starting Hitachi Compute Systems Manager on page 174
- Stopping Hitachi Compute Systems Manager on page 175
- Changing the System account password on page 54

Related references

- Prerequisites for restoring the database on page 182

Troubleshooting example: database corruption in a Windows cluster environment

If you cannot restore a database using the `hcmds64db` or `hcmds64dbtrans` command in a Windows cluster environment, Hitachi Compute Systems Manager generates an error message. The following example describes how to use `hcmds64dbrepair` command to restore a database that was exported with the `hcmds64dbtrans` command. You complete all database management tasks on the active node.

Possible cause

The database in a Windows cluster environment might be corrupted.

Countermeasure

1. Verify that the available capacity in the following directory is greater than the size of the database:
   HCS-Common-Component-installation-folder\tmp
   When restoring the database, the archived database files are extracted to this directory.
2. Temporarily stop Compute Systems Manager within the cluster by using the following command:
   HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvstate /soff /r *HCS-Cluster-group-name*

3. To restore the database, use the following command on the Compute Systems Manager active node:
   HCS-Common-Component-installation-folder\bin\hcmds64dbrepair /trans *exported-database-archive-file*
   You must use the absolute path to the location of the database archive files.
4. Restart Compute Systems Manager within the cluster by using the following command:
   HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvstate /son /r *HCS-Cluster-group-name*
5. Using the Compute Systems Manager interface, check the status of the Compute Systems Manager tasks. If a task is incomplete or has failed, recreate the task or update the task schedule as needed.
6. If Hitachi Device Manager is accessing Hitachi Tuning Manager using a remote connection, the settings are reset when you restore the database. This means you must set up the connection again.
7. Change the Compute Systems Manager System account password.
   This step is required because the hcmds64dbrepair command resets the System account back to the default password.

Related concepts

- Troubleshooting overview on page 254

Related tasks

- Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Windows) on page 232

Related references

- Prerequisites for restoring the database on page 182

Troubleshooting example: database corruption in a Linux cluster environment

If you cannot restore a database using the hcmds64db or hcmds64dbtrans command in a Linux cluster environment, Hitachi Compute Systems Manager generates an error message. The following example describes how to use hcmds64dbrepair command to restore a database that was exported with the hcmds64dbtrans command. You complete all database management tasks on the active node.

Possible cause

The database in a Linux cluster environment might be corrupted.

Countermeasure

1. Verify that the available capacity in the following directory is greater than the size of the database:

HCS-Common-Component-installation-directory/tmp

When restoring the database, the archived database files are extracted to this directory.

2. Delete the Hitachi Command Suite product services registered in the cluster management software group, including the Compute Systems Manager services.
3. Verify that the cluster management software group was moved to the active node. If the group was moved to the standby node, move it to the active node.
4. To restore the database, use the following command:
   HCS-Common-Component-installation-directory/bin/hcmds64dbrepair -trans *exported-database-archive-file*
5. Stop the Hitachi Command Suite products by using the following command:
   HCS-Common-Component-installation-directory/bin/hcmds64srv -stop
6. Re-register the services that were deleted from the cluster management software group.
7. In the cluster management software, select the active note to start the services in the cluster environment.
8. Using the Compute Systems Manager interface, check the status of the Compute Systems Manager tasks. If a task is incomplete or has failed, recreate the task or update the task schedule as needed.
9. If Hitachi Device Manager is accessing Hitachi Tuning Manager using a remote connection, the settings are reset when you restore the database. This means you must set up the connection again.
10. Change the Compute Systems Manager System account password.
    This step is required because the hcmds64dbrepair command resets the System account back to the default password.

Related concepts

- Troubleshooting overview on page 254

Related tasks

- Registering services to a cluster environment (Linux) on page 226
- Deleting services from the cluster management software (Linux) on page 229
- Starting Hitachi Compute Systems Manager in a cluster environment (Linux) on page 234
- Starting Hitachi Compute Systems Manager on page 174

Related references

- Prerequisites for restoring the database on page 182

Collecting maintenance information

This module provides information about collecting maintenance information for troubleshooting Hitachi Compute Systems Manager issues.

About collecting maintenance information

If your Hitachi Compute Systems Manager system is experiencing a failure and you cannot identify the cause or recover from the failure, contact the Hitachi Data Systems support center after collecting the following information:

- System status after the failure
- Date and time when the failure occurred
- Situation where the failure occurred
- Network configuration of the management server and the managed resource
- Operating system for the management server and the managed host
- Maintenance information for the computers (the management server and the managed resource) where the failure occurred

  You can obtain the following maintenance information from a management server:
  - Log files
  - Database files
  - Java VM thread dumps

    The information provided in Java VM thread dumps can help you to identify the cause of the following issues:

    - The Compute Systems Manager login window is not displayed even though the GUI is running.

    - The Compute Systems Manager main window is not displayed after you log in to Compute Systems Manager.

  You can obtain the following maintenance information from a managed resource:
  - Managed hosts
    - System information
    - From Windows hosts: Event log information (application logs and system logs)
    - From Linux or Solaris hosts: System log information
  - Managed hypervisors
    - From Hyper-V: the execution results of the `net start` command
    - From VMware ESX/ESXi: System log information
  - Managed chassis, servers, and LPARs
    - Alert notifications
    - Lamp information

- Error and configuration information for a chassis (when a managed blade server is mounted)
- Error and configuration information for LPAR Manager (when a managed LPAR exists)

For additional information about obtaining maintenance information, see the associated hardware manual for the managed chassis and server.

Related concepts

- Troubleshooting overview on page 254

Related tasks

- Collecting management server maintenance information on page 260
- Collecting maintenance information for a managed host on Windows on page 265
- Collecting maintenance information for a managed host on Linux or Solaris on page 266
- Collecting Java VM thread information on Windows on page 262

Collecting management server maintenance information

To collect management server maintenance information, use the following command:

In Windows:

```
HCS-Common-Component-installation-folder\bin\hcmds64getlogs /dir
directory-name [/types Hitachi-Command-Suite-product-name
[Hitachi-Command-Suite-product-name...]] [/arc archive-file-name]
[/logtypes log-file-type [log-file-type...]]
```

In Linux:

```
HCS-Common-Component-installation-directory/bin/hcmds64getlogs -
dirdirectory-name [-types Hitachi-Command-Suite-product-name
[Hitachi-Command-Suite-product-name...]] [-arc archive-file-name]
[-logtypes log-file-type [log-file-type...]]
```

For example, if you store maintenance resources in `c:\logs` (Windows) or `/var/tmp/logs` (Linux), you would use the following command:

In Windows:

```
HCS-Common-Component-installation-folder\bin\hcmds64getlogs /dir
c:\logs
```

In Linux:

```
HCS-Common-Component-installation-directory/bin/hcmds64getlogs -
dir /var/tmp/logs
```

Using one of these commands, you would obtain maintenance information for all Hitachi Command Suite products.

To collect maintenance information for Compute Systems Manager only, use the `hcmds64getlogs` command as follows:

In Windows:

```
HCS-Common-Component-installation-folder\bin\hcmds64getlogs /dir
c:\logs /types HCSM
```

In Linux:

```
HCS-Common-Component-installation-directory/bin/hcmds64getlogs -
dir /var/tmp/logs -types HCSM
```

The `hcmds64getlogs` command parameters are listed in the following table:

Parameter	Description
dir	Specifies the name of the directory on a local disk that stores maintenance information. If the directory already exists, empty it. • The maximum path name length is 41 characters. For details about the maximum path name length for applications other than Compute Systems Manager, see the manual for the applicable product. • All printable ASCII character are allowed, except the following special characters:\ / : , ; * ? " < > | $ % & ' • You can use backslashes (\), colons (:), and slashes (/) as path delimiters, but do not specify a path delimiter at the end of a path name. • In Windows, to specify a space character in a path name, enclose the path name in double quotation marks ("). In Linux, you cannot use spaces in a path name.
types	Specify the type of maintenance information that you want to obtain. • To obtain maintenance information for specific Hitachi Command Suite products only (for a reason such as a failure), specify the name of the products from which you want to obtain maintenance information. For details about the other Hitachi Command Suite product names, see the documentation for each product. To specify multiple product names, separate them by a space. • To obtain maintenance information for Compute Systems Manager, specify HCSM. • To specify multiple product names, separate them by a space. • If using the `types` option and the `logtypes` option together, you must specify "log" in the `logtypes` parameter. • If you omit the types option, maintenance information for all Hitachi Command Suite products installed on the management server is obtained. If a product that uses the 32-bit version of Hitachi Command Suite Common Component (Hitachi File Services Manager or Hitachi Storage Navigator Modular 2) is installed on the management server, the maintenance information of that product is also obtained.
arc	Specify the name of the archive files to create. • If you do not specify this parameter, the default file name is `HiCommand_log_64`. • The archive files are output under the directory specified in the `dir` option. • If the archive files are generated, each file has an extension corresponding to the type of each archive file (.jar, .hdb.jar, .db.jar, or .csv.jar).

Parameter	Description
	• For the file name, you can specify any printable ASCII character except the following special characters:\ / : , ; * ? " < > | $ % & ' ` In Linux, you cannot use spaces in a file name.
logtypes	Specify the type of log to create if you want to obtain only specific log files for a reason such as a failure. • Select one of the following log types:log—obtains .jar files and .hdb.jar files only.db—obtains .db.jar files only.csv—obtains .csv.jar files only. • To specify multiple types, separate them with a space. • If you omit this option, all log files are obtained.

The `hcmds64getlogs` command generates the following return values:

- 0: Normal termination
- 1: Parameter error
- 2: Abnormal termination

When using this command to collect maintenance information, use the following guidelines:

- Do not run multiple commands concurrently.
- When the command terminates, if the KAPM05318-I or KAPM05319-E message does not display, it means that the command terminated due to lack of space in the directory specified in the `dir` option. Ensure that the directory you specify has enough unused space, and then run the command again.

After running this command, the management server maintenance information is collected and sent to log files, database files, and four archive files (.jar, .hdb.jar, .db.jar, and .csv.jar).

Related concepts

- About collecting maintenance information on page 259

Collecting Java VM thread information on Windows

If the management server is running on Windows and you encounter issues with displaying the user interface login or main window, you must collect Java™ VM maintenance information.

You can collect Java VM thread information for the following services:

- HBase 64 Storage Mgmt SSO Service
- HCS Compute Systems Manager Web Service

Procedure

1. Create a file named `dump` in each of the following directories:
   - *HCS-Common-Component-installation-folder*`\uCPSB\CC\web\containers\HBase64StgMgmtSSOService`

- *HCS-Common-Component-installation-folder*\uCPSB\CC\web\containers\ComputeSystemsManagerWebService

2. Access the Windows **Services** dialog box.
3. Stop and restart the following services:
   - **HBase 64 Storage Mgmt SSO Service**
   - **HCS Compute Systems Manager Web Service**

   The system generates the Java VM thread dumps in the following locations. The file names of the Java VM thread dumps differ depending on the JDK running on the system.

   When using the default JDK provided with Compute Systems Manager:
   - *HCS-Common-Component-installation-folder*\uCPSB\CC\web\containers\HBase64StgMgmtSSOService\javacore*xxx.xxxx*.txt
   - *HCS-Common-Component-installation-folder*\uCPSB\CC\web\containers\ComputeSystemsManagerWebService\javacore*xxx.xxxx*.txt

   When using the Oracle JDK:
   - *HCS-Common-Component-installation-folder*\uCPSB\CC\web\containers\HBase64StgMgmtSSOService\HBase64StgMgmtSSOService.log
   - *HCS-Common-Component-installation-folder*\uCPSB\CC\web\containers\ComputeSystemsManagerWebService\ComputeSystemsManagerWebService.log

   Note: If you use the Oracle JDK, the Java VM thread dump is overwritten each time the dump is generated. Therefore, after the system generates the Java VM thread dump, save it using a different name.

Result

After completing this procedure, you have Java VM maintenance information.

Related concepts

- About collecting maintenance information on page 259

Related tasks

- Collecting Java VM thread information on Linux on page 263

Collecting Java VM thread information on Linux

If the management server is running on Linux and you encounter issues with displaying the user interface login or main window, you must collect Java™ VM maintenance information.

You can collect Java VM thread information for the following services:

- HBase 64 Storage Mgmt SSO Service
- HCS Compute Systems Manager Web Service

Procedure

1. Run the following command to stop the HBase 64 Storage Mgmt SSO Service.

   ```
   kill -3 PID
   ```

   where *PID* indicates the process ID listed at the bottom of the following file:

   HCS-Common-Component-installation-directory/uCPSB/CC/web/containers/HBase64StgMgmtSSOService/logs/cjstdout.log

2. Run the following command to stop the HCS Compute Systems Manager Web Service.

   ```
   kill -3 PID
   ```

   where *PID* indicates the process ID listed at the bottom of the following file:

   HCS-Common-Component-installation-directory/uCPSB/CC/web/containers/ComputeSystemsManagerWebService/logs/cjstdout.log

3. Restart Compute Systems Manager.

   The system generates the Java VM thread dumps in the following locations. The file names of the Java VM thread dumps differ depending on the JDK running on the system.

   When using the default JDK provided with Compute Systems Manager:

   - *HCS-Common-Component-installation-folder*/uCPSB/CC/web/containers/HBase64StgMgmtSSOService/javacore*xxx*.*xxxx*.txt
   - *HCS-Common-Component-installation-folder*/uCPSB/CC/web/containers/ComputeSystemsManagerWebService/javacore*xxx*.*xxxx*.txt

   When using the Oracle JDK:

   - *HCS-Common-Component-installation-folder*/uCPSB/CC/web/containers/HBase64StgMgmtSSOService/HBase64StgMgmtSSOService.log
   - *HCS-Common-Component-installation-folder*/uCPSB/CC/web/containers/ComputeSystemsManagerWebService/ComputeSystemsManagerWebService.log

Note: If you use the Oracle JDK, the Java VM thread dump is overwritten each time the dump is generated. Therefore, after the system generates the Java VM thread dump, save it using a different name.

Result

After completing this procedure, you have Java VM maintenance information.

Related concepts

- About collecting maintenance information on page 259

Related tasks

- Collecting Java VM thread information on Windows on page 262

Collecting maintenance information for a managed host on Windows

You can collect maintenance information for a managed host running Windows.

Procedure

1. Collect event log information. Collecting event log information consists of saving a total of four files:
   - Application event information in text or csv format
   - Application event information in event log or event file format
   - System event information in text or csv format
   - System event information in event log or event file format

   a. Open the **Event Viewer** by selecting **Start > Administrative Tools > Event Viewer**.
   b. For Windows Server 2008 and 2012, in the left pane, expand the tree view and select **Windows Logs**.
   c. Right-click **Applications**, and select **Save log file as**.
   d. In the **Save "Application" As** dialog, enter a file name, select a file type (either **text** or **CSV**), and click **Save**.
   e. Collect the log file in a different format by right-clicking **Applications** again, selecting **Save event as** or **Save all event as**, entering a file name, and selecting a file type of **event log** or **event file**.
   f. If the **Display information** dialog box opens, leave the default settings, and click **OK**.
   g. Repeat steps c-f, but instead of selecting **Applications**, right-click **System**.

   You now have four saved event log files.
2. Collect system information.

a. Run the `msinfo32` command.
b. In the left pane, select **System Summary**.
c. From the **File** menu, select **Export**, and then save the system information as a text file.

Result

After completing this procedure, you have all the maintenance information for the Windows managed host.

Related concepts

- About collecting maintenance information on page 259

Collecting maintenance information for a managed host on Linux or Solaris

You can collect maintenance information for a managed host running Linux or Solaris.

Procedure

1. Collect system log information as follows:
   a. Make a copy of the `/etc/syslog.conf` or `/etc/rsyslog.conf` file.
   b. For Linux hosts, run the `ls -l /var/log/messages*` command and pipe the results to a file. Then make a copy of the `/var/log/messages*` file.
   c. For Solaris hosts, run the `ls -l /var/adm/messages*` command and pipe the results to a file. Then make a copy of the `/var/adm/messages*` file.
2. Collect system information as follows:
   a. Make a copy of the `/etc/services` file and `/etc/hosts` file.
   b. Run the following commands and save the results to a file:

      ```
      uname -a
      ps -elf
      ```

   c. For Linux hosts only, run the `rpm -qa` command and pipe the results to a file.
   d. For Linux hosts only, make a copy of the release-specific file:

      For Red Hat Linux, make a copy of the `/etc/redhat-release` file.

      For SUSE Linux, make a copy of the `/etc/SuSE-release` file.

      For Oracle Linux, make a copy of the `/etc/oracle-release` or `/etc/enterprise-release`.
   e. For Solaris hosts only, run the `pkginfo` command and pipe the results to a file. For Solaris 11, also run the `pkg info` command and pipe the results to a file.

Result

After completing this procedure, you have all the maintenance information for the Linux or Solaris managed host.

Related concepts

- About collecting maintenance information on page 259

Reviewing audit log information

This module provides information about reviewing audit log information.

About audit logs

When using Hitachi Compute Systems Manager, you can use audit logs to record user operations so that you retain proof of compliance for auditors and evaluators who must verify your adherence to regulations, security evaluation standards, and other business standards. To set up Compute Systems Manager to generate audit log data, you must edit the environment settings maintained in the audit properties file (`auditlog.conf`).

Related tasks

- Setting up audit logs on page 267
- Viewing the audit logs on page 268

Related references

- Audit log categories and event descriptions on page 269
- Audit log message format and information on page 278
- Audit event messages for tasks on page 280
- Audit event messages for processing requests on page 281
- Audit log detailed messages for system requests on page 281

Setting up audit logs

When using Hitachi Compute Systems Manager, you can record user operations in audit logs. You configure audit log settings in the `auditlog.conf` file.

Procedure

1. Stop Compute Systems Manager.
2. Configure the audit log settings as described in the Properties appendix by accessing the following file:
   - In Windows:
     HCS-Common-Component-installation-folder`\conf\sec\auditlog.conf`
   - In Linux:

HCS-Common-Component-installation-directory/conf/sec/auditlog.conf

Compute Systems Manager might generate a large volume of audit log data. You can change the log file size and back up or archive the generated log files based on the volume for your environment.

3. Start Compute Systems Manager.

Result

Compute Systems Manager now generates user operation data and stores it in the audit logs.

Related concepts

- About audit logs on page 267

Related tasks

- Viewing the audit logs on page 268

Related references

- Properties related to audit logs (auditlog.conf) on page 319

Viewing the audit logs

When using Hitachi Compute Systems Manager, you can record user operations in audit logs. To view the data, you must access the audit log.

Audit log data is output as event logs and is accessed as follows:

- For Windows operating systems:
  Select Event Viewer > Windows Logs > Application > Event Properties > General.
  The Event Properties window opens and displays a description of the event. Event messages use the following format:
  program-name[*process-id*]: *message-portion*

- For Linux operating systems:
  Locate and open the system `syslog` file. Within the `syslog` file, the messages are listed using the following format:
  syslog-header-portion message-portion
  The format of the *syslog-header-portion* differs depending on the operating system environment.
  For example, when using `rsyslog`, if you specify `$ActionFileDefaultTemplate=RSYSLOG_SyslogProtocol23Format` in `/etc/rsyslog.conf`, data is output in a format that supports RFC 5424.

Related concepts

- About audit logs on page 267

Related tasks

- Setting up audit logs on page 267

Related references

- Audit log categories and event descriptions on page 269
- Audit log message format and information on page 278
- Properties related to audit logs (auditlog.conf) on page 319

Audit log categories and event descriptions

Audit logs are divided into the categories and each audit event within a category is assigned a severity level and message ID. You can configure which audit log data is recorded in the audit logs according to the severity level of the events.

Audit logs are divided into the following categories:

- StartStop
- Authentication
- ExternalService
- ConfigurationAccess

Within each audit log category, there are associated audit events. Each audit event includes a severity level and a message ID. The following table includes detailed information for the audit log categories and the associated audit events.

Audit log category and description	Type description	Audit event	Severity	Message ID
StartStop Events indicating the starting or stopping of hardware or software such as the following: • Starting or shutting down an OS • Starting or stopping a hardware component • Starting or stopping Hitachi Command Suite products	Starting and stopping software	Successful SSO server start	6	KAPM00090-I
		Failed SSO server start	3	KAPM00091-E
		SSO server stop	6	KAPM00092-I
Authentication Events indicating that a user succeeded or failed in a connection or authentication such as the following: • User authentication • Automatic account locking	User authentication	Successful login	6	KAPM01124-I
		Successful login (to the external authentication server)	6	KAPM02450-I
		Failed login (wrong user ID or password)	4	KAPM02291-W

Audit log category and description	Type description	Audit event	Severity	Message ID
		Failed login (logged in as a locked user)	4	KAPM02291-W
		Failed login (logged in as a non-existing user)	4	KAPM02291-W
		Failed login (no permission)	4	KAPM01095-E
		Failed login (authentication failure)	4	KAPM01125-E
		Failed login (to the external authentication server)	4	KAPM02451-W
		Successful logout	6	KAPM08009-I
		Failed logout	4	KAPM01126-W
	Automatic account lock	Automatic account lock (repeated authentication failure or expiration of account)	4	KAPM02292-W
ExternalService Events indicating the results of communication with external services such as the following: • Communication with an external server, such as NTP or DNS • Communication with a management server (SNMP)	Communication with the external authentication server	Successful communication with the LDAP directory server	6	KAPM10116-I
		Failed communication with the LDAP directory server	3	KAPM10117-E
		Successful communication with the Kerberos server	6	KAPM10120-I
		Failed communication with the Kerberos server (no response)	3	KAPM10121-E
		Successful communication with the DNS server	6	KAPM10122-I
		Failed communication with the DNS server (no response)	3	KAPM10123-E

Audit log category and description	Type description	Audit event	Severity	Message ID
	Authentication with an external authentication server	Successful TLS negotiation with the LDAP directory server	6	KAPM10124-I
		Failed TLS negotiation with the LDAP directory server	3	KAPM10125-E
		Successful authentication of the user for an information search on the LDAP directory server	6	KAPM10126-I
		Failed authentication of the user for an information search on the LDAP directory server	3	KAPM10127-W
	User authentication on an external authentication server	Successful user authentication on the LDAP directory server	6	KAPM10128-I
		User not found on the LDAP directory server	4	KAPM10129-W
		Failed user authentication on the LDAP directory server	4	KAPM10130-W
		Successful user authentication on the Kerberos server	6	KAPM10133-I
		Failed user authentication on the Kerberos server	4	KAPM10134-W
	Acquisition of information from an external authentication server	Successful acquisition of user information from the LDAP directory server	6	KAPM10135-I
		Failed acquisition of user information from the LDAP directory server	3	KAPM10136-E

Audit log category and description	Type description	Audit event	Severity	Message ID
		Successful acquisition of the SRV record from the DNS server	6	KAPM10137-I
		Failed acquisition of the SRV record from the DNS server	3	KAPM10138-E
ConfigurationAccess Events indicating that the administrator succeeded or failed in performing an operation such as the following: • Reference or update of configuration information • Update of account settings including addition or deletion of accounts • Security configuration • Reference or update of audit log settings	User registration (using a management client	Successful user registration	6	KAPM07230-I
		Failed user registration	3	KAPM07240-E
	User deletion (using a management client	Successful single user deletion	6	KAPM07231-I
		Failed single user deletion	3	KAPM07240-E
		Successful multiple user deletion	6	KAPM07231-I
		Failed multiple user deletion	3	KAPM07240-E
	Password change (using the Users and Permissions window)	Successful password change by the administrator	6	KAPM07232-I
		Failed password change by the administrator	3	KAPM07240-E
	Password change (using the User Profile window)	Failed authentication processing for verifying old password	3	KAPM07239-E
		Successful change of login user's own password	6	KAPM07232-I
		Failed change of login user's own password	3	KAPM07240-E
	Profile change	Successful profile change	6	KAPM07233-I
		Failed profile change	3	KAPM07240-E
	Permission change	Successful permission change	6	KAPM02280-I
		Failed permission change	3	KAPM07240-E

Audit log category and description	Type description	Audit event	Severity	Message ID
	Account lock Note: If an account is locked because the authentication method changed for a user without a password, the event is not recorded in the audit log.	Successful account lock	6	KAPM07235-I
		Failed account lock	3	KAPM07240-E
	Account lock release Note: If an account is unlocked because a password was set for a user, the event is not recorded in the audit log.	Successful account lock release	6	KAPM07236-I
		Failed account lock release	3	KAPM07240-E
		Successful account lock release using the `hcmds64unlockaccount` command	6	KAPM07236-I
		Failed account lock release using the `hcmds64unlockaccount` command	3	KAPM07240-E
	Authorization method change	Successful authentication method change	6	KAPM02452-I
		Failed authentication method change	3	KAPM02453-E
	Authorization group addition (using a management client)	Successful addition of an authorization group	6	KAPM07247-I
		Failed addition of an authorization group	3	KAPM07248-E
	Authorization group deletion (using a management client)	Successful deletion of one authorization group	6	KAPM07249-I
		Failed deletion of one authorization group	6	KAPM07248-E
		Successful deletion of	6	KAPM07249-I

Audit log category and description	Type description	Audit event	Severity	Message ID
		multiple authorization groups		
		Failed deletion of multiple authorization groups	3	KAPM07248-E
	Authorization group permission change (using a management client)	Successful change of an authorization group's permission	6	KAPM07250-I
		Failed change of an authorization group's permission	3	KAPM07248-E
	User registration (processed on the management server)	Successful registration of user	6	KAPM07241-I
		Failed registration of user	3	KAPM07242-E
	User information update (processed on the management server)	Successful update of user information	6	KAPM07243-I
		Failed update of user information	3	KAPM07244-E
	User deletion (processed on the management server)	Successful deletion of user	6	KAPM07245-I
		Failed deletion of user	3	KAPM07246-E
	Authorization group registration (processed on the management server)	Successful registration of an authorization group	6	KAPM07251-I
		Failed registration of an authorization group	3	KAPM07252-E
	Authorization group deletion (processed on the management server)	Successful deletion of an authorization group	6	KAPM07253-I
		Failed deletion of an authorization group	3	KAPM07254-E
	Authorization group permission	Successful change of an authorization	6	KAPM07255-I

Audit log category and description	Type description	Audit event	Severity	Message ID
	change (processed on the management server)	group's permission		
		Failed change of an authorization group's permission	3	KAPM07256-E
	Database backup or restore	Successful backup using the `hcmds64backups` or `hcmds64db` command	6	KAPM05561-I
		Failed backup using the `hcmds64backups` or `hcmds64db` command	3	KAPM05562-E
		Successful full restore using the `hcmds64db` command	6	KAPM05563-I
		Failed full restore using the `hcmds64db` command	3	KAPM05564-E
		Successful partial restore using the `hcmds64db` command	6	KAPM05565-I
		Failed partial restore using the `hcmds64db` command	3	KAPM05566-E
	Database export or import	Successful database export	6	KAPM06543-I
		Failed database export	3	KAPM06544-E
		Successful database import	6	KAPM06545-I
		Failed database import	3	KAPM06546-E
	Database area creation or deletion	Successful database area creation	6	KAPM06348-I
		Failed database area creation	3	KAPM06349-E
		Successful database area deletion	6	KAPM06350-I

Audit log category and description	Type description	Audit event	Severity	Message ID
		Failed database area deletion	3	KAPM06351-E
	Authentication data input/ output	Successful data output using the `hcmds64authmove` command	6	KAPM05832-I
		Failed data output using the `hcmds64authmove` command	3	KAPM05833-E
		Successful data input using the `hcmds64authmove` command	6	KAPM05834-I
		Failed data input using the `hcmds64authmove` command	3	KAPM05835-E
	Resource group creation	Successful resource group creation	6	KAPM07257-I
		Failed resource group creation	3	KAPM07258-E
	Resource group deletion	Successful resource group deletion	6	KAPM07259-I
		Failed resource group deletion	3	KAPM07260-E
	Editing resource group properties	Successful resource group property editing	6	KAPM07261-I
		Failed resource group property editing	3	KAPM07262-E
	User group registration	Successful user group registration	6	KAPM07263-I
		Failed user group registration	3	KAPM07264-E
	User group deletion	Successful user group deletion	6	KAPM07265-I
		Failed user group deletion	3	KAPM07266-E
	User group update	Successful user group update	6	KAPM07267-I
		Failed user group update	3	KAPM07268-E

Audit log category and description	Type description	Audit event	Severity	Message ID
	Role registration	Successful registration of a role	6	KAPM07269-I
		Failed registration of a role	3	KAPM07270-E
	Role deletion	Successful deletion of a role	6	KAPM07271-I
		Failed deletion of a role	3	KAPM07272-E
	Role update	Successful update of a role	6	KAPM07273-I
		Failed update of a role	3	KAPM07274-E
	Assignment of a user account to a user group	Successful assignment of a user account to a user group	6	KAPM07275-I
		Failed assignment of a user account to a user group	3	KAPM07276-E
	Assignment of a permission to a role	Successful assignment of the permission to the role	6	KAPM07277-I
		Failed assignment of the permission to the role	3	KAPM07278-E
	Assignment of the following types of items: • User group and external authenticati on group • Resource • Role	Successful assignment of the following types of items: • User group and external authentication group • Resource group • Role	6	KAPM07279-I
		Failed assignment of the following types of items: • User group and external authentication group • Resource group • Role	3	KAPM07280-E
	Compute Systems	Request reception	6	KASV27000-I

Audit log category and description	Type description	Audit event	Severity	Message ID
	Manager Processing processing	Response transmission (normal)	6	KASV27002-I
		Response transmission (abnormal)	3	KASV27003-E
	Task operations	Successful task cancellation	6	KASV27004-I
		Failed task cancellation	4	KASV27005-W
		Successful task registration	6	KASV27006-I
		Failed task registration	4	KASV27007-W
		Successful task deletion	6	KASV27008-I
		Failed task deletion	4	KASV27009-W
		Successful task execution	6	KASV27010-I
		Failed task execution	4	KASV27011-W
		Successful task rescheduling	6	KASV27012-I
		Failed task rescheduling	4	KASV27013-W
		Successful move to History	6	KASV27014-I
		Failed move to History	4	KASV27015-W

Related concepts

- About audit logs on page 267

Related tasks

- Viewing the audit logs on page 268

Related references

- Audit log message format and information on page 278
- Audit log detailed messages for system requests on page 281

Audit log message format and information

When the system sends audit events to an audit log, the event includes a message.

The format for the log entries is as follows:

program-name [*process-ID*]: *message portion*

The format of the message portion is as follows:

uniform-identifier,unified-specification-revision-number,serial-number, message-ID,date-and-time,detected-entity,detected-location,audit-event-type,audit-event-result,audit-event-result-subject-identification-information,hardware-identification-information,location-information, location-identification-information,FQDN,redundancy-identification-information, agent-information,request-source-host,request-source-port-number,request-destination-host,request-destination-port-number,batch-operation-identifier,log-data-type-information,application-identification-information,reserved-area,message-text

In a `syslog` file, a message cannot exceed 953 characters.

Note: Not all items are output for each audit event.

The following table includes a description for each audit log message parameter.

Message output	Description
uniform-identifier	Fixed to CELFSS
unified-specification-revision-number	Fixed to 1.1
serial-number	Serial number of audit log messages
message-ID	Message ID
date-and-time	Date and time when the message was output
detected-entity	Component or process name
detected-location	Host name
audit-event-type	Event type
audit-event-result	Event result
audit-event-result-subject-identification-information	Account ID, process ID, or IP address corresponding to the event
hardware-identification-information	Hardware model or serial number
location-information	Identification information for the hardware component
location-identification-information	Location identification information.
FQDN	Fully qualified domain name
redundancy-identification-information	Fully qualified domain name

Message output	Description
agent-information	Agent information
request-source-host	Host name of the request sender
request-source-port-number	Port number of the request sender
request-destination-port-number	Port number of the request destination
request-destination-host	Host name of the request destination
batch-operation-identifier	Serial number of operations through the program
log-data-type-information	Fixed to BasicLog or DetailLog
application-identification-information	Program identification information
reserved-area	Not output - this is a reserved space.
message-text	Text describing the event

The following is an example of the message portion of an audit log login event:

```
CELFSS,1.1,0,KAPM01124-I,2014-07-22T14:08:23.1+09:00,HBase-
SSO,management-
host,Authentication,Success,uid=system,BasicLog,"The login was
successful.(session ID = session_id)"
```

Related tasks

- Viewing the audit logs on page 268

Related references

- Audit event messages for processing requests on page 281
- Audit log categories and event descriptions on page 269
- Audit log detailed messages for system requests on page 281

Audit event messages for tasks

The format of message text in the audit log data varies depending on the audit event. Each type of audit event includes a different set of variables. The following table includes a description of the variables that are used in the message text for Hitachi Compute Systems Manager task event messages.

Message text variables	Description
unique-key	A unique key value for a task. The key is output in the following format: uk=
task-name	The name of the task that completed the operation. The name is output in the following format:

Message text variables	Description
	taskname=

Related tasks

- Viewing the audit logs on page 268

Related references

- Audit log message format and information on page 278
- Audit log categories and event descriptions on page 269
- Audit log detailed messages for system requests on page 281

Audit event messages for processing requests

The format of message text in the audit log data varies depending on the audit event. Each type of audit event includes a different set of variables. The following table includes a description of the variables that are used in the message text for Hitachi Compute Systems Manager server processing requests.

Message text variables	Description
unique-ID	A unique request identifier. For response transmission, the unique ID of the request is output. For processing using the SVP, this ID is also output as audit log data on the SVP.
detailed-message	Detailed information about the request.
error-message-ID	The ID of the error message.

Related tasks

- Viewing the audit logs on page 268

Related references

- Audit log message format and information on page 278
- Audit log categories and event descriptions on page 269
- Audit log detailed messages for system requests on page 281

Audit log detailed messages for system requests

The output format of a detailed message related to a Hitachi Compute Systems Manager receive request is as follows:

command target [*parameter*]

The variable within the brackets ([ ]) might not appear.

Detailed Compute Systems Manager receive request messages contain the following variables:

- *command*—A character string (three characters) that indicates the operation (for example, addition, deletion, modification, or reference) to perform on the resource. The following table provides detailed command output information.

Output character string	Full name	Operation
Add	Add	Addition
Del	Delete	Deletion
Get	Get	Acquisition
Mod	Modify	Modification
Set	Set	Setting

- *target*—Information that identifies the operation to perform. The following table provides detailed target output information.

Output character string	Full name	Operation
Alerts	Alerts	Alert information reference or deletion
Chassis	Chassis	Chassis setting or reference
Server	Server	Server setting or reference
Host	Host	Host setting or reference
LGrp	LogicalGroup	Logical group setting or reference
SrvI	ServerInfo	Compute Systems Manager information acquisition
User	User	User setting or reference

- *parameter*—Information that identifies the operation to perform and the resource where the operation runs. (This information is output only when it is specified by request.)
  The parameter output details include the following variables:
  - *Element*—Element name output as a character string.
  - *Attribute* (format: info='...')—Element attribute values output as character strings or numeric values. If more than one value is output, the values are separated by a comma (,).
    If no corresponding attribute or value was specified, no attribute value is output.
    If an attribute value contains a single-quotation mark (') or comma (,), the quotation mark or comma is replaced with a question mark (?).

  The format and content of the parameter output in detail messages is presented as follows:
  <element attribute/>
  The following table provides detailed information about the sequence where attributes are output for each element.

Output character string	Full name and content	Sequence of attribute values output
Alert	Alert (information about the Compute Systems Manager error or a managed resource error)	alert number
Chassis	Chassis (chassis information about the error)	chassis name, chassis IP address
Server	Server (server information)	server name, server IP address
Host	Host (host information)	host name, host IP address
User	User (account information of a single Compute Systems Manager user)	user ID

Related tasks

- Viewing the audit logs on page 268

Related references

- Audit log message format and information on page 278
- Audit log categories and event descriptions on page 269
- Audit event messages for processing requests on page 281
- Audit event messages for tasks on page 280

Log file settings

This module provides information about configuring log file settings.

About log file settings

When using Hitachi Compute Systems Manager, you can change the log file settings when you require more detailed log data. Under standard system operation, there is no need for you to change the log file settings, but there are certain situations where additional data is useful. For example, in most cases you need more detailed data when investigating or reproducing failure conditions.

You can change the following settings for the Compute Systems Manager Message log files:

- Maximum size of the log file
- Maximum number of log files
- Logging level

Related tasks

- Changing Compute Systems Manager log file settings on page 284

Changing Compute Systems Manager log file settings

You can change the Hitachi Compute Systems Manager log file settings based on your log file requirements.

Procedure

1. Stop Compute Systems Manager.
2. Access the `logger.properties` file as follows:
   - In Windows:
     HCSM-Installation-folder`\ComputeSystemsManager\conf\logger.properties`
   - In Linux:
     HCSM-installation-directory`/ComputeSystemsManager/conf/logger.properties`
3. Edit the following log file settings:
   - `message.maxFileSizeInMB`
     Specify a size for the log file. If the specified file size is exceeded, messages are overwritten, beginning in sequence from the oldest.
   - `message.maxBackupIndex`
     Specify the maximum number of log files.
   - `message.logLevel`
     Specify the level of detail to send to the log files.
4. Save and close the properties file.
5. Start Compute Systems Manager.

Result

The new log file settings take effect when Compute Systems Manager starts.

Related concepts

- About log file settings on page 283

Related tasks

- Starting Hitachi Compute Systems Manager on page 174
- Stopping Hitachi Compute Systems Manager on page 175

Related references

- Properties related to Hitachi Compute Systems Manager server log files (logger.properties) on page 293

A

Ports

This appendix includes the port numbers associated with Hitachi Compute Systems Manager (HCSM) and Hitachi Command Suite (HCS) Common Component.

Hitachi Compute Systems Manager server ports

The Hitachi Compute Systems Manager server uses the ports listed in the following table:

Port number (default)	Description
162/UDP	These ports are used for SNMP trap reception. If 162/UDP is being used by another product, 22601/UDP is recommended.
22610/TCP	Used for communication with Hitachi Device Manager.
22611/TCP	Used for receiving alerts from a Hitachi server.

Related tasks

- Changing Hitachi Compute Systems Manager ports on page 74

Related references

- Hitachi Compute Systems Manager properties requiring updates for port number changes on page 73

Hitachi Command Suite Common Component ports

The Hitachi Command Suite Common Component uses the ports listed in the following table:

Port number (default)	Description
22015/TCP	This port is used for access to the Hitachi Command Suite Common Component service (HBase 64 Storage Mgmt Web Service) during non-SSL communication with management clients (web client and CLI). If this port number is used by a product other than Hitachi Command Suite products, change the port for either that product or for Hitachi Command Suite Common Component. To block non-SSL communication to the management server from external servers, you must edit the `user_httpsd.conf` file.
22016/TCP	This port is used for access to the Hitachi Command Suite Common Component service (HBase 64 Storage Mgmt Web Service) when SSL is used for communication with management clients (web client and CLI). If this port number is used by a product other than Hitachi Command Suite products, change the port for either that product or for Hitachi Command Suite Common Component.
22017/TCP to 22026/TCP	These ports are reserved.

Port number (default)	Description
22027/TCP	This port is used for internal communication with Hitachi Command Suite Common Component (to communicate with the Web server). If this port number is used by a product other than Hitachi Command Suite products, change the port for either that product or for Hitachi Command Suite Common Component.
22028/TCP	This port is used for internal communication with the Hitachi Command Suite Common Component (to receive termination messages from the Web server). If this port number is used by a product other than Hitachi Command Suite products, change the port for either that product or for Hitachi Command Suite Common Component.
22029/TCP to 22030/TCP	These ports are reserved.
22031/TCP	This port is used for internal communication with Hitachi Command Suite Common Component (communication with the HSSO-dedicated Web server). If this port number is used by a product other than Hitachi Command Suite products, change the port for either that product or for Hitachi Command Suite Common Component.
22032/TCP	This port is used for internal communication with Hitachi Command Suite Common Component (to communicate with the database). If this port number is used by a product other than Hitachi Command Suite products, change the port for either that product or for Hitachi Command Suite Common Component.
22033/TCP	This port is used for internal communication with Hitachi Command Suite Common Component (to communicate with the Web server). If this port number is used by a product other than Hitachi Command Suite products, change the port for either that product or for Hitachi Command Suite Common Component.
22034/TCP	This port is used for internal communication with Hitachi Command Suite Common Component (to receive termination messages from the Web server). If this port number is used by a product other than Hitachi Command Suite products, change the port for either that product or for Hitachi Command Suite Common Component.

Related tasks

- Changing Hitachi Compute Systems Manager ports on page 74

Related references

- Hitachi Compute Systems Manager server ports on page 286
- Hitachi Command Suite properties requiring updates for port number changes on page 71

Deployment Manager ports

Deployment Manager uses the ports listed in the following table:

Port number (default)	Description
67/UDP	Used for PXE booting of managed resources. This port number cannot be changed.
69/UDP	Used for PXE booting of managed resources. This port number cannot be changed.
80/TCP*	Used for internal communication with the IIS service process. This port number can be changed.
4011/UDP	Used for PXE booting of managed resources. This port number cannot be changed.
26500/TCP*	Used for internal communication between the IIS service process and Deployment Manager. This port number can be changed.
26501/TCP or 56020/TCP*	Used for restoration and backup of managed resource disks. The default is 26501/TCP. This port number can be changed. If an attempt to change this port number fails, the system uses the default (56020/TCP).
26502/TCP or 56022/TCP*	Used for PXE booting of managed resources. The default is 26502/TCP. This port number can be changed. If an attempt to change this port number fails, the system uses the default (56020/TCP).
26503/TCP or 56030/TCP*	Used for PXE booting of managed resources. The default is 26503/TCP. This port number can be changed. If an attempt to change this port number fails, the system uses the default (56030/TCP).
26504/TCP to 26507/TCP	These ports are reserved.
26508/TCP or 56023/TCP*	Used for performing deployment operations on managed resources. The default is 26508/TCP. This port number can be changed. If an attempt to change this port number fails, the system uses the default (56023/TCP).
56011/TCP 56024/TCP 56028/TCP 56060/TCP	These ports are reserved.

* If a product other than Deployment Manager is using this port number, you must change the Deployment Manager port number.

Related tasks

- Changing the Deployment Manager port number on page 171

Related references

- Properties related to Deployment Manager ports (port.ini) on page 321

B

Properties

This appendix includes the Hitachi Compute Systems Manager (HCSM) and Hitachi Command Suite (HCS) Common Component properties.

Properties for Hitachi Compute Systems Manager server

This module provides information about the Hitachi Compute Systems Manager server properties files.

About the Hitachi Compute Systems Manager server properties

The Hitachi Compute Systems Manager server properties define the settings for Compute Systems Manager ports and logs. When you change a property, the new setting takes affect when you restart Compute Systems Manager.

Related concepts

- About the Hitachi Command Suite Common Component properties on page 294

Related references

- Hitachi Compute Systems Manager server properties files on page 290
- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 291
- Properties related to Hitachi Compute Systems Manager server log files (logger.properties) on page 293

Hitachi Compute Systems Manager server properties files

Hitachi Compute Systems Manager settings for ports and logs are stored in the properties files listed in the following table:

File name	Location	Description
user.properties	In Windows: *HCSM-installation-directory*\ComputeSystemsManager\conf\user.properties In Linux: *HCSM-installation-directory*/ComputeSystemsManager/conf/user.properties	This file includes port-related and function-related properties used by the Compute Systems Manager server.
logger.properties	In Windows: *HCSM-installation-directory*\ComputeSystemsManager\conf\logger.properties In Linux: *HCSM-installation-directory*/	This file includes log output-related properties.

File name	Location	Description
	ComputeSystemsManager/conf/logger.properties	

Related concepts

- About the Hitachi Compute Systems Manager server properties on page 290

Related references

- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 291
- Properties related to Hitachi Compute Systems Manager server log files (logger.properties) on page 293

Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties)

You use the `user.properties` file to change the ports used by the Hitachi Compute Systems Manager server and to change the settings related to the Compute Systems Manager server functions, such as the command timeout period and temperature display.

The Compute Systems Manager `user.properties` file includes the port-related and function-related parameters listed in the following table:

Property	Description
snmp.trap.receive.port	Specifies the port for receiving SNMP traps. Value range: 1 to 65535 The default value is 162 or 22601.
server.rmi.port	Specifies the port for receiving RMI requests from Hitachi Device Manager. Value range: 1 to 65535 The default value is 22610.
server.process.timeout	Specifies the timeout period for processing commands. Value range: 0 to 100000 (seconds) The default value is 1800 (seconds) If you do not want a command to timeout until it finishes processing, specify 0.
svp.alert.receive.port	Specifies the port for receiving alerts from a Hitachi server. Value range: 1 to 65535 The default value is 22611.

Property	Description
hcsm.keystore.filename	Specifies the name of the keystore file used by Compute Systems Manager for SSL communication between the management server and a Hitachi server (including an LPAR Manager running on a blade server). Value: *character_string* The default value is hcsm_default.keystore.
powermonitoring.temperature.unit	Specifies the temperature measurement unit. Value: F or C (represents Fahrenheit and Celsius) The default value is F.
hcsm.shared.directory	Specifies the path of the Compute Systems Manager work directory. If you plan to use Compute Systems Manager in a cluster environment, specify the path of a directory on the shared disk. Value: *character_string* If the specified directory does not exist, the default path is used. The default is as follows: In Windows: *HCSM-installation-folder*\shared Because path names include backslashes, you must add an escape character before every backslash in a path name. In the properties file, the backslash (\) is a character that requires an escape sequence. In Linux: *HCSM-installation-directory*/shared
winrm.maxEnvelopeSize	Specifies the maximum envelope size (MaxEnvelopeSizekb) value if you specify a value other than the recommended value of 512 for MaxEnvelopeSizekb on managed servers and then enable WinRM. If you set different values on multiple managed hosts, specify the maximum value among these values. Value range: 512 to 4194304 The default value is 512.
hcsm.certification.verify	Specifies whether the management server checks the certificate sent from a Hitachi server when SSL communication is used between the management server and the Hitachi server (including an LPAR Manager running on a blade server). Enable: Checks the certificate. The communication is permitted if the certificate sent matches the certificate for the Hitachi server that is registered to the keystore of the management server. Disable: Does not check the certificate. The default value is Disable.

Property	Description
	If you specify Enable, you must register the certificate for the Hitachi server to the keystore of the management server.
`hvm.lpar.migration.allow.plaintext`	Specifies whether to enable unencrypted communication between the management server and an LPAR manager when you migrate LPARs. Enable: Enables unencrypted communication. Disable: Disables unencrypted communication. The default value is Enable.
`svp.bind.address`	Specify the IP address of the management server to register on a Hitachi server when SSL communication is used between the management server and the Hitachi server. The default value is blank. If you use the default value, the IP address based on the operating system specification of the management server is registered. In a cluster environment, the IP address of the active node and the standby node are registered.
`hcsm.display.storage.systems.list`	Specifies whether to display a list of storage systems on the Resources tab. Enable: Displays the list. Disable: Does not display the list. The default value is Disable.

Related concepts

- About the Hitachi Compute Systems Manager server properties on page 290

Related references

- Hitachi Compute Systems Manager server properties files on page 290

Properties related to Hitachi Compute Systems Manager server log files (logger.properties)

You can change the Hitachi Compute Systems Manager log file settings by editing the `logger.properties` file listed in the following table:

Property	Description
`message.maxFileSizeInMB`	Specifies the maximum size of a log file (in MB). Select a value from 1 to 2047. The default is 1.
`message.maxBackupIndex`	Specifies the maximum number of log files. Select a value from 1 to 16.

Property	Description
	The default is 10.
`message.logLevel`	Specifies the logging level. Select a value from -1 to 1000. The default is 20. To disable logging, select -1. Note: We recommend that you set the value to 30 for reproducing test failures.

Related concepts

- About the Hitachi Compute Systems Manager server properties on page 290

Related references

- Hitachi Compute Systems Manager server properties files on page 290

Properties for Hitachi Command Suite Common Component

This module provides information about the Hitachi Command Suite (HCS) Common Component properties files.

About the Hitachi Command Suite Common Component properties

The Hitachi Command Suite Common Component properties define the settings for Hitachi Command Suite Common Component functionality. When you change a property, the new setting takes affect when you restart Compute Systems Manager.

Note: Any changes made to Hitachi Command Suite Common Component properties files are applied to all Hitachi Command Suite products that run in the same environment.

Related concepts

- About the Hitachi Compute Systems Manager server properties on page 290

Related references

- Properties files for Hitachi Command Suite Common Component on page 294

Properties files for Hitachi Command Suite Common Component

The properties files for Hitachi Command Suite Common Component are listed in the following table:

File name	Location	Description
user_httpsd.conf	In Windows: *HCS-Common-Component-installation-directory*\uCPSB\httpsd\conf\user_httpsd.conf In Linux: *HCS-Common-Component-installation-directory*/uCPSB/httpsd/conf/user_httpsd.conf	Contains properties related to the Web server.
usrconf.properties (SSO)	In Windows: *HCS-Common-Component-installation-directory*\uCPSB\CC\web\containers\HBase64StgMgmtSSOService\usrconf\usrconf.properties In Linux: *HCS-Common-Component-installation-directory*/uCPSB/CC/web/containers/HBase64StgMgmtSSOService/usrconf/usrconf.properties	
usrconf.properties (HCSM)	In Windows: *HCS-Common-Component-installation-directory*\uCPSB\CC\web\containers\ComputeSystemsManagerWebService\usrconf\usrconf.properties In Linux: *HCS-Common-Component-installation-directory*/uCPSB/CC/web/containers/ComputeSystemsManagerWebService/usrconf/usrconf.properties	
workers.properties	In Windows: *HCS-Common-Component-installation-directory*\uCPSB\CC\web\redirector\workers.properties In Linux: *HCS-Common-Component-installation-directory*/uCPSB/CC/web/redirector/workers.properties	
user_hsso_httpsd.conf	In Windows: *HCS-Common-Component-installation-directory*\uCPSB\conf\user_hsso_httpsd.conf In Linux: *HCS-Common-Component-installation-directory*/uCPSB/conf/user_hsso_httpsd.conf	

File name	Location	Description
HiRDB.ini	In Windows: *HCS-Common-Component-installation-directory*\HDB\CONF\emb\HiRDB.ini In Linux: *HCS-Common-Component-installation-directory*/HDB/CONF/emb/HiRDB.ini	Contains properties related to the database.
pdsys	In Windows: *HCS-Common-Component-installation-directory*\HDB\CONF\pdsys In Linux: *HCS-Common-Component-installation-directory*/HDB/CONF/pdsys	
def_pdsys	In Windows: *HCS-Common-Component-installation-directory*\database\work\def_pdsys In Linux: *HCS-Common-Component-installation-directory*/database/work/def_pdsys	
pdutsys	In Windows: *HCS-Common-Component-installation-directory*\HDB\CONF\pdutsys In Linux: *HCS-Common-Component-installation-directory*/HDB/CONF/pdutsys	
def_pdutsys	In Windows: *HCS-Common-Component-installation-directory*\database\work\def_pdutsys In Linux: *HCS-Common-Component-installation-directory*/database/work/def_pdutsys	
user.conf	In Windows: *HCS-Common-Component-installation-directory*\conf\user.conf In Linux: *HCS-Common-Component-installation-directory*/conf/user.conf	Contains properties related to user accounts.
exauth.properties	In Windows: *HCS-Common-Component-installation-directory*\conf\exauth.properties	Contains properties related to communication with an external authentication server.

File name	Location	Description
	Sample file location: *HCS-Common-Component-installation-directory*\sample\conf\exauth.properties In Linux: *HCS-Common-Component-installation-directory*/conf/exauth.properties Sample file location: *HCS-Common-Component-installation-directory*/sample/conf/exauth.properties	
auditlog.conf	In Windows: *HCS-Common-Component-installation-directory*\conf\sec\auditlog.conf In Linux: *HCS-Common-Component-installation-directory*/conf/sec/auditlog.conf	Contains properties related to audit logs.
cluster.conf	In Windows: *HCS-Common-Component-installation-directory*\conf\cluster.conf In Linux: *HCS-Common-Component-installation-directory*/conf/cluster.conf	Contains properties related to clustering.

Related references

- Properties related to web server communication including SSL settings (user_httpsd.conf) on page 298
- Properties related to the web server for Hitachi Compute Systems Manager (usrconf.properties) on page 301
- Properties related to the web server (workers.properties) on page 302
- Properties related to the HSSO-dedicated web server (user_hsso_httpsd.conf) on page 303
- Properties related to the database (HiRDB.ini) on page 303
- Properties related to the database (pdsys) on page 304
- Properties related to the database (def_pdsys) on page 304
- Properties related to the database (pdutsys) on page 305
- Properties related to the database (def_pdutsys) on page 305
- Properties related to System account locking (user.conf) on page 306
- Properties related to LDAP directory server connections (exauth.properties) on page 306
- Example properties file for external LDAP directory server connections (exauth.properties) on page 310
- Example properties file for Kerberos server connections (exauth.properties) on page 317

- Properties related to audit logs (auditlog.conf) on page 319
- Properties related to clustering (cluster.conf) on page 321

Properties related to web server communication including SSL settings (user_httpsd.conf)

The `user_httpsd.conf` properties file for Common Component web server communication contains the parameters listed in the following table:

Property	Description
`ServerName` *host-name*	Specifies the host name or IP address of the Compute Systems Manager management server. By default, this is the host name set for the OS. You must update this parameter if the host name or IP address of the Compute Systems Manager server changes. If making a change, we recommend specifying a host name. To use SSL communication, specify the same host name as the one you specified when creating the certificate signing request. The host name is case sensitive.
`Listen` *port-number*	Specifies the port number for accessing the HBase 64 Storage Mgmt Web Service. The default value is 22015. If this value changes, the same port number must be specified for the `Listen [::]:` property and the `#Listen 127.0.0.1:` property.
`Listen [::]:` *port-number*	Specifies the port number for accessing the HBase 64 Storage Mgmt Web Service. The default value is 22015. If this value changes, the same port number must be specified for the `Listen` property and the `#Listen 127.0.0.1:` property.
`#Listen 127.0.0.1:` *port-number*	This is a parameter for SSL communication. Delete the hash mark (#) at the beginning of the line if you want to enable SSL communication and block non-SSL communication from external servers to the management server. Specifies the port number for accessing the HBase 64 Storage Mgmt Web Service. The default value is 22015. If this value changes, the same port number must be specified for the `Listen` property and the `Listen [::]:` property.
`#Listen` *port-number*	Parameter for SSL communication. To use SSL, delete the preceding hash mark (#). Specifies the port number for accessing HBase 64 Storage Mgmt Web Service using SSL.

Property	Description
	The default value is 22016. If this is changed, the same port number must be specified for the `#Listen [::]:` property.
`#Listen [::]: port-number`	Parameter for SSL communication. To use SSL, do not delete the preceding hash mark (#). Specifies the port number for accessing HBase 64 Storage Mgmt Web Service using SSL. The default value is 22016. The port number of the `#Listen` property must be specified.
`#<VirtualHost host-name:port-number>`	Parameter for SSL communication. To use SSL, delete the preceding hash mark (#). If a name is specified for the host name, change the name to "*". For port number, specify the port number for accessing HBase 64 Storage Mgmt Web Service using SSL. The default value is 22016.
`# ServerName host-name`	Parameter for SSL communication. To use SSL, delete the preceding hash mark (#). Specifies the host name of the Compute Systems Manager management server. By default, this is the host name set for the OS. You must update this parameter if the host name of the Compute Systems Manager server changes. Specify the same host name as the one you specified when creating the certificate signing request. The host name is case sensitive.
`# SSLEnable`	Parameter for SSL communication. To use SSL, delete the preceding hash mark (#).
`# SSLProtocol`	Parameter for SSL communication. To use SSL, delete the preceding hash mark (#).
`# SSLRequiredCiphers`	Parameter for SSL communication. To use SSL, delete the preceding hash mark (#).
`# SSLRequireSSL`	Parameter for SSL communication. To use SSL, delete the preceding hash mark (#).
`# SSLCertificateKeyFile`	Parameter for SSL communication. To use SSL, delete the preceding hash mark (#). In SSLCertificateFile, specify the full path name of the private key. Do not specify a symbolic link and junction for the path.
`# SSLCertificateFile`	Parameter for SSL communication. To use SSL, delete the preceding hash mark (#). In SSLCertificateFile, specify the absolute path of the certificate file received from the Certificate Authority (CA) or the self-signed certificate file.

Property	Description
	Do not specify a symbolic link and junction for the path.
`# SSLCACertificateFile`	Parameter for SSL communication. If you are using SSL communication, in most cases you do not have to delete the preceding hash mark (#). If you are using the chained server certificate issued from the certificate authority on your system, you must delete the preceding hash mark (#), and then specify the chained certificate file of the certificate authority using an absolute path. By using a text editor to link multiple certificates (in PEM format), multiple certificates can co-exist in a single file. However, you cannot specify a symbolic link and junction for the path.
`# </VirtualHost>`	Parameter for SSL communication. To use SSL, delete the preceding hash mark (#).
`#HWSLogSSLVerbose On`	Parameter for SSL communication. To use SSL, delete the preceding hash mark (#).

`<Location / ComputeSystemsManager>`	Parameter for restricting management client access. To restrict access, add this property to the last line of the `user_httpsd.conf` file using the following format:
	
	`<Location /ComputeSystemsManager>`
	
	`order allow,deny`
	
	`allow from` *`management-client`* `[`*`management-client`*`...]`
	
	`</Location>`
	
	For additional information about how to restrict clients using this property, see the following section.

You can control Compute Systems Manager management server access by only allowing access to specific management clients. You allow access using the `<Location /ComputeSystemsManager>` property. All management clients that are not allowed access are restricted from accessing the management server.

For example, the following entry allows management client access from all computers in the hitachi.com domain and restricts access to any clients outside of the domain:

```
<Location /ComputeSystemsManager>

order allow,deny

allow from hitachi.com

</Location>
```

When creating a management client entry, use the following syntax:

- Specify management clients using one of the following formats:
  - Domain name (for example: hitachi.datasystem.com)
  - Partial domain name (for example: hitachi)

    - Full IPv4 address (for example: 10.1.2.3 127.0.0.1)
    - Partial IPv4 address (for example: 10.1 - meaning 10.1.0.0/16)
    - IPv4 network/netmask (for example: 10.1.0.0/255.255.0.0)
    - IPv4 Network/c (when using CIDR notation, c is a decimal integer indicating the number of bits for identifying a network; for example: 10.1.0.0/16)
- To allow access for multiple management clients, choose either method:
    - Use a single command line for allowing access and delimit the list of hosts using spaces.
    - Use a separate line for each host.
- If you use the web client or CLI for Hitachi Command Suite products on the management server, you must also specify the local loopback address (127.0.0.1 or *localhost-name*).
- Ensure that all entries follow the specified format. If there are extra spaces or tabs, access fails.

Related tasks

- Restricting management server access from a management client on page 131
- Setting up SSL on the server for secure client communication on page 115

Related references

- Properties files for Hitachi Command Suite Common Component on page 294

Properties related to the web server for Hitachi Compute Systems Manager (usrconf.properties)

The `usrconf.properties` file includes parameters for Hitachi Compute Systems Manager web server communication.

Note: The `usrconf.properties` file exists for each Web container service.

The following table lists the Compute Systems Manager `usrconf.properties` file parameters:

Property	Description
`webserver.connector.ajp13.port`	Specifies the port number for accessing the Web server. The default value is 22027. If you change this value, you must update the port number so that the `worker.ComputeSystemsManagerWebService.port` property in the `workers.properties` file is the same.
`webserver.shutdown.port`	Specifies the port used for receiving termination messages from the Web server.

Property	Description
	The default value is 22028.

The following table lists the `usrconf.properties` file parameters related to the web container server for Common Component single sign-on:

Property	Description
`webserver.connector.ajp13.port`	Specifies the port number for accessing the Web server. The default value is 22033. If you change this value, you must update the port number so that the `worker.HBase64StgMgmtSSOService.port` property in the `workers.properties` file is the same.
`webserver.shutdown.port`	Specifies the port used for receiving termination messages from the Web server. The default value is 22034.

Related references

- Properties files for Hitachi Command Suite Common Component on page 294
- Properties related to the web server (workers.properties) on page 302

Properties related to the web server (workers.properties)

The `workers.properties` file for Common Component web server communication includes the parameters listed in the following table:

Property	Description
`worker.ComputeSystemsManagerWebService.port`	Specifies the port number for accessing the Web server. The default value is 22027. If you change this value, you must update the `webserver.connector.ajp13.port` property in the `usrconf.properties` file for Compute Systems Manager so that it is the same.
`worker.HBase64StgMgmtSSOService.port`	Specifies the port number for accessing the Web server. The default value is 22033. If you change this value, you must update the `webserver.connector.ajp13.port` property in the `usrconf.properties` file for Common Component single sign-on so that it is the same.

Related references

- Properties files for Hitachi Command Suite Common Component on page 294

- Properties related to the web server for Hitachi Compute Systems Manager (usrconf.properties) on page 301

Properties related to the HSSO-dedicated web server (user_hsso_httpsd.conf)

The `user_hsso_httpsd.conf` properties file for Common Component web server communication contains the parameters listed in the following table:

Property	Description
Listen	Specifies the port number for accessing the HBase 64 Storage Mgmt Web SSO Service. The default value is 22031.

Related references

- Properties files for Hitachi Command Suite Common Component on page 294

Properties related to the database (HiRDB.ini)

The Common Component `HiRDB.ini` properties file contains the database-related parameters listed in the following table:

Property	Description
`PDNAMEPORT`	Specifies the port number used for the database. The default value is 22032. If you change this value, you must update the port number in the `pd_name_port` property in the `pdsys` file and the `pd_name_port` property in the `def_pdsys` file.
`PDHOST`	Specifies the IP address. You usually do not change this value. Change this value if the host name or IP address of the Compute Systems Manager management server changes. If the old IP address is specified, change the value to the loopback address 127.0.0.1.

Related references

- Properties files for Hitachi Command Suite Common Component on page 294
- Properties related to the database (pdsys) on page 304
- Properties related to the database (def_pdsys) on page 304

Properties related to the database (pdsys)

The Common Component `pdsys` properties file contains the database-related parameters listed in the following table:

Property	Description
`pd_name_port`	Specifies the port number used for the database. The default value is 22032. If you change this value, you must update the port number in the `PDNAMEPORT` property in the `HiRDB.ini` file and the `pd_name_port` property in the `def_pdsys` file.
`pdunit -x`	Specifies the IP address. You usually do not change this value. Change this value if the host name or IP address of the Compute Systems Manager management server changes. If the old IP address is specified, change the value to the loopback address 127.0.0.1.

Related references

- Properties files for Hitachi Command Suite Common Component on page 294
- Properties related to the database (HiRDB.ini) on page 303
- Properties related to the database (def_pdsys) on page 304

Properties related to the database (def_pdsys)

The Common Component `def_pdsys` properties file contains the database-related parameters listed in the following table:

Table 1 def_pdsys properties file parameters

Property	Description
`pd_name_port`	Specifies the port number used for the database. The default value is 22032. If you change this value, you must update the port number in the `PDNAMEPORT` property in the `HiRDB.ini` file and the `pd_name_port property` in the `pdsys` file.
`pdunit -x`	Specifies the IP address. You usually do not change this value. Change this value if the host name or IP address of the Compute Systems Manager management server changes. If the old IP address is specified, change the value to the loopback address 127.0.0.1.

Related references

- Properties files for Hitachi Command Suite Common Component on page 294
- Properties related to the database (HiRDB.ini) on page 303
- Properties related to the database (pdsys) on page 304

Properties related to the database (pdutsys)

The Common Component `pdutdsys` properties file contains the database-related parameters listed in the following table:

Property	Description
`pd_hostname`	Specifies the IP address. You usually do not change this value. Change this value if the host name or IP address of the Compute Systems Manager management server changes. If the old IP address is specified, change the value to the loopback address 127.0.0.1.

Related references

- Properties files for Hitachi Command Suite Common Component on page 294
- Properties related to the database (HiRDB.ini) on page 303
- Properties related to the database (def_pdutsys) on page 305

Properties related to the database (def_pdutsys)

The Common Component `def_pdutsys` properties file contains the database-related parameters listed in the following table:

Property	Description
`pd_hostname`	Specifies the IP address. You usually do not change this value. Change this value if the host name or IP address of the Compute Systems Manager management server changes. If the old IP address is specified, change the value to the loopback address 127.0.0.1.

Related references

- Properties files for Hitachi Command Suite Common Component on page 294
- Properties related to the database (HiRDB.ini) on page 303
- Properties related to the database (pdutsys) on page 305

Properties related to System account locking (user.conf)

The Common Component `user.conf` file includes the user account parameters listed in the following table:

Property	Description
`account.lock.system`	Specifies whether account locking is enabled for the System account. True indicates that System account automatic and manual locking are enabled. False indicates that System account automatic and manual locking are disabled.

Related tasks

- Enabling System account locking on page 69

Related references

- Properties files for Hitachi Command Suite Common Component on page 294

Properties related to LDAP directory server connections (exauth.properties)

The `exauth.properties` file contains parameters for connecting to an external LDAP directory server for authentication.

You specify different parameters depending on whether you directly specify LDAP directory server information or use a DNS server to obtain the server information.

You can view a sample file in the following location:

In Windows:

HCS-Common-Component-installation-folder`\sample\conf\exauth.properties`

You can use the sample file as a starting point by copying the file to the following directory:

HCS-Common-Component-installation-folder`\conf\exauth.properties`

In Linux:

HCS-Common-Component-installation-directory`/sample/conf/exauth.properties`

You can use the sample file as a starting point by copying the file to the following directory:

HCS-Common-Component-installation-directory/conf/exauth.properties

Note: When specifying property values, do not type a space character at the beginning or end of the values. In addition, do not enclose property values in double quotation marks ("). If you do, Hitachi Compute Systems Manager ignores the value and uses the default.

The exauth.properties file parameters are listed in the following table:

Property	Description	Possible Values
auth.server.type	Specifies the type of external authentication server. Specify ldap (to connect to an external LDAP directory server).	ldap or internal Default value: internal (used when not connecting to an external server)
auth.server.name	Specifies the server identification name of the LDAP directory server. You can specify any name for this property to identify the LDAP directory server for which you are obtaining the port number and the connection protocol. ServerName is set as the initial value. You must specify at least one name. When specifying multiple LDAP directory server identification names, separate the names with commas (,). Do not register the same server identification name more than one time. Note: This property value is used in several of the other properties within this file and is listed as follows: auth.server.name-property-value	The name value cannot exceed 64 characters and must consist of the following characters only: 0 to 9 A to Z a to z ! # ( ) + - . = @ [ ] ^ _ { } ~ Default value: none
auth.group.mapping	Specifies whether to link to an external authorization server. Specify true to connect to an external authorization server. Specify false if you do not want to connect to an external authorization server.	true or false Default value: false (used when not connecting to an external authorization server)
auth.ocsp.enable	Specifies whether to verify the validity of an LDAP directory server electronic signature by using an OCSP responder or a CRL when StartTLS is used for secure communication. Specify true to validate the electronic signature certificate. Specify false if you do not want to validate the electronic signature certificate.	true or false Default value: false

Property	Description	Possible Values
auth.ocsp.responderURL	Specifies the URL of an OCSP responder if you want to use a responder other than the one specified in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If you omit this value, the OCSP responder specified in the AIA field is used.	URL of an OCSP responder Default value: none
auth.ldap.*auth.server.name-property-value*.protocol	Specifies the protocol for connecting to the LDAP directory server (required). When communicating in plain text format, specify ldap. When using StartTLS communication, specify tls. Before specifying tls, ensure that one of the following encryption methods is supported on the LDAP directory server: • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA	ldap or tls Default value: none
auth.ldap.*auth.server.name-property-value*.host	Specifies the host name or IP address of the LDAP server. If you specify host name, ensure that the host name can be resolved to an IP address. If you specify the IP address, you can use an IPv4 address. This attribute is required. Default value: none Note: When using StartTLS as the protocol for connecting to the LDAP directory server, specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.	host name or IP address Default: none
auth.ldap.*auth.server.name-property-value*.port	Specifies the port number of the LDAP directory server. Ensure that the port you specify is set as the listen port number on the LDAP directory server.	1 to 65535 Default value: 389
auth.ldap.*auth.server.name-property-value*.timeout	Specifies the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out.	0 to 120 (seconds) Default value: 15
auth.ldap.*auth.server.name-property-value*.attr	Specifies the attribute (Attribute Type) to use as the user ID during authentication. • Hierarchical structure model Specify the name of the attribute containing the unique value used for	Default value: sAMAccountName Modify this value for your configuration.

Property	Description	Possible Values
	identifying the user. The value stored in this attribute is used as the user ID for Hitachi Command Suite. (This value must not include characters that are invalid for Hitachi Command Suite user IDs.) For example, if you are using Active Directory and you want to use the Windows logon ID for a Hitachi Command Suite user, specify the attribute name sAMAccountName where the Windows logon ID is defined. • Flat model Specify the RDN attribute name of the user entry. This attribute is required.	
auth.ldap.*auth.server.name-property-value*.basedn	Specifies the BaseDN, which is the DN of the entry used as the start point when searching for LDAP user information on the LDAP directory server. The user entries located below this DN in the hierarchy are checked during authentication. If you must escape any of the characters in the BaseDN, ensure that you escape the characters correctly because the specified value is passed to the LDAP directory server without change. • Hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries required for searching. The specified attribute cannot include characters that are invalid in a Hitachi Command Suite user ID. • Flat model Specify the DN of the hierarchy just the user entries required for searching. When specifying the DN, follow the rules defined in RFC4514. For example, you must use a backslash (\) to escape each of the following characters: spaces # + ; , < = > \ This attribute is required.	Default value: none
auth.ldap.auth.server.name-property-value.retry.interval	Specifies the retry interval when an LDAP directory server connection attempt fails.	1 to 60 (seconds) Default value: 1
auth.ldap.auth.server.name-property-value.retry.times	Specifies the number of retries to attempt when an LDAP directory server connection fails. If you specify 0, no retries are attempted.	0 to 50 Default value: 20
auth.ldap.auth.server.name-property-value.domain.name	Specifies the name of the domain managed by the LDAP directory server. This property is required for the following configurations:	Default value: none

Property	Description	Possible Values
	• Using a DNS server to obtain LDAP directory server information. • Directly specifying LDAP directory server information and also linking to a remote authorization server.	
auth.ldap.*auth.server.name-property-value*.dns_lookup	Specifies DNS-related retries. If, however, the following values are also set in the properties file, the LDAP server connection is made using the these attribute values instead of using the DNS server information: • auth.ldap.*auth.server.name-property-value*.host • auth.ldap.*auth.server.name-property-value*.port	true or false Default value: false

Related concepts

- About setting up secure communication for an external authentication server on page 131

Related tasks

- Configuring an LDAP server connection on page 139

Related references

- Properties files for Hitachi Command Suite Common Component on page 294
- Example properties file for external LDAP directory server connections (exauth.properties) on page 310

Example properties file for external LDAP directory server connections (exauth.properties)

When using Hitachi Compute Systems Manager, you can use an external authentication server. To set up a connection with an external LDAP directory server for authentication, you edit the properties in the `exauth.properties` file on the Compute Systems Manager management server. The following examples include the parameter settings that you use to set up your LDAP directory server connection. Depending on the type of connection, some parameters might not apply to your environment.

The following example shows the parameters that you specify when directly entering information for the LDAP directory server when connecting to an external authentication server only:

```
auth.server.type=ldap

auth.server.name=ServerName
```

```
auth.group.mapping=false

auth.ocsp.enable=false

auth.ocsp.responderURL=

auth.ldap.ServerName.protocol=ldap

auth.ldap.ServerName.host=ldap.example.com

auth.ldap.ServerName.port=389

auth.ldap.ServerName.timeout=15

auth.ldap.ServerName.attr=sAMAccountName

auth.ldap.ServerName.basedn=dc=Example,dc=com

auth.ldap.ServerName.retry.interval=1

auth.ldap.ServerName.retry.times=20

auth.ldap.ServerName.dns_lookup=false
```

The following example shows the parameters that you specify when using a DNS server information to obtain information about the LDAP directory server when linking with an external authentication server only:

```
auth.server.type=ldap

auth.server.name=ServerName

auth.group.mapping=false

auth.ldap.ServerName.protocol=ldap

auth.ldap.ServerName.timeout=15

auth.ldap.ServerName.attr=sAMAccountName

auth.ldap.ServerName.basedn=dc=Example,dc=com

auth.ldap.ServerName.retry.interval=1

auth.ldap.ServerName.retry.times=20

auth.ldap.ServerName.domain.name=EXAMPLE.COM

auth.ldap.ServerName.dns_lookup=true
```

The following example shows the parameters when entering information about the LDAP directory server directly when also linking with an external authorization server:

```
auth.server.type=ldap

auth.server.name=ServerName
```

```
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=false
```

The following example shows the parameters that you specify when using a DNS server information to obtain information about the LDAP directory server when also linking with an external authorization server:

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

Related concepts

- About Hitachi Compute Systems Manager security settings on page 114
- About setting up secure communication for an external authentication server on page 131

Related tasks

- Configuring an LDAP server connection on page 139

Related references

- Properties related to LDAP directory server connections (exauth.properties) on page 306

Properties related to Kerberos server connections (exauth.properties)

The `exauth.properties` file contains parameters for connecting to an external Kerberos server for authentication.

You specify different parameters depending on whether you directly specify external authentication server information or use a DNS server to obtain the server information.

You can view a sample file in the following location:

In Windows:

HCS-Common-Component-installation-folder`\sample\conf\exauth.properties`

You can use the sample file as a starting point by copying the file to the following directory:

HCS-Common-Component-installation-folder`\conf\exauth.properties`

In Linux:

HCS-Common-Component-installation-directory`/sample/conf/exauth.properties`

You can use the sample file as a starting point by copying the file to the following directory:

HCS-Common-Component-installation-directory`/conf/exauth.properties`

Note: When specifying property values, do not type a space character at the beginning or end of the values. In addition, do not enclose property values in double quotation marks ("). If you do, Hitachi Compute Systems Manager ignores the value and uses the default.

The `exauth.properties` file parameters are listed in the following table:

Property	Description	Possible Values
`auth.server.type`	Specifies the type of external authentication server.	kerberos or internal

Property	Description	Possible Values
	Specify kerberos (to connect to an external Kerberos server).	Default value: internal (used when not connecting to an external server)
auth.group.mapping	Specifies whether to link to an external authorization server. Specify true to connect to an external authorization server. Specify false if you do not want to connect to an external authorization server.	true or false Default value: false (used when not connecting to an external authorization server)
auth.ocsp.enable	Specifies whether to verify the validity of an LDAP directory server electronic signature by using an OCSP responder or a CRL when StartTLS is used for secure communication. Specify true to validate the electronic signature certificate. Specify false if you do not want to validate the electronic signature certificate.	true or false Default value: false
auth.ocsp.responderURL	Specifies the URL of an OCSP responder if you want to use a responder other than the one specified in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If you omit this value, the OCSP responder specified in the AIA field is used.	URL of an OCSP responder Default value: none
auth.kerberos.default_realm	Specifies the default realm name. If you specify a user ID but not a realm name in the login window of the GUI, the user is authenticated as a user who belongs to the realm specified for this attribute. (required)	realm name Default value: none
auth.kerberos.dns_lookup_kdc	Specifies whether to look up the Kerberos server using DNS. This attribute is required. Specify true If all the following attributes values are already set, the Kerberos server will not be looked up by the DNS server. • realm_name • *value-specified-for-realm_name*.realm • *value-specified-for-realm_name*.kdc	true or false Default value: false
auth.kerberos.default_tkt_enctypes	Specifies the encryption type used for Kerberos authentication. You can use the following encryption types: • AES128-CTS • AES256-CTS • RC4-HMAC • DES3-CBC-SHA1 • DES-CBC-MD5 • DES-CBC-CRC	encryption type Default value: none (DES-CBC-MD5 is used for authentication.)

Property	Description	Possible Values
	If you want to specify multiple encryption types, use a comma to separate the encryption types. Among the specified encryption types, an encryption type that is supported by both the management server OS and a Kerberos server will be used.	
auth.kerberos.clockskew	Specifies the acceptable range of difference between the management server time and Kerberos server time. If the difference exceeds this value, an authentication error occurs.	0 to 300 (seconds} Default: 300
auth.kerberos.timeout	Specifies the amount of time to wait before timing out when connecting to the Kerberos server. If you specify 0, the system waits until a communication error occurs without timing out.	0 to 120 (seconds) Default value: 3
auth.kerberos.realm_name	Specifies the realm identification names. You can specify any name for this attribute in order to identify which realms the property attribute settings are applied to. If you specify 0, the system waits until a communication error occurs without timing out.	realm identification names Default value: none
auth.kerberos.*value-specified-for-auth.kerberos.realm_name*.realm	Specifies the name of the realm set on the Kerberos server. (required) Use the value specified in the "realm-name" property.	realm name Default value: none
auth.kerberos.*value-specified-for-auth.kerberos.realm_name*.kdc	Specifies information about the Kerberos server in the following format: *host-name-or-IP-address*[:*port-number*] *host-name-or-IP-address* If you specify the host name, make sure beforehand that the name can be resolved to an IP address. If you specify the IP address, use an IPv4 address. Note that you cannot specify the loopback address (localhost or 127.0.0.1). *port-number* Make sure beforehand that the port you specify is set as the listen port number on the Kerberos server. If you do not specify a port number or the specified port number cannot be used in a Kerberos server, 88 is assumed. When specifying multiple Kerberos servers, separate them with commas as follows:	Default value: none

Property	Description	Possible Values
	host-name-or-IP-address[:*port-number*],*host-name-or-IP-address*[:*port-number*],... This attribute is required. **Note:** When using StartTLS as the protocol for connecting to an external authentication server, in the host attribute specify the same host as the value of the CN in the LDAP directory server certificate. You cannot use an IP address.	
auth.group.*realm-name*.protocol	Specifies the protocol for connecting to the LDAP directory server (required). When communicating in plain text format, specify ldap. When using StartTLS communication, specify tls. Before specifying tls, ensure that one of the following encryption methods is supported on the Kerberos server: • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA **Note:** When communicating by using StartTLS as the protocol for connecting to the LDAP directory server, you need to specify the security settings of Common Component. Do not specify a space character at the beginning or end of set values. In addition, do not enclose set values in double quotation marks ("). If you do so, the value is ignored and the default value is used.	ldap or tls Default value: ldap
auth.group.*realm-name*.port	Specifies port number of the LDAP directory server. Ensure beforehand that the port you specify is set as the listen port number on the LDAP directory server.	1 to 65535 Default value: 389
auth.group.*realm-name*.basedn	Specifies the BaseDN, which is the DN of the entry used as the start point when searching for LDAP user information on the LDAP directory server. The user entries located below the hierarchy in this DN are checked during authorization.	DN(BaseDN) Default value: none

Property	Description	Possible Values
	Specify the DN of the hierarchy that includes all of the user entries to be searched. Specify the DN by following the rules defined in RFC4514. For example, if spaces or any of the following characters are included in a DN, you need to use a backslash (\) to escape each character: # + ; , < = > \ If you must escape any of the characters in the BaseDN, ensure that you escape the characters correctly because the specified value is passed to the LDAP directory server without change. If you omit this attribute, the value specified in the `defaultNamingContext` property of Active Directory is assumed as the BaseDN.	
`auth.group.`*`realm-name`*`.timeout`	Specifies the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out.	0 to 120 (seconds) Default value: 15
`auth.group.`*`realm-name`*`.retry.interval`	Specifies the retry interval when an LDAP directory server connection attempt fails.	1 to 60 (seconds) Default value: 1
`auth.group.`*`realm-name`*`.retry.times`	Specifies the number of retries to attempt when an LDAP directory server connection fails. If you specify 0, no retries are attempted.	0 to 50 Default value: 20

Related references

- Example properties file for Kerberos server connections (exauth.properties) on page 317

Example properties file for Kerberos server connections (exauth.properties)

When using Hitachi Compute Systems Manager, you can use an external authentication server. To set up a connection with an external Kerberos server for authentication, you edit the properties in the `exauth.properties` file on the Compute Systems Manager management server. The following examples include the parameter settings that you use to set up your Kerberos server connection. Depending on the type of connection, some parameters might not apply to your environment.

The following example shows the parameters that you specify when directly entering information for the Kerberos server (when not connecting to an external authorization server):

```
auth.server.type=kerberos

auth.group.mapping=false

auth.ocsp.enable=false

auth.ocsp.responderURL=

auth.kerberos.default_realm=EXAMPLE.COM

auth.kerberos.dns_lookup_kdc=false

auth.kerberos.clockskew=300

auth.kerberos.timeout=3

auth.kerberos.realm_name=RealmName

auth.kerberos.RealmName.realm=EXAMPLE.COM

auth.kerberos.RealmName.kdc=kerberos.example.com:88
```

The following example shows the parameters that you specify when using a DNS server information to obtain information about the Kerberos server (when not linking with an external authorization server):

```
auth.server.type=kerberos

auth.group.mapping=false

auth.kerberos.default_realm=EXAMPLE.COM

auth.kerberos.dns_lookup_kdc=true

auth.kerberos.clockskew=300

auth.kerberos.timeout=3
```

The following example shows the parameters when entering information about the Kerberos directory server directly when also linking with an external authorization server:

```
auth.server.type=kerberos

auth.group.mapping=true

auth.ocsp.enable=false

auth.ocsp.responderURL=

auth.kerberos.default_realm=EXAMPLE.COM

auth.kerberos.dns_lookup_kdc=false

auth.kerberos.clockskew=300

auth.kerberos.timeout=3
```

```
auth.kerberos.realm_name=RealmName

auth.kerberos.RealmName.realm=EXAMPLE.COM

auth.kerberos.RealmName.kdc=kerberos.example.com:88

auth.group.EXAMPLE.COM.protocol=ldap

auth.group.EXAMPLE.COM.port=389

auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com

auth.group.EXAMPLE.COM.timeout=15

auth.group.EXAMPLE.COM.retry.interval=1

auth.group.EXAMPLE.COM.retry.times=20
```

The following example shows the parameters that you specify when using a DNS server information to obtain information about the Kerberos server when also linking with an external authorization server:

```
auth.server.type=kerberos

auth.group.mapping=true

auth.kerberos.default_realm=EXAMPLE.COM

auth.kerberos.dns_lookup_kdc=true

auth.kerberos.clockskew=300

auth.kerberos.timeout=3
```

Related references

- Properties related to Kerberos server connections (exauth.properties) on page 313

Properties related to audit logs (auditlog.conf)

The Common Component `auditlog.conf` file contains parameters related to audit logs as listed in the following table:

Property	Description
`Log.Facility`	Unused - Ignored even if specified.
`Log.Event.Category`	Specifies the audit event categories that you want generated. To specify multiple categories, separate them using commas, but do not insert spaces between categories and commas. This parameter value is required for audit logging to function. Valid values: StartStop, Authentication, ConfigurationAccess, ExternalService

Property	Description
	If an invalid category name is specified, the specified file name is ignored. Default value: none
Log.Level	Specifies the severity level of audit events that you want generated. Events with the specified severity level or lower are output to the event log file. If an invalid value or a non-numeric character is specified, the default value is used. Value range: 0 to 7 - severity level Default value: 6

The following table shows the correspondence between the audit event severity levels and event log data types.

Audit event severity	Type of event log data
0	Error
1	
2	
3	
4	Warning
5	Information
6	
7	

The following is an example of a `auditlog.conf` file where events related to Authentication or ConfigurationAccess services are generated. For Windows, `Log.Level 6` specifies that the system output audit log data corresponding to Error, Warning, and Information levels. For Linux, `Log.Facility 1` outputs the audit log data to the syslog file that is defined as the user facility in the `syslog.conf` file.

```
# Specify an integer for Facility. (specifiable range: 1-23)

Log.Facility 1

# Specify the event category.

# You can specify any of the following:

# StartStop, Failure, LinkStatus, ExternalService,

# Authentication, ContentAccess,
```

```
# ConfigurationAccess, Maintenance, or AnomalyEvent.

Log.Event.Category Authentication,ConfigurationAccess

# Specify an integer for Severity. (specifiable range: 0-7)

Log.Level 6
```

Related concepts

- About audit logs on page 267

Related references

- Properties files for Hitachi Command Suite Common Component on page 294

Properties related to clustering (cluster.conf)

The Common Component `cluster.conf` file contains parameters related to clustering as listed in the following table:

Property	Description
`mode`	Specifies the node type as follows: For the active node, specify "online". For the standby node, specify "standby".
`virtualhost`	Specifies a logical host name. You must specify a host name. You cannot specify an IP address. You must also ensure that the logical host name is associated with an access-enabled IP address.
`onlinehost`	Specifies the host name of the active node. You must specify a host name. You cannot specify an IP address.
`standbyhost`	Specifies the host name of the standby node. You must specify a host name. You cannot specify an IP address.

Related references

- Properties files for Hitachi Command Suite Common Component on page 294

Properties related to Deployment Manager ports (port.ini)

If you change the Deployment Manager port number, you must edit the `port.ini` properties file.

The `port.ini` file is located in the following folder:

HCSM-installation-folder`\ComputeSystemsManager\DeploymentManager\PXE\Images`

The Deployment Manager `port.ini` file includes the port and function-related parameters listed in the following table:

Property	Description
BackupRestoreUnicast	This port is used for managed resource disk backup and restoration. The default value is 26501. If an attempt to change this port number fails, the system uses the default value 56020/tcp.
BOOTNIC	This port is used for managed resource PXE booting. The default value is 26502. If an attempt to change this port number fails, the system uses the default value 56022/tcp.
FSC	This port is used for managed resource PXE booting. The default value is 26503. If an attempt to change this port number fails, the system uses the default value 56030/tcp.
FTUnicast	This port is used for operating managed resource disks. The default value is 26508. If an attempt to change this port number fails, the system uses the default value 56023/tcp.

C

Upgrading the software from v7.*x*

The module explains how to upgrade Hitachi Compute Systems Manager from v7.*x* on the management server.

- ☐ About upgrading from Hitachi Compute Systems Manager v7.x
- ☐ Prerequisites for upgrading the software from v7.x
- ☐ Upgrading the software from v7.x in a non-cluster environment
- ☐ Upgrading the software from v7.x in a cluster environment

About upgrading from Hitachi Compute Systems Manager v7.*x*

To upgrade Hitachi Compute Systems Manager from v7.*x* on the management server, you must install Compute Systems Manager v8.0 or later and complete some additional tasks, which depend on whether you are upgrading in a cluster environment.

Related tasks

- Upgrading the software from v7.x in a non-cluster environment on page 325
- Upgrading the software from v7.x in a cluster environment on page 327

Related references

- Prerequisites for upgrading the software from v7.x on page 324

Prerequisites for upgrading the software from v7.*x*

Before beginning an upgrade from v7.*x*, ensure that you are aware of the following:

- Hitachi Compute Systems Manager v7.*x* is removed during the upgrade. This includes removing all files and directories that were created during the Compute Systems Manager installation. If you want to reuse these directories, you must back them up in a different location before running the upgrade.
- If any Hitachi Command Suite products v7.*x* or earlier are installed, you must upgrade all Hitachi Command Suite products to v8.0 or later before you start using the upgraded Compute Systems Manager software.
- Do not install any Hitachi Command Suite products v7.x or earlier on a Compute Systems Manager management server that you upgraded to v8.0 or later.
- After you upgrade Compute Systems Manager, the default port number for non-SSL communications changes from 23015 to 22015.
  If the management server URL is already registered in the Web browser or if a port number for non-SSL communications is registered as a firewall exception, you must update these settings.
- Compute Systems Manager v8.0 or later management servers use the following command names and the following default installation locations:
  - Command names:
    `hcmds`*`xxxx`* changes to `hcmds64`*`xxxx`*
  - Default Compute Systems Manager installation folder (Windows):
    v7.*x* folders:
    Windows (32-bit): `%ProgramFiles%\HiCommand`

Windows (64-bit): `%ProgramFiles(x86)%\HiCommand`
v8.0 or later folders change to the following:
`%ProgramFiles%\HiCommand`

Note: Deployment Manager is installed in the folder set for `%ProgramFiles(x86)%`

`%ProgramFiles%` and `%ProgramFiles(x86)%` are Windows environment variables.

- Default Hitachi Command Suite Common Component installation folder (Windows)
  v7.*x* folder:
  HCSM-installation-folder\Base
  v8.0 or later folder changes to the following:
  HCSM-installation-folder\Base64
  If you were using scripts on the management server before the upgrade that contain any the command names or file paths listed here, you must revise the command names and file paths in these scripts to continue using them on the management server after you upgrade Compute Systems Manager.

Related concepts

- About upgrading from Hitachi Compute Systems Manager v7.x on page 324

Related tasks

- Upgrading the software from v7.x in a non-cluster environment on page 325
- Upgrading the software from v7.x in a cluster environment on page 327

Upgrading the software from v7.*x* in a non-cluster environment

You can upgrade a Hitachi Compute Systems Manager v7.*x* management server to v8.*x* in a non-cluster environment by completing the prerequisite tasks and then completing the upgrade process.

Prerequisites

Before you begin upgrading, verify the following:

- The pre-installation checklist is complete.
- If you plan to install Deployment Manager, verify that your system meets the Deployment Manager installation prerequisites.

- If you plan to install other Hitachi Command Suite products by using the integrated installation media, ensure that the system meets the installation requirements for all the products.
- If any products using Hitachi Command Suite Common Component are installed, the services for those products are stopped.
- The Windows Services dialog box and Event Viewer dialog box are closed.
- The management server settings have been reviewed.
  The following settings are inherited from Compute Systems Manager v7.*x* during an upgrade to v8.*x* or later:
  - Databases
  - Authentication information about Hitachi Command Suite product databases including Compute Systems Manager
  - MIB files, including SNMP trap definitions
    The MIB files are moved to the installation directory after the upgrade.
  - Properties files on the Compute Systems Manager server (`user.properties` and `logger.properties`)
    The content of the properties files for v7.*x* are merged into the properties files for the upgraded version.

  Files and settings that are not included in the previous list are initialized after the upgrade. If you have made changes to any settings not in this list, you must make a note of these settings so that you can modify them after the installation finishes.
- If in use, Deployment Manager is removed.
  Removing Deployment Manager requires using the v7.*x* installation media. When you run the Compute Systems Manager installation wizard, select Deployment Manager to remove it.

Procedure

1. Mount the installation media on the management server.
   If you are using the integrated installation media and the installation window does not open automatically, double-click *integrated-installation-media*\index.html.
2. Start the installation wizard.
   - If you are using the Compute Systems Manager installation media, run the following command:
     HCSM-installation-media\HCSM_SERVER\setup.exe
   - If you are using the integrated installation media, the installation window opens. Select **HCSM**, and then click **Install**.
3. Follow the installation wizard prompts and specify the required information.
4. In the Install Complete window, click **Finish**.
5. If you need to modify any management server settings overwritten by the upgrade, reconfigure the settings as needed.
6. Restart Compute Systems Manager.

7. Verify that you can access Compute Systems Manager using a web browser.

Note:

- If Compute Systems Manager is installed in an environment in which SSL communication is enabled or in which the port number for Hitachi Command Suite Common Component was changed, the GUI might not start, even if you select the **After the installation finishes, start Hitachi Command Suite GUI** check box in the Install Complete window.
  If this problem occurs, check the management server information that changed, and then enter the URL for Compute Systems Manager in the web browser address bar to start the GUI.
- A blank or transitional window might open after you log on to Compute Systems Manager if Internet Explorer 11 is set as the default browser. In this case, restart the web browser and type the URL for Compute Systems Manager in the web browser address bar.

Result

You can now start using the new version of Compute Systems Manager.

Related concepts

- About upgrading from Hitachi Compute Systems Manager v7.x on page 324
- About installing Hitachi Compute Systems Manager on page 46

Related tasks

- Verifying access to the management server on page 52
- Installing Deployment Manager on page 169
- Starting Hitachi Compute Systems Manager on page 174
- Stopping Hitachi Compute Systems Manager on page 175

Related references

- Prerequisites for upgrading the software from v7.x on page 324

Upgrading the software from v7.*x* in a cluster environment

You can upgrade Hitachi Compute Systems Manager v7.*x* on a management server in a cluster environment.

Prerequisites

Before you begin upgrading, verify the following:

- The pre-installation checklist is complete.
- If you plan to install Deployment Manager, verify that your system meets the Deployment Manager installation prerequisites.
- If you plan to install other Hitachi Command Suite products by using the integrated installation media, ensure that the system meets the installation requirements for all the products.
- If any products using Hitachi Command Suite Common Component are installed, the services for those products are stopped.
- The Windows Firewall is enabled, ensure the service is running.
- The Windows Services dialog box and Event Viewer dialog box are closed.
- The management server settings have been reviewed.
  The following settings are inherited from Compute Systems Manager v7.*x* during an upgrade to v8.*x* or later:
  - Databases
  - Authentication information about Hitachi Command Suite product databases including Compute Systems Manager
  - MIB files, including SNMP trap definitions
    The MIB files are moved to the installation directory after the upgrade.
  - Properties files on the Compute Systems Manager server (`user.properties` and `logger.properties`)
    The content of the properties files for v7.*x* are merged into the properties files for the upgraded version.

  Files and settings that are not included in the previous list are initialized after the upgrade. If you have made changes to any settings not in this list, you must make a note of these settings so that you can modify them after the installation finishes.
- Verify that there is adequate free disk space on the management server running in the cluster environment.
- Check the port number used for the database.
  If you upgrade Compute Systems Manager, the database port number is set to the default (22032/tcp).
  If you have changed the port number from the default, record the port number that you are using.
- If other Hitachi Command Suite product services are already registered to the cluster management application group used by the installation wizard, note the following:
  When you run an installation on an active node, all registered services are removed and then re-registered by default when you complete the installation on the standby node. If you changed the service resource names, record the resource names in advance, and then manually change the names after the installation is finished.

Note: This step does not apply to Hitachi File Services Manager resources because they are not removed during the installation.

Procedure

1. Using the cluster management software, do the following:
   a. Move the owner of the group in which Hitachi Command Suite services are registered to the active node.
   b. Bring the cluster management IP address and shared disks online.
2. If you are using Deployment Manager, remove it from the active node. To remove the software, use the v7.*x* installation media and within the Compute Systems Manager installation wizard, select Deployment Manager, and remove it.
3. Upgrade Compute Systems Manager on the active node by running the installation wizard, selecting the cluster configuration option, and specifying the required information.

   If another Hitachi Command Suite product already exists in the cluster environment, you do not need to specify any settings because the installation program automatically uses the existing configuration settings.

   Note: You cannot install Deployment Manager by using the All-in-One Installer.

4. After completing the upgrade on the active node, use the cluster management software to move the owner of the group in which Hitachi Command Suite services are registered to the standby node.
5. If you are using Deployment Manager, remove it from the standby node. To remove the software, use the v7.*x* installation media and within the Compute Systems Manager installation wizard, select Deployment Manager, and remove it.
6. Upgrade Compute Systems Manager on the standby node by running the installation wizard.

   During the installation or upgrade, ensure you follow these requirements:
   - Install Compute Systems Manager in the same location as on the active node.
   - If you installed Deployment Manager on the active node, install it on the standby node.

   Note: When completing a new installation of multiple Hitachi Command Suite products on a standby node, install the products in the order that they were installed on the active node.

7. If you changed the database port number to a port number other than the default, specify the port number that you recorded earlier.

Note: If a product that uses the 32-bit version of Hitachi Command Suite Common Component is installed (Hitachi File Services Manager or Hitachi Storage Navigator Modular 2), make sure that the port numbers you set do not conflict with the port number used by these products.

8. To start Compute Systems Manager in the cluster, run the following command :

   HCS-Common-Component-installation-folder\Clustersetup\hcmds64clustersrvstate /son /r *group-name*

9. To register a plug-in license, enter the license key on the standby node.
10. To manage a Hitachi server, change the settings as needed so that the management server IP address registered on the Hitachi server can be used as the cluster management IP address.

    Specify the cluster management IP address for the `svp.bind.address` property of the following file:

    HCSM-installation-folder\ComputeSystemsManager\conf\user.properties

Tip:

- If the `svp.bind.address` property is not specified, the IP address of the active and standby nodes is registered on the Hitachi server.
- The management server IP address, with which the Hitachi server is communicating, is registered on the Hitachi server. If you specify the `svp.bind.address` property, the IP address specified for the property is also registered. You can check the management server IP addresses registered on the Hitachi servers by using the Web console. If you find management server IP addresses that are no longer in use, delete them.

11. Using the cluster management software, move the owner of the group in which you registered the Compute Systems Manager services to the active node.
12. If you registered a plug-in license on the standby node, enter the same license key on the active node.
13. If you installed Deployment Manager, set up the cluster environment so that you can enable and use Deployment Manager.

Related concepts

- Hitachi Compute Systems Manager services used in a cluster environment on page 191
- About verifying the installation environment on page 41

Related tasks

- Installing Deployment Manager on page 169
- Temporarily stopping Hitachi Compute Systems Manager in a cluster environment (Windows) on page 232
- Installing the software (Windows) on page 47
- Changing Hitachi Compute Systems Manager ports on page 74
- Stopping Hitachi Compute Systems Manager on page 175

Related references

- Command format for migrating to a Linux cluster environment on page 247
- Synchronizing settings in a cluster environment on page 230
- Hitachi Command Suite properties requiring updates for port number changes on page 71
- Prerequisites for installing Deployment Manager on page 166
- Prerequisites for upgrading the software from v7.x on page 324
- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 291
- Properties related to clustering (cluster.conf) on page 321

Glossary

A

active blade server

A server that is actively running your applications. When using the N+M cold standby feature for redundancy, the *running* server is referred to as an active server and the failover server is referred to as the *standby* server.

alert

A notification that a certain event has occurred. Alerts are triggered when errors or failures occur on a component of a managed resource, or when thresholds are exceeded.

B

base DN

The starting point in the active directory hierarchy at which your searches begin.

C

certificate

Refers to a digital certificate used with SSL. The browser examines the certificate and determines whether it is authentic before allowing communication.

certificate signing request

A message that is sent from an applicant to a certification authority to apply for a digital identity certificate.

chassis

A housing in which blades and other various shared electronic components are mounted.

CLI

command line interface

CSV

comma-separated values

D

daemon

A Linux program that runs in the background.

device (dev or DEV)

A physical or logical unit with a specific function.

discovery

A process that finds and identifies network objects. For example, discovery may find and identify all hosts within a specified IP address range.

Distributed Component Object Model (DCOM)

A Microsoft Windows interface in which client programs can request services from other network computers.

Domain Name System (DNS)

A hierarchical distributed naming system for computers.

F

FC

Fibre Channel

Fibre Channel Information Tool (fcinfo)

A tool used on Microsoft Windows servers that enables remote gathering of Fibre Channel information for servers connected to SAN storage.

G

GUI

graphical user interface

H

HBA

See host bus adapter.

host bus adapter (HBA)

One or more dedicated adapter cards that are installed in a host, have unique WWN addresses, and provide Fibre Channel I/O connectivity to storage systems, typically through Fibre Channel switches. Unlike general-purpose Ethernet adapters, which handle a multitude of network protocols, host bus adapters are dedicated to high-speed block transfers for optimized I/O performance.

hypervisor

Software that enables multiple guest operating systems (virtual machines) to run concurrently on a single physical host computer. Each operating system runs independently, but the hypervisor controls the host processor and resources.

I

inventory

Information about managed resources, such as operating system version, hardware status, and IP address.

IPMI

Intelligent Platform Management Interface

J

Java heap dump

A record of all live Java objects and classes that is used for troubleshooting diagnostics.

Java thread

A Java program's path of execution.

JDK

Java Development Kit

K

key password

Unlocks the private keys stored in the keystore.

keystore

A keystore contains private keys and certificates with corresponding public keys that are used for secure SSL communications.

L

lights-out management (LOM)

Provides remote management of discovered hosts by connecting to a host's management interface from the Hitachi Compute Systems Manager management client.

Lightweight Directory Access Protocol (LDAP) server

A server that provides distributed directory service such as user account information.

logical group

A user-defined collection of managed resources, grouped together by installation location, organization, or use.

M

managed resource

Any system, such as a host, chassis, or server, managed by Hitachi Compute Systems Manager.

management client

A computer used to operate a graphical user interface client or a command-line interface client.

management information base (MIB)

A virtual database of objects that can be monitored by a network management system. SNMP uses standardized MIBs that allow any SNMP-based tool to monitor any device defined by a MIB file.

management module

A component installed in a chassis that controls the blades and other various shared electronic components.

management target

Any system, such as hosts, servers, or chassis, within an IP address range that is targeted to be managed by a software application.

N

N+M cold standby

A failover mechanism for servers that increases availability. With N+M cold standby, "N" servers are active and running your applications, and "M" servers are on standby, powered off, and not consuming data center resources. If a failure occurs on a running blade server, the software detects the failure and automatically replaces the failed blade with a standby blade.

O

object identifier (OID)

OIDs uniquely identify managed objects. SNMP traps can be distinguished from each other because they have unique OIDs.

P

performance profile

A user-defined set of performance metrics and data collection interval settings used to collect and analyze managed host performance data.

power profile

A user-defined set of performance metrics and data collection interval settings used to collect and analyze chassis power consumption data.

private key

An encryption/decryption key known only to the party or parties that exchange secure communication.

properties file

A file that defines aspects of the operating environment. The operating environment can be modified by changing the appropriate properties file.

R

remote method invocation (RMI) request

A request to invoke a program on a remote computer.

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.

root

A Linux user account that has access to all commands and files.

S

SAN

See storage area network.

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.

self-signed certificate

A digital identity certificate signed by the person who created it, rather than a trusted certificate authority.

SNMP

Simple Network Management Protocol

SNMP trap

An event generated by an SNMP agent from the managed resource that communicates an event, such as an error or failure.

SRV (service) record

A specification of data in DNS for defining the location (host name and port number) of servers or services.

SSH (secure shell)

A network protocol for secure data communication.

standby blade server

A server that remains powered-off until it is required to replace another server on which a failure occurs. When using the N+M cold-standby feature for redundancy, the running server is referred to as an *active* server, and the failover server is referred to as the *standby* server.

storage area network (SAN)

A network of shared storage devices that contain disks for storing data.

su command

The su command changes user credentials on a Linux system to those of the root user or to the user specified by the Name parameter, and then initiates a new session.

sudo command

The sudo (superuser do) command allows a system administrator to change user credentials on a Linux system to those of the root user or to the user specified by the Name parameter, and then initiates a new session. The session is usually limited and all actions are recorded in a log.

T

threshold

A user-defined limit that triggers an alert when reached or exceeded.

transport layer security (TLS)

Transport layer security (TLS) and its predecessor, secure sockets layer (SSL), are cryptographic protocols that provide communication security over the Internet.

truststore

A truststore contains public keys in the form of trusted third-party certificates, such as those from a certificate authority (CA) or from another party with which you must set up secure SSL communication.

truststore file

A key database file that contains public keys for a trusted entity.

U

User Access Control (UAC)

Management of user accounts in Windows Server 2008.

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.

V

virtual machine

One instance of an operating system along with one or more applications running in an isolated partition within the computer. A VM enables different operating systems to run in the same computer at the same time as well as prevents applications from interfering with each other. All virtual machines run simultaneously.

virtual machine manager (VMM)

Software that manages hypervisors and the associated virtual machines (for the fundamental concept, see *virtual machine*). VMMs can manage multiple hypervisors and all virtual machines running on the hypervisor. VMMs can create virtual machines, change virtual machine configuration, and migrate virtual machines to a different hypervisor.

W

wake-on-LAN (WOL)

An ethernet computer networking standard that allows a computer or server to be turned on or *awakened* from a remote location by a network message.

Windows Management Instrumentation (WMI)

A method for managing Windows devices, for example, to connect to Windows hosts.

Index

D

E

F

H

I

J

K

L

M

O

P

R

S

T

U

Hitachi Data Systems

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

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

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

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

Hitachi Data Systems

MK-91HC195-15