# Contents

Preface

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intended audience</td>
<td>12</td>
</tr>
<tr>
<td>Product version</td>
<td>12</td>
</tr>
<tr>
<td>Release notes</td>
<td>12</td>
</tr>
<tr>
<td>Document revision level</td>
<td>12</td>
</tr>
<tr>
<td>Referenced documents</td>
<td>12</td>
</tr>
<tr>
<td>Document conventions</td>
<td>13</td>
</tr>
<tr>
<td>Conventions for storage capacity values</td>
<td>13</td>
</tr>
<tr>
<td>Accessing product documentation</td>
<td>14</td>
</tr>
<tr>
<td>Getting help</td>
<td>14</td>
</tr>
<tr>
<td>Comments</td>
<td>15</td>
</tr>
</tbody>
</table>

1 Hitachi Compute Systems Manager overview

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hitachi Compute Systems Manager overview</td>
<td>18</td>
</tr>
<tr>
<td>About Hitachi Compute Systems Manager</td>
<td>18</td>
</tr>
<tr>
<td>About Hitachi Compute Systems Manager managed resources</td>
<td>18</td>
</tr>
<tr>
<td>Hitachi Compute Systems Manager system configuration</td>
<td>19</td>
</tr>
<tr>
<td>About Hitachi Compute Systems Manager components</td>
<td>19</td>
</tr>
<tr>
<td>About basic system configuration</td>
<td>20</td>
</tr>
<tr>
<td>About Hitachi Compute Systems Manager LAN configuration</td>
<td>21</td>
</tr>
<tr>
<td>About related Hitachi Command Suite products</td>
<td>21</td>
</tr>
<tr>
<td>Hitachi Compute Systems Manager overview workflow</td>
<td>21</td>
</tr>
<tr>
<td>Installation and initial configuration workflows</td>
<td>23</td>
</tr>
<tr>
<td>Installation workflow</td>
<td>23</td>
</tr>
<tr>
<td>Post-installation workflow</td>
<td>23</td>
</tr>
<tr>
<td>System configuration workflows</td>
<td>25</td>
</tr>
<tr>
<td>SNMP trap setup workflow</td>
<td>25</td>
</tr>
<tr>
<td>Managed host setup workflow</td>
<td>25</td>
</tr>
<tr>
<td>Secure communications workflows</td>
<td>27</td>
</tr>
<tr>
<td>Workflow for setting up secure communication with management clients</td>
<td>27</td>
</tr>
<tr>
<td>Workflow for setting up secure communication with an SMTP server</td>
<td>28</td>
</tr>
<tr>
<td>Workflow for setting up secure communication with managed servers</td>
<td>29</td>
</tr>
</tbody>
</table>
2 Installing Hitachi Compute Systems Manager........................................... 39

Verifying system prerequisites required for installation........................................ 40
  About verifying system prerequisites.................................................................. 40
  Verifying the system prerequisites........................................................................ 40
  Avoiding port conflicts....................................................................................... 40
  Adding the management server host name to the hosts file (Linux)...................... 41
  Configuring kernel parameters and shell restrictions (Linux)................................. 41
  Registering firewall exceptions (Linux)................................................................ 42
  Verifying the server time setting.......................................................................... 42

Verifying the installation environment...................................................................... 43
  About verifying the installation environment....................................................... 43
  Rules for specifying path names........................................................................... 44
  Preparing the installation directories.................................................................... 45
  Specifying management server information during installation........................... 47

Installing Hitachi Compute Systems Manager.................................................... 47
  About installing Hitachi Compute Systems Manager............................................. 47
  Installing the software (Windows)....................................................................... 48
  Installing from the integrated media by using the all-in-one installer (Windows).... 50
  Installing the software (Linux)............................................................................ 51
  Setting requirements for virus scanning program settings..................................... 52

Post-installation tasks............................................................................................. 53
  About Hitachi Compute Systems Manager post-installation tasks........................ 53
  Verifying access to the management server........................................................ 53
  Registering a license............................................................................................. 54
  Changing the System account password............................................................... 55
  Setting an e-mail address for the System account................................................ 55
  Setting up e-mail notifications............................................................................. 56
  Setting up the alert level for e-mail notifications................................................... 56
  Adding resources to Hitachi Compute Systems Manager...................................... 57

Optional initial setup tasks....................................................................................... 58
  Creating a server administrator account............................................................... 58
  Creating resource groups..................................................................................... 59
  Creating user groups and setting up access control............................................. 59

Completing the initial setup...................................................................................... 60

Removing Hitachi Compute Systems Manager..................................................... 60
  About removing Hitachi Compute Systems Manager.......................................... 60
  Prerequisites for removing the software.............................................................. 61
  Removing the software (Windows)....................................................................... 62
  Removing the software by using the all-in-one uninstaller (Windows)................... 63
  Removing the software (Linux)............................................................................ 63
Prerequisites for determining LDAP server connection properties........................132
Prerequisites for using a DNS server to connect to an LDAP server.....................132
Connecting to an LDAP directory server.................................................................133
Configuring an LDAP server connection...............................................................133
Configuring SSL for a secure LDAP server connection........................................135
Verifying an LDAP server connection................................................................136
Connecting to a Kerberos server............................................................................137
Encryption types for Kerberos authentication....................................................137
Configuring a Kerberos server connection............................................................138
Verifying a Kerberos server connection.............................................................139
Settings for connecting to an LDAP server............................................................140
Settings for connecting directly to an LDAP server.............................................140
Settings for using DNS to connect to an LDAP server........................................141
Settings for connecting directly to an LDAP server and an authorization server...142
Settings for using DNS to connect to an LDAP server and an authorization server .................................................................143
Settings for connecting to a Kerberos server..........................................................144
Settings for connecting directly to a Kerberos server............................................144
Settings for using DNS to connect to a Kerberos server......................................145
Settings for connecting directly to a Kerberos server and an authorization server.146
Settings for using DNS to connect to a Kerberos server and an authorization server .....................................................................................................................147
Commands for connecting to an external authentication server........................147
About using commands to connect to an external authentication server.............147
Command format for verifying an external server connection.............................148
Using an LDAP search user account when connecting to an LDAP server...........150
Prerequisites for registering a search user............................................................150
Command format for registering a search user..................................................151
Checking the registration status of an LDAP search user....................................152
Deleting an LDAP search user..........................................................................153
LDAP certificates for secure communications.......................................................153
Prerequisites for configuring a secure LDAP server connection........................153
Rules for importing LDAP directory server certificates......................................154
Command format for importing LDAP server certificates...................................154

7 Installing and configuring Deployment Manager.............................................157
About Deployment Manager environment settings..................................................158
Prerequisites for installing Deployment Manager.....................................................158
Installing Internet Information Server....................................................................159
Installing .NET Framework for Deployment Manager........................................160
Installing Deployment Manager.............................................................................161
Prerequisites for using Deployment Manager..........................................................161
Configuring managed resources for use with Deployment Manager..................162
Changing the Deployment Manager port number....................................................162
Editing Deployment Manager properties and settings files when changing ports...163

8 Administering the management server..........................................................165
Starting and Stopping Hitachi Compute Systems Manager.....................................166
About starting and stopping Hitachi Computer Systems Manager........................166
Starting Hitachi Compute Systems Manager.......................................................166
9 Implementing Hitachi Compute Systems Manager in a cluster environment

About implementing and using HCSM in a cluster environment.............................. 180
HCSM services used in a cluster environment......................................................... 181
Prerequisites for implementing HCSM in a cluster environment............................. 181
  Determining which method to use when implementing HCSM in a cluster
  environment........................................................................................................ 181
  Verifying the free disk space of a management server in a cluster environment... 185
Checking the cluster environment configuration using the cluster management
  software.............................................................................................................. 186
Installing Hitachi Compute Systems Manager in a cluster environment.................... 186
  Setting up a new instance of HCSM on an active node...................................... 187
  Setting up a new instance of HCSM on a standby node..................................... 190
Upgrading Hitachi Compute Systems Manager in a cluster environment............... 193
  Upgrading or overwriting HCSM on an active node.......................................... 193
  Upgrading or overwriting HCSM on a standby node........................................ 195
Migrating Hitachi Compute Systems Manager (HCSM) to a cluster environment..... 197
Configuring HCSM within a cluster environment.................................................... 201
  Settings requirements for virus scanning programs in a cluster environment...... 201
  Synchronizing settings in a cluster environment.............................................. 201
  Setting up a cluster within Windows Server Failover Clustering......................... 202
  Setting up Deployment Manager in a cluster environment using Windows Server
  Failover Clustering.......................................................................................... 204
Starting and stopping services in a cluster environment......................................... 207
  Bringing HCSM services online from cluster management software.................. 207
  Taking HCSM services offline from cluster management software..................... 207
  Temporarily stopping HCSM in a cluster environment....................................... 208
  Restarting HCSM in a cluster environment...................................................... 209
Managing the database in a cluster environment.................................................... 210
  Backing up the database in a cluster environment.......................................... 210
  Restoring the database in a cluster environment............................................. 211
  Exporting the database in a cluster environment............................................ 212
  Importing the database in a cluster environment.......................................... 213
  Command format for migrating to a cluster environment.............................. 214
Removing Deployment Manager from a cluster environment................................ 215
Removing the software in a cluster environment.................................................. 217
Properties related to the database (pdsys)..........................................................269
Properties related to the database (def_pdsys)..................................................270
Properties related to the database (pdutsys).....................................................271
Properties related to the database (def pdutsys)..............................................271
Properties related to System account locking (user.conf).................................271
Properties related to LDAP directory server connections (exauth.properties)........272
Example properties file for external LDAP directory server connections (exauth.properties)......................................................................................... 276
Properties related to Kerberos server connections (exauth.properties)..............277
Example properties file for Kerberos server connections (exauth.properties)......279
Properties related to audit logs (auditlog.conf)................................................283
Properties related to clustering (cluster.conf)...................................................287
Properties related to Deployment Manager ports (port.ini)................................288

C Upgrading the HCSM software from v7.x..........................................................289
About upgrading the HCSM software.................................................................290
Prerequisites for upgrading the HCSM software...............................................290
Upgrading the HCSM software in a non-cluster environment.............................291
Upgrading from HCSM in a cluster environment................................................293
  Upgrading the HCSM software on an active node.........................................293
  Upgrading the HCSM software on a standby node.......................................298

Glossary...........................................................................................................303

Index..............................................................................................................311
This manual describes how to install and configure Hitachi Compute Systems Manager (HCSM).

- Intended audience
- Product version
- Release notes
- Document revision level
- Referenced documents
- Document conventions
- Conventions for storage capacity values
- Accessing product documentation
- Getting help
- Comments
Intended audience

This document provides instructions for server administrators.

Product version

This document revision applies to Hitachi Compute Systems Manager (HCSM) v8.1.

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.

Document revision level

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MK-91HC195-01</td>
<td>November 2011</td>
<td>Initial release</td>
</tr>
<tr>
<td>MK-91HC195-02</td>
<td>July 2012</td>
<td>Supersedes and replaces MK-91HC195-01</td>
</tr>
<tr>
<td>MK-91HC195-03</td>
<td>September 2012</td>
<td>Supersedes and replaces MK-91HC195-02</td>
</tr>
<tr>
<td>MK-91HC195-04</td>
<td>November 2012</td>
<td>Supersedes and replaces MK-91HC195-03</td>
</tr>
<tr>
<td>MK-91HC195-05</td>
<td>February 2013</td>
<td>Supersedes and replaces MK-91HC195-04</td>
</tr>
<tr>
<td>MK-91HC195-06</td>
<td>May 2013</td>
<td>Supersedes and replaces MK-91HC195-05</td>
</tr>
<tr>
<td>MK-91HC195-07</td>
<td>August 2013</td>
<td>Supersedes and replaces MK-91HC195-06</td>
</tr>
<tr>
<td>MK-91HC195-08</td>
<td>October 2013</td>
<td>Supersedes and replaces MK-91HC195-07</td>
</tr>
<tr>
<td>MK-91HC195-09</td>
<td>April 2014</td>
<td>Supersedes and replaces MK-91HC195-08</td>
</tr>
<tr>
<td>MK-91HC195-10</td>
<td>August 2014</td>
<td>Supersedes and replaces MK-91HC195-09</td>
</tr>
<tr>
<td>MK-91HC195-11</td>
<td>October 2014</td>
<td>Supersedes and replaces MK-91HC195-10</td>
</tr>
</tbody>
</table>

Referenced documents

Hitachi Compute Systems Manager documents:
- *Hitachi Compute Systems Manager User Guide*, MK-91HC194
- *Hitachi Compute Systems Manager CLI Reference Guide*, MK-91HC196
- *Hitachi 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:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold</td>
<td>Indicates text on a window, other than the window title, including menus,</td>
</tr>
<tr>
<td></td>
<td>menu options, buttons, fields, and labels. Example: Click OK.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Indicates a variable, which is a placeholder for actual text provided by the</td>
</tr>
<tr>
<td></td>
<td>user or system. Example: copy source-file target-file</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Angled brackets (&lt; &gt;) are also used to indicate variables.</td>
</tr>
<tr>
<td>Monospace</td>
<td>Indicates text that is displayed on screen or entered by the user. Example:</td>
</tr>
<tr>
<td></td>
<td>pairdisplay -g oradb</td>
</tr>
<tr>
<td>&lt; &gt; angled brackets</td>
<td>Indicates a variable, which is a placeholder for actual text provided by the</td>
</tr>
<tr>
<td></td>
<td>user or system. Example: pairdisplay -g &lt;group&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Italic font is also used to indicate variables.</td>
</tr>
<tr>
<td>[ ] square brackets</td>
<td>Indicates optional values. Example: [ a</td>
</tr>
<tr>
<td></td>
<td>b, or nothing.</td>
</tr>
<tr>
<td>{ } braces</td>
<td>Indicates required or expected values. Example: { a</td>
</tr>
<tr>
<td></td>
<td>must choose either a or b.</td>
</tr>
<tr>
<td></td>
<td>vertical bar</td>
</tr>
<tr>
<td></td>
<td>Examples: [ a</td>
</tr>
<tr>
<td></td>
<td>{ a</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Note</td>
<td>Calls attention to important or additional information.</td>
</tr>
<tr>
<td>☀</td>
<td>Tip</td>
<td>Provides helpful information, guidelines, or suggestions for performing tasks more effectively.</td>
</tr>
<tr>
<td>!</td>
<td>Caution</td>
<td>Warns the user of adverse conditions or consequences (for example, disruptive operations).</td>
</tr>
<tr>
<td>!</td>
<td>WARNING</td>
<td>Warns the user of severe conditions or consequences (for example, destructive operations).</td>
</tr>
</tbody>
</table>

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:
<table>
<thead>
<tr>
<th>Physical capacity unit</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 kilobyte (KB)</td>
<td>1,000 (10^3) bytes</td>
</tr>
<tr>
<td>1 megabyte (MB)</td>
<td>1,000 KB or 1,000(^2) bytes</td>
</tr>
<tr>
<td>1 gigabyte (GB)</td>
<td>1,000 MB or 1,000(^3) bytes</td>
</tr>
<tr>
<td>1 terabyte (TB)</td>
<td>1,000 GB or 1,000(^4) bytes</td>
</tr>
<tr>
<td>1 petabyte (PB)</td>
<td>1,000 TB or 1,000(^5) bytes</td>
</tr>
<tr>
<td>1 exabyte (EB)</td>
<td>1,000 PB or 1,000(^6) bytes</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Logical capacity unit</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 block</td>
<td>512 bytes</td>
</tr>
<tr>
<td>1 KB</td>
<td>1,024 (2^{10}) bytes</td>
</tr>
<tr>
<td>1 MB</td>
<td>1,024 KB or 1,024(^2) bytes</td>
</tr>
<tr>
<td>1 GB</td>
<td>1,024 MB or 1,024(^3) bytes</td>
</tr>
<tr>
<td>1 TB</td>
<td>1,024 GB or 1,024(^4) bytes</td>
</tr>
<tr>
<td>1 PB</td>
<td>1,024 TB or 1,024(^5) bytes</td>
</tr>
<tr>
<td>1 EB</td>
<td>1,024 PB or 1,024(^6) bytes</td>
</tr>
</tbody>
</table>

**Accessing product documentation**

Product user documentation is available on the Hitachi Data Systems Portal: [https://portal.hds.com](https://portal.hds.com). 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 Portal](https://portal.hds.com) is the destination for technical support of your current or previously-sold storage systems, midrange and enterprise servers, and combined solution offerings. The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week. If you need technical support, log on to the Hitachi Data Systems Support Portal for contact information: [https://portal.hds.com](https://portal.hds.com)

[Hitachi Data Systems Community](https://community.hds.com) is a new global online community for HDS customers, partners, independent software vendors, employees, and prospects. It is an open discussion among these groups about the HDS portfolio of products and services. It is the destination to get answers, discover insights, and make connections. The HDS Community complements our existing Support Portal and support services by providing an area where
you can get answers to non-critical issues and questions. **Join the conversation today!** Go to [community.hds.com](http://community.hds.com), register, and complete your profile.

**Comments**

Please send us your comments on this document to [doc.comments@hds.com](mailto: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!**
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 (HCSM) management software and the resources that the software manages.

About Hitachi Compute Systems Manager

Hitachi Compute Systems Manager (HCSM), 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 HCSM in an environment that uses HCS products, you can centrally manage and operate storage and server resources. If you install HCSM on the same server where HCS is installed, the server automatically synchronizes information for hosts managed by HCSM 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 HCSM from a management client.
• Configure the HCSM system settings by using the HCSM user interface.
• Manage HCSM users by using an external authentication server.
• Use common HCS functionality to centrally manage HCS settings for users and security.

Related concepts
• About Hitachi Compute Systems Manager components on page 19
• About Hitachi Compute Systems Manager managed resources on page 18
• About basic system configuration on page 20
• About Hitachi Compute Systems Manager LAN configuration on page 21

About Hitachi Compute Systems Manager managed resources

Hitachi Compute Systems Manager (HCSM) 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 HCSM management system. After you add a target to the system, it becomes a managed host (server-specific) or managed resource (generic). HCSM manages the following resources:
• Windows, Linux, and Solaris hosts
  HCSM manages both physical and virtual Windows, Linux, and Solaris hosts.
• Hypervisors
HCSM manages both Hyper-V and VMware.
- Virtual machines (VMs)
  HCSM 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
  HCSM manages LPARs at the blade server level.

Related concepts
- About Hitachi Compute Systems Manager on page 18
- About basic system configuration on page 20

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 21

About Hitachi Compute Systems Manager components

Hitachi Compute Systems Manager (HCSM) consists of the following components:
- Management server
  The management server is a computer where the HCSM software is installed and runs. The HCSM management system consists of the following components:
  ○ Hitachi Command Suite (HCS) Common Component
    Provides functionality common to HCS products and related to users and security.
  ○ HCSM server
    Provides central management and operation of remote resources.
- Management clients
  A management client is a computer that runs either the HCSM 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 HCSM 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 18
- About basic system configuration on page 20

About basic system configuration

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

![Basic System Configuration Diagram]

The basic system configuration environment is set up as follows:
- HCSM is installed as a standalone product without any additional Hitachi Command Suite (HCS) products.
- Users are managed with HCSM instead of an external authentication server.
- Communication between management servers and management clients does not use SSL for secure communications.

Related concepts
- About Hitachi Compute Systems Manager LAN configuration on page 21
About Hitachi Compute Systems Manager LAN configuration

When using Hitachi Compute Systems Manager (HCSM), 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 (HCSM) is a part of the Hitachi Command Suite (HCS) 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

If you install HCSM on the same server as other HCS products, you can use common settings to manage users and security. In addition, if HCSM 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 HCSM and Hitachi Device Manager, not information for other types of resources.

Related concepts
- About Hitachi Compute Systems Manager on page 18

Hitachi Compute Systems Manager overview workflow

The following figure illustrates an overview workflow, which includes installing, configuring, and using Hitachi Compute Systems Manager (HCSM).
This manual includes system installation, setup, management, and maintenance information. For details about managing resources, see the *Hitachi Compute Systems Manager User Guide*.

**Related concepts**

- [Installation workflow](#) on page 23
- [Post-installation workflow](#) on page 23
- [SNMP trap setup workflow](#) on page 25
- [Managed host setup workflow](#) on page 25
- [Workflow for setting up secure communication with managed servers](#) on page 29
- [Workflow for setting up secure communication with management clients](#) on page 27
- [Workflow for setting up secure communication with an SMTP server](#) on page 28
- [Workflow for setting up secure communication with an LDAP directory server](#) on page 29
- [Workflow for setting up a Kerberos authentication server](#) on page 31
- [Database management workflow](#) on page 34
- [Workflow for setting up an LDAP directory server](#) on page 30
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 (HCSM).

![Installation Workflow Diagram]

Related concepts

- [Post-installation workflow](#) on page 23
- [Managed host setup workflow](#) on page 25
- [About installing Hitachi Compute Systems Manager](#) on page 47
- [About verifying system prerequisites](#) on page 40

Post-installation workflow

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

- About Hitachi Compute Systems Manager post-installation tasks on page 53
- Managed host setup workflow on page 25

Related tasks

- Verifying access to the management server on page 53
- Registering a license on page 54
- Changing the System account password on page 55
- Setting an e-mail address for the System account on page 55
- Setting up e-mail notifications on page 56
- Setting up the alert level for e-mail notifications on page 56
- Adding resources to Hitachi Compute Systems Manager on page 57
System configuration workflows

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

SNMP trap setup workflow

To enable HCSM 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 (HCSM).
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:
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.

![Workflow Diagram for Setting Up Secure Communication]

**Related tasks**
- Setting up SSL on the server for secure client communication on page 111
- Setting up SSL on web-based management clients on page 117
- Setting up SSL on management clients running the CLI on page 118

**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 HCSM user interface.

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

![Workflow Diagram for Setting up Secure Communication with SMTP Server]

**Related concepts**
- About using an external authentication server on page 128

**Related tasks**
- Setting up SSL for communicating with the SMTP server on page 120
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 HCSM, you can create a new self-signed certificate on the server and enable it from the HCSM 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 110

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 125

Related tasks

- Configuring SSL for a secure LDAP server connection on page 135

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 an HCSM 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 HCSM 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 HCSM authentication.
Workflow for setting up a Kerberos authentication server

To set up a Kerberos server for authentication, you must register an HCSM user account and specify connection settings on the management server and the HCSM interface.

The following figure illustrates the basic workflow for setting up a Kerberos server for HCSM authentication.
Related concepts

- [About using an external authentication server](#) on page 128

Related tasks

- [Configuring a Kerberos server connection](#) on page 138
- [Verifying a Kerberos server connection](#) on page 139

**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 HCSM.

Deployment Manager can only be used when the management server is running Windows.
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 (HCSM) management server to a different server, you must install HCSM 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.
Database management workflow

When using Hitachi Compute Systems Manager (HCSM), 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 HCSM database.
Related concepts

- About database management on page 171

Related tasks

- Backing up the database on page 172
- Exporting the database on page 175
- Restoring the database on page 174
- Importing the database on page 176

Workflow for updating the network configuration

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

The following figure illustrates the basic workflow for updating the management server after you implement network configuration changes.
When using Hitachi Compute Systems Manager (HCSM), if the system does not function properly, you might have to troubleshoot HCSM.

The following figure illustrates the basic workflow for troubleshooting HCSM.

**Troubleshooting workflow**

- 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 78
- Backing up the database on page 172

**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 78
- Backing up the database on page 172
Related concepts

- [Troubleshooting overview](#) on page 222
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 (HCSM), 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 Hitachi 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 43

Related tasks

• Verifying the system prerequisites on page 40
• Avoiding port conflicts on page 40
• Verifying the server time setting on page 42
• Adding the management server host name to the hosts file (Linux) on page 41
• Configuring kernel parameters and shell restrictions (Linux) on page 41
• Registering firewall exceptions (Linux) on page 42

Verifying the system prerequisites

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

Related concepts

• About verifying system prerequisites on page 40

Avoiding port conflicts

Before a new installation of HCSM, verify that the ports that HCSM to use 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:** HCSM uses the 162 UDP port to receive SNMP traps. If a product other than HCSM 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 HCSM 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 40

**Related references**
- [Hitachi Compute Systems Manager server ports](#) on page 252
- [Hitachi Command Suite Common Component ports](#) on page 252

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

Before you install HCSM 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 40

**Configuring kernel parameters and shell restrictions (Linux)**

Before you install HCSM 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 40
Registering firewall exceptions (Linux)

Use the text mode setup utility to specify registered port number exceptions.

Related concepts
• About verifying system prerequisites on page 40

Related tasks
• Registering management server firewall exceptions (Linux) on page 85

Verifying the server time setting

All HCSM task and alert occurrence times are based on the HCSM management server time setting. Therefore, it is important that you verify the accuracy of the server OS time setting and reset it if necessary before installing HCSM. If you change the HCSM server time while the Hitachi Command Suite (HCS) Common Component and HCS product services are running, HCSM 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 HCSM 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. HCSM cannot support the new DST rules unless the server provides support.

Related concepts
• About verifying system prerequisites on page 40

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 81
Verifying the installation environment

This module provides information about verifying the HCSM server environment and recording required information before installation.

Related concepts

• About verifying the installation environment on page 43

Related tasks

• Preparing the installation directories on page 45
• Specifying management server information during installation on page 47

Related references

• Rules for specifying path names on page 44

About verifying the installation environment

During the Hitachi Compute Systems Manager (HCSM) 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:

• HCSM 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 HCSM. 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

• HCSM 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 HCSM in an environment in which a Hitachi Command Suite product has already been configured)
  In Windows:
  `HCSM-installation-folder\ComputeSystemsManager_backup`
  When installing HCSM 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 HCSM on a server already running another Hitachi Command Suite (HCS) 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 47
- [Preparing the installation directories](#) on page 45

Related references
- [Rules for specifying path names](#) on page 44

Rules for specifying path names

During new HCSM 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 HCSM 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.
    - 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 43

Related tasks
- Preparing the installation directories on page 45

Preparing the installation directories

During new HCSM installations, the installation wizard prompts you for the HCSM installation directory and the HCSM 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 HCSM on a machine that is already running another Hitachi Command Suite (HCS) product, the installation program installs the HCS Common Component in the same location as the existing HCS product regardless of whether you change the HCSM 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.
   - HCSM software:
     Windows default:
     \Program-Files-folder\HiCommand
     Linux default:
     /opt/HiCommand
   - HCSM 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 HCSM 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 HCSM 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 43

Related references
- [Rules for specifying path names](#) on page 44
Specifying management server information during installation

During new HCSM 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 OS. When specifying the host name, ensure that the name does not exceed 128 characters. 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 43

Installing Hitachi Compute Systems Manager

This module provides information about installing HCSM from different types of media.

Related concepts
- About installing Hitachi Compute Systems Manager on page 47

Related tasks
- Installing the software (Windows) on page 48
- Installing the software (Linux) on page 51
- Installing from the integrated media by using the all-in-one installer (Windows) on page 50

About installing Hitachi Compute Systems Manager

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

If you purchase Hitachi Compute Systems Manager as a component of another HCS product, you install the product from integrated installation media for Windows by using the all-in-one installer. The all-in-one installer installs HCSM along with the following products:
- Hitachi Device Manager
- Hitachi Tiered Storage Manager
- Hitachi Replication Manager
- Hitachi Tuning Manager
- Hitachi Storage Navigator Modular 2

You cannot use the all-in-one installer to install into a cluster environment or 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 HCSM installer instead and specify an IP address.

The HCSM installation types are as follows:

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

The procedure for installing HCSM is the same for all installation types except for an upgrade from version 7.x.

Note: If you install HCSM in an environment in which a virus scanning program is running, you must change the virus scanning program settings after installation.

Related concepts

- [About upgrading the HCSM software](#) on page 290

Related tasks

- [Installing the software (Windows)](#) on page 48
- [Installing the software (Linux)](#) on page 51
- [Installing from the integrated media by using the all-in-one installer (Windows)](#) on page 50

Related references

- [Setting requirements for virus scanning program settings](#) on page 52

**Installing the software (Windows)**

If you purchased HCSM with another Hitachi Command Suite product, install the software from the integrated product DVD. If you purchased Hitachi Compute System Manager (HCSM) as a separate component, install HCSM from the standalone media.
Note: If you want to install other HCS 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 HCS 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 HCSM 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 HCSM system.

9. Click Finish.

Note:
- If HCSM 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
HCSM is now installed and DCOM is enabled.

Related concepts
• About installing Hitachi Compute Systems Manager on page 47

Related tasks
• Installing Deployment Manager on page 161

Related references
• Setting requirements for virus scanning program settings on page 52

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

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

⚠️ Note: If you want to install other HCS 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. Ensure that the host name consists of only alphanumeric characters (A-Z, a-z, 0-9), periods (.), or hyphens (-).
3. If the server is running any products that use the Hitachi Command Suite 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 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.
6. In the Installation window, click All-in-One Installer.
7. In the Select Products window, select Hitachi Compute Systems Manager.
8. Follow the on-screen instructions and enter the required information.
9. 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.

10. Click Finish.

**Related concepts**
- About installing Hitachi Compute Systems Manager on page 47

**Related references**
- Setting requirements for virus scanning program settings on page 52

**Installing the software (Linux)**

Before installing HCSM 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 HCSM:

**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 HCS 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 was automatically mounted, unmount it.
3. Mount the installation media.
   - You can specify the following characters for the mount path of the installation media:
     - A-Z a-z 0-9 _ /

**Note:** Do not specify the noexec option.

4. Move to the installation directory:
5. Run the `./install.sh` command to install HCSM.

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

6. Enter the required information when prompted.

**Related concepts**
- [About installing Hitachi Compute Systems Manager](#) on page 47

**Related tasks**
- [Verifying access to the management server](#) on page 53

**Related references**
- [Setting requirements for virus scanning program settings](#) on page 52

## 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 47
Post-installation tasks

This module provides information about required HCSM 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 (HCSM), you must complete the following post-installation tasks:

- Verify access to the HCSM 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 HCSM 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 53
- Registering a license on page 54
- Changing the System account password on page 55
- Setting an e-mail address for the System account on page 55
- Setting up e-mail notifications on page 56
- Setting up the alert level for e-mail notifications on page 56
- Adding resources to Hitachi Compute Systems Manager on page 57
- Creating a server administrator account on page 58
- Creating resource groups on page 59
- Creating user groups and setting up access control on page 59
- Completing the initial setup on page 60

Verifying access to the management server

After you install HCSM, 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 HCSM.
3. Check the browser settings and modify them as required. For details about browser settings, see the Hitachi Compute Systems Manager User Guide.

4. In the address bar, specify the HCSM 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 Hitachi 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 53

Registering a license
You must register plug-in licenses to use specific functions of HCSM.

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 HCSM license key displays in the License window.

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

Related concepts
- About Hitachi Compute Systems Manager post-installation tasks on page 53

Changing the System account password

If you installed HCSM in an environment in that no other Hitachi Command Suite (HCS) 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 HCS 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 Compute Systems Manager User Guide.

Related concepts
- About Hitachi Compute Systems Manager post-installation tasks on page 53

Setting an e-mail address for the System account

Before Hitachi Compute Systems Manager (HCSM) can send e-mail notifications about HCSM system operations to the System, 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, then click OK.

Result

The System account e-mail address is set up.

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

Related concepts

• About Hitachi Compute Systems Manager post-installation tasks on page 53

Setting up e-mail notifications

Before HCSM can send e-mail notifications when HCSM alerts occur or when an HCSM 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 HCSM Administration tab System Settings option. For details about setting up e-mail notification, see the Hitachi Compute Systems Manager User Guide.

Related concepts

• About Hitachi Compute Systems Manager post-installation tasks on page 53

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.
The e-mail notification alert level is set up.

You can also set e-mail notification alert levels by using the HCSM Administration tab Automated Event Handling option. For details about setting the alert level for e-mail notifications, see the *Hitachi Compute Systems Manager User Guide*.

**Related concepts**
- [About Hitachi Compute Systems Manager post-installation tasks](#) on page 53

**Related tasks**
- [Setting up e-mail notifications](#) on page 56

### Adding resources to Hitachi Compute Systems Manager

Before you begin using HCSM to manage resources, set up the management targets and then add them to HCSM.

**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 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 HCSM on a management server that is running the Hitachi Command Suite (HCS) Device Manager component, all existing hosts that meet HCSM management target requirements are automatically imported into HCSM as managed hosts. This applies only to discovered hosts, not other discovered resources.

Related concepts

- About Hitachi Compute Systems Manager post-installation tasks on page 53

Related references

- Prerequisites for managing Windows hosts on page 89
- Prerequisites for managing Linux or Solaris hosts on page 96

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 HCSM Administration tab.

Creating a server administrator account

As part of the initial setup, create a server administrator account for managing HCSM. 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 Compute Systems Manager User Guide.

Related concepts

- About Hitachi Compute Systems Manager post-installation tasks on page 53
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 HCSM Administration tab Resource Groups option. For details about creating resource groups, see the Hitachi Compute Systems Manager User Guide.

Related tasks

- Creating a server administrator account on page 58
- Adding resources to Hitachi Compute Systems Manager on page 57

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 HCSM Administration tab User Groups option. For details about creating user groups and setting up access control, see the *Hitachi Compute Systems Manager User Guide*.

**Related tasks**

- [Changing the System account password](#) on page 55
- [Creating a server administrator account](#) on page 58

**Completing the initial setup**

Before you can view managed resource information using HCSM, you must complete the initial setup of the HCSM 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 HCSM to manage resources.

**Related concepts**

- [About Hitachi Compute Systems Manager post-installation tasks](#) on page 53

**Removing Hitachi Compute Systems Manager**

This module provides information about removing HCSM.

**About removing Hitachi Compute Systems Manager**

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

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

In Windows, you can remove HCSM 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
Note: Hitachi Storage Navigator Modular 2 cannot be removed by using the all-in-one uninstaller. You must remove Hitachi Storage Navigator Modular 2 individually.

If you use the all-in-one uninstaller, all HCS product files are removed.

If you remove HCSM only, the properties files, database files, log files, and other HCSM-related files are deleted. The files and directories that are not deleted when HCSM 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 62
- [Removing the software (Linux)] on page 63
- [Removing the software by using the all-in-one uninstaller (Windows)] on page 63

Related references

- [Prerequisites for removing the software] on page 61

Prerequisites for removing the software

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

Before removing the HCSM 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 HCSM 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 60

Related tasks
- Removing the software (Windows) on page 62

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

⚠️ Note: If you remove HCSM, 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 HCSM software is removed from the server.

Related concepts
- About removing Hitachi Compute Systems Manager on page 60

Related tasks
- Removing the software by using the all-in-one uninstaller (Windows) on page 63

Related references
- Prerequisites for removing the software on page 61
Removing the software by using the all-in-one uninstaller (Windows)

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

**Note:** If you remove HCS 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 HCS software is removed from the server.

**Related concepts**
- [About removing Hitachi Compute Systems Manager](#) on page 60

**Related references**
- [Prerequisites for removing the software](#) on page 61

Removing the software (Linux)

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

**Note:** If you remove HCSM, 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 HCSM software is removed from the management server.
Related concepts

- [About removing Hitachi Compute Systems Manager](#) on page 60

Related references

- [Prerequisites for removing the software](#) on page 61
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 (HCSM) 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 HCSM 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 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 HCSM.
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 HCSM.

**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 166
   • [Stopping Hitachi Compute Systems Manager](#) on page 167

---

**About monitoring inband SNMP traps**

If you want HCSM 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 HCSM management server.

Configuring HCSM to monitor inband driver traps consists of the following tasks:

• Configuring managed hosts to send SNMP traps
• Configuring the HCSM 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 94
• [Configuring a Linux host to send SNMP inband traps (optional)](#) on page 104
• [Configuring a Solaris host to send SNMP inband traps (optional)](#) on page 106
Configuring the management server to receive inband SNMP traps

Before HCSM 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 HCSM 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 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 94
- Configuring a Linux host to send SNMP inband traps (optional) on page 104
- Configuring a Solaris host to send SNMP inband traps (optional) on page 106
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 (HCSM), 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 HCSM, 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 HCSM 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 (HCS) products along with HCSM, the settings you specify for HCSM apply to all HCS user accounts.

---

Related tasks

- [Enabling System account locking](#) on page 69
- [Unlocking user accounts](#) on page 70

---

**Enabling System account locking**

When you install HCSM, 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 (HCS) Common Component properties file as follows:
   
   - In Windows:
     
     \`HCS-Common-Component-installation-folder\conf\user.conf\`
   
   - In Linux
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 271

Unlocking user accounts
You can unlock user accounts other than your own by using the HCSM 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 Compute Systems Manager User Guide.

Procedure
1. Start HCSM.
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 170
- Starting Hitachi Compute Systems Manager on page 166

Changing management server system settings
This module provides information about changing Hitachi Compute Systems Manager (HCSM) management server system settings.

Changing Hitachi Compute Systems Manager port numbers
This module provides information about changing Hitachi Compute Systems Manager (HCSM) port numbers.

HCS properties requiring updates for port number changes
After modifying the HCSM port numbers, you must update the Hitachi Command Suite (HCS) common component properties listed in the following table:

<table>
<thead>
<tr>
<th>Port Number (default)</th>
<th>Properties File Path (HCS Common Component installation directory)</th>
<th>Location to Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>22015/TCP</td>
<td>In Windows: \uCPSB\httpsd\conf\user_httpsd.conf</td>
<td>Listen</td>
</tr>
<tr>
<td></td>
<td>In Linux: /uCPSB/httpsd/conf/user_httpsd.conf</td>
<td>Listen [::]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>#Listen 127.0.0.1:</td>
</tr>
<tr>
<td>22016/TCP</td>
<td>In Windows: \uCPSB\httpsd\conf\user_httpsd.conf</td>
<td>host-name:port-number in the &lt;VirtualHost&gt; tag</td>
</tr>
<tr>
<td></td>
<td>In Linux: /uCPSB/httpsd/conf/user_httpsd.conf</td>
<td>Listen</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Listen [::]:</td>
</tr>
<tr>
<td>22027/TCP</td>
<td>In Windows: \uCPSB\CC\web\redirector\workers.properties</td>
<td>worker.ComputeSystemsManagerWebService.port</td>
</tr>
<tr>
<td></td>
<td>In Linux: /uCPSB/CC/web/redirector/ workers.properties</td>
<td></td>
</tr>
<tr>
<td>Port Number (default)</td>
<td>Properties File Path (HCS Common Component installation directory)</td>
<td>Location to Edit</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>In Windows: \uCPSB\CC\web\containers \ComputeSystemsManagerWebService\usrconf \usrconf.properties In Linux: /uCPSB/CC/web/containers/ ComputeSystemsManagerWebService/usrconf/ usrconf.properties</td>
<td>webserver.connector.ajp13.port</td>
<td></td>
</tr>
<tr>
<td>22028/TCP</td>
<td>In Windows: \uCPSB\CC\web\containers \ComputeSystemsManagerWebService\usrconf \usrconf.properties In Linux: /uCPSB/CC/web/containers/ ComputeSystemsManagerWebService/usrconf/ usrconf.properties</td>
<td>webserver.shutdown.port</td>
</tr>
<tr>
<td>22031/TCP</td>
<td>In Windows: \uCPSB\httpsd\conf\user_hsso_httpsd.conf In Linux: /uCPSB/httpsd/conf/user_hsso_httpsd.conf</td>
<td>Listen</td>
</tr>
<tr>
<td>22032/TCP</td>
<td>In Windows: \HDB\CONF\emb\HiRDB.ini In Linux: /HDB/CONF/emb/HiRDB.ini In Windows: \HDB\CONF\pdsys In Linux: /HDB/CONF/pdsys In Windows: \database\work\def_pdsys In Linux: /database/work/def_pdsys</td>
<td>PDNAMEPORT pd_name_port pd_name_port</td>
</tr>
<tr>
<td>22033/TCP</td>
<td>In Windows: \uCPSB\CC\web\redirector \workers.properties In Linux:</td>
<td>worker.HBase64StgMgmtSSOSer vice.port</td>
</tr>
</tbody>
</table>
### Related tasks
- **Changing Hitachi Compute Systems Manager ports** on page 74

#### HCSM properties requiring updates for port number changes

After modifying the HCSM port numbers, you must update the HCSM properties listed in the following table:

<table>
<thead>
<tr>
<th>Port Number (default)</th>
<th>Properties File Path (HCSM installation directory)</th>
<th>Location to Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>162/UDP or 22601/UDP</td>
<td>ComputeSystemsManager\conf \user.properties</td>
<td>snmp.trap.receive.port</td>
</tr>
<tr>
<td></td>
<td>ComputeSystemsManager/conf/ \user.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ComputeSystemsManager/ conf/ \user.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: The default is 162/UDP. If 162/UDP is in use for another product, 22601/UDP becomes the default.</td>
<td></td>
</tr>
<tr>
<td>22610/TCP</td>
<td>ComputeSystemsManager\conf \user.properties</td>
<td>server.rmi.port</td>
</tr>
<tr>
<td></td>
<td>ComputeSystemsManager/conf/ \user.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux: ComputeSystemsManager/ conf/ \user.properties</td>
<td></td>
</tr>
</tbody>
</table>

---

---

**Configuring the management server**

73

Hitachi Compute Systems Manager Installation and Configuration Guide
Changing Hitachi Compute Systems Manager ports

You can change the port numbers used for HCSM after installation if necessary.

**Procedure**

1. Stop HCSM.
2. Edit the HCSM properties or the HCS Common Component properties.
3. Start HCSM.
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 HCSM.

**Related tasks**

- [Changing Hitachi Compute Systems Manager ports](#) on page 74
- [Starting Hitachi Compute Systems Manager](#) on page 166
- [Stopping Hitachi Compute Systems Manager](#) on page 167

**Related references**

- [HCS properties requiring updates for port number changes](#) on page 71
- [HCSM properties requiring updates for port number changes](#) on page 73
- [Hitachi Compute Systems Manager server ports](#) on page 252
- [Hitachi Compute Systems Manager server properties files](#) on page 256
- [Hitachi Command Suite Common Component ports](#) on page 252
Changing the management server host name or IP address

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

You can change the host name or IP address of the management server after installing HCSM.

The management server host name cannot exceed 128 characters and is case-sensitive.

Procedure

1. Ensure that you have a record of the new management server host name and IP address.
   If you need to verify the host name on a Windows machine, use the `ipconfig /ALL` command to display the host name.
2. To change the IP address, first unmanage all the chassis.
3. Stop HCSM.
5. If the OS of the management server is Linux and if 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. Write the new host name into the line above the `localhost` line.
6. If you are also using other HCS products, revise the settings for these products as needed.
7. Change the IP address or the host name of the management server, then restart the computer.
8. Verify that all HCSM services are running.
9. If you use the old host name or IP address to access the management server from a browser, update the HCSM URL.
10. Verify that you can access HCSM using the new URL.
11. If you changed the IP address, you must access the chassis resource list and change the status from unmanaged back to managed.
12. 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 78
- Starting Hitachi Compute Systems Manager on page 166
- Stopping Hitachi Compute Systems Manager on page 167

Related references
- HCS properties requiring changes for management server host name changes on page 76
- HCS properties requiring changes for management server IP address changes on page 77
- Properties files for Hitachi Command Suite Common Component on page 260
- Hitachi Compute Systems Manager server properties files on page 256

HCS properties requiring changes for management server host name changes

After modifying the host name of the management server, you must update the HCS common properties listed in the following table:

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

<table>
<thead>
<tr>
<th>Properties File Path (HCS Common Component installation directory)</th>
<th>Properties</th>
<th>Required Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Windows: \uCPSB\httpsd\conf\user_httpsd.conf</td>
<td>ServerName</td>
<td>Change the value to the new host name.</td>
</tr>
<tr>
<td>In Linux: /uCPSB/httpsd/conf/user_httpsd.conf</td>
<td>&lt;VirtualHost&gt; tag</td>
<td>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 (*).</td>
</tr>
<tr>
<td></td>
<td>Servername in the &lt;VirtualHost&gt; tag</td>
<td>If TLS or SSL is used for communication between the management server and management clients, change the value to the new host name.</td>
</tr>
<tr>
<td>In Windows: \HDB\CONF\pdsys \database\work\def_pdsys</td>
<td>the -x option of pdunit</td>
<td>Change the value to the loopback address 127.0.0.1.</td>
</tr>
<tr>
<td>In Linux: /HDB/CONF/pdsys</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Properties File Path (HCS Common Component installation directory)

<table>
<thead>
<tr>
<th>Properties File Path</th>
<th>Properties</th>
<th>Required Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>/database/work/def_pdsys</td>
<td>pd_hostname</td>
<td></td>
</tr>
<tr>
<td>In Windows: \HDB\CONF\pdutsys \database\work\def_pdsys</td>
<td>PDHOST</td>
<td></td>
</tr>
<tr>
<td>In Linux: /HDB/CONF/pdutsys /database/work/def_pdsys</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 260

**HCS properties requiring changes for management server IP address changes**

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

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

Properties File Path (HCS Common Component installation directory)

<table>
<thead>
<tr>
<th>Properties File Path</th>
<th>Properties</th>
<th>Required Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Windows: \uCP5B\httpsd\conf \user_httpsd.conf</td>
<td>ServerName</td>
<td>Change the value to the new host name or new IP address.</td>
</tr>
<tr>
<td>In Linux: /uCP5B/httpsd/conf/ user_httpsd.conf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In Windows: \HDB\CONF\pdutsys \database\work\def_pdsys</td>
<td>the -x option of pdunit</td>
<td>If the old IP value is specified, change the value to the loopback address 127.0.0.1.</td>
</tr>
</tbody>
</table>
## 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 HCSM management server URL if you change the management server host name or IP address, the HCSM ports, or any SSL settings. If HCSM runs on the same management server as other Hitachi Command Suite (HCS) products, you can change all the HCS 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:

---

### Related tasks

- [Changing the management server host name or IP address](#) on page 75
If you still want to change the URL, go to the next step.

2. Change only the HCSM 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 HCS HCSM 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 HCSM using the new URL.

Related references
• Configuration changes that require updating the management server URL on page 80

Configuration changes that require updating the management server URL
You must update the URL that you use to access HCSM 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 78

Using a different Oracle JDK version
You can change the version of Oracle™ JDK that you use with HCSM after installation if necessary. Refer to the release notes for supported Oracle JDK versions.

Procedure
1. Stop HCSM.
2. To change the Oracle JDK version, use the following command:
   • In Windows:
     HCS-Common-Component-installation-folder\bin\hcmds64chgdjdk
   • In Linux:
     HCS-Common-Component-installation-directory/bin/hcmds64chgdjdk
3. Within the window that opens, select the JDK version to use.
4. Start HCSM.
5. If you use TLS or SSL communication, you must re-import the following certificates on the management server:
   - Server certificate for HCS Common Component and a certificate from a certificate authority
   - Server certificate for HCSM 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 HCSM.

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 166
- Stopping Hitachi Compute Systems Manager on page 167
- Setting up SSL on the server for secure client communication on page 111
- Setting up SSL on web-based management clients on page 117
- Setting up SSL on management clients running the CLI on page 118
- Configuring SSL for a secure LDAP server connection on page 135

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 reset the server time setting manually after installing HCSM. 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 HCSM 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 HCSM task schedules and alert times are accurate.

Procedure

1. Stop HCSM.
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 HCSM Management server reflects the correct time.

Postrequisites

Note: When running HCSM 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. HCSM cannot support the new DST rules unless the server provides support.

Related references

- Conditions that require resetting the management server time setting on page 81

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 HCSM.
2. Open the user.properties file:
   - In Windows:
     HCSM-installation-folder\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 HCSM.

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 257

Changing the Hitachi Compute Systems Manager temperature measurement unit

You can change the temperature measurement unit that is displayed in the HCSM user interface. This is the unit that is used for measuring the temperature of managed resources. HCSM 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 HCSM.
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 HCSM.
Result
The temperature measurement unit is updated.

Related references
• Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 257

Registering management server firewall exceptions (Windows)

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

Note: If Windows firewall is enabled before you install HCSM, the HCSM 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 HCSM.

Result
HCSM can now access the required resources through Windows firewall.

Related tasks
• Configuring a firewall for Windows Server 2003 hosts on page 90
• Configuring a firewall for Windows Server 2008 or Windows Server 2012 hosts on page 91

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 registered 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 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)](page 85)

### 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 HCSM in an environment in which the firewall is enabled.
- You enable the firewall after installing HCSM.

#### 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 is displayed.
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 HCSM.
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 HCSM.

**Related tasks**

- [Enabling WinRM on Windows hosts](#) on page 92
- [Starting Hitachi Compute Systems Manager](#) on page 166
- [Stopping Hitachi Compute Systems Manager](#) on page 167

**Related references**

- [Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties)](#) on page 257
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 (HCSM) controls the power functions on managed hosts based on the host lights-out-management (LOM) information. If the host uses Wake-on-LAN (WoL), HCSM 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, HCSM can power on the host using WoL. If you want HCSM 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 89
- [Prerequisites for managing Linux or Solaris hosts](#) on page 96

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 HCSM. When Alive Monitor is running, LOM errors are reported to the host so that HCSM 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 89
- Prerequisites for managing a Hitachi rack-mounted server on page 89

Prerequisites for managing a Hitachi blade server

Before you can manage Hitachi blade servers using HCSM, 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 Hitachi Compute Systems Manager 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 HCSM, 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 Hitachi Compute Systems Manager 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 HCSM, 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 HCSM target hosts.
- The Windows host runs a version of the Windows operating system that is supported by HCSM.
• 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 HCSM to monitor performance data. If Quality of Service Packet Scheduler is enabled, HCSM 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 90
• Configuring a firewall for Windows Server 2008 or Windows Server 2012 hosts on page 91
• Enabling DCOM for Windows hosts on page 92
• Enabling WinRM on Windows hosts on page 92
• Setting up a remote connection with UAC on Windows Server 2008 or Windows Server 2012 on page 93
• Installing the fcinfo tool on Windows Server 2003 (optional) on page 94
• Enabling Wake-on-LAN on page 88
• Configuring a Windows host to send SNMP inband traps (optional) on page 94

Configuring a firewall for Windows Server 2003 hosts

Before HCSM 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 HCSM can communicate with the host.

Related references
• Prerequisites for managing Windows hosts on page 89

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

Before HCSM 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 HCSM can communicate with the host.
Related references

- Prerequisites for managing Windows hosts on page 89

Enabling DCOM for Windows hosts

Before HCSM 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 HCSM can obtain server management information.

Related references

- Prerequisites for managing Windows hosts on page 89

Enabling WinRM on Windows hosts

By enabling Windows Remote Management (WinRM), HCSM 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)](page 86)

Related references

• [Prerequisites for managing Windows hosts](page 89)

---

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

Before HCSM 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 89

Installing the fcinfo tool on Windows Server 2003 (optional)

If you want HCSM 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 HCSM 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
HCSM is now able to obtain HBA information for managed SAN resources.

Related references
• Prerequisites for managing Windows hosts on page 89

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

If you want HCSM 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 HCSM the 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 HCSM server, and then click **Add**.
   
   e. If the port number of the HCSM 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:

   ```bash
   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 HCSM 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 89
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 HCSM, 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 HCSM target hosts.
- Host runs a version of the Linux or Solaris OS that is supported by HCSM.
- Linux hosts are running the `sysstat` package. This package is required if you want to use HCSM to monitor performance data about physical disks.

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 HCSM.
- Permit access for the HCSM 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 99

Related tasks

- [Setting up an account on the Linux or Solaris host for use with Hitachi Compute Systems Manager](#) on page 97
- [Verifying the Linux or Solaris files and directories](#) on page 96
- [Setting up an IP connection with a Linux or Solaris host](#) on page 98
- [Setting up root user access for a Linux or Solaris host](#) on page 99
- [Setting up permission for normal users to use the su command with Linux or Solaris hosts](#) on page 100
- [Setting up permission for normal users to use the Linux sudo command](#) on page 101
- [Configuring a Linux host to send SNMP inband traps (optional)](#) on page 104
- [Enabling Wake-on-LAN](#) on page 88

Verifying the Linux or Solaris files and directories

Before HCSM 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 96

Setting up an account on the Linux or Solaris host for use with Hitachi Compute Systems Manager

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

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 account creation command. (adduser for Linux hosts or useradd for Solaris hosts).

2. Set up empty initialization scripts for the HCSM account as follows:
   • For bash: /etc/profile, ~/.bash_profile, ~/.bashrc
   • For tcsh: /etc/csh.login, /etc/csh.cshrc, ~/.login, ~/.cshrc

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 99
Setting up an IP connection with a Linux or Solaris host

Before HCSM 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 OS, 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 Linux hosts: /etc/rc.d/init.d/sshd restart
   For Solaris hosts: 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 96
About permissions for logging into a Linux or Solaris managed host

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

When using HCSM, 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 the Linux or Solaris host for use with Hitachi Compute Systems Manager on page 97
- Setting up an IP connection with a Linux or Solaris host on page 98
- Setting up root user access for a Linux or Solaris host on page 99
- Setting up permission for normal users to use the su command with Linux or Solaris hosts on page 100
- Setting up permission for normal users to use the Linux sudo command on page 101
- Setting up permission for normal users to use the Solaris pfexec command on page 103

Setting up root user access for a Linux or Solaris host

Before HCSM can communicate with a Linux or Solaris host using the SSH protocol, you must set up login access. If you want HCSM 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 HCSM 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 Compute Systems Manager User Guide*.

### Result

HCSM 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 su command with Linux or Solaris hosts](#) on page 100
- [Setting up permission for normal users to use the Linux sudo command](#) on page 101

### Related references

- [Prerequisites for managing Linux or Solaris hosts](#) on page 96

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

Before HCSM 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 HCSM management server:
   - IP address: host IP address
   - Port number: host SSH port number
   - User name: normal user ID
   - Password: normal user password
   - su Password: root user password

   For details about how to set up managed hosts using the HCSM interface, see the *Hitachi 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 99

**Related tasks**

- Setting up root user access for a Linux or Solaris host on page 99
- Setting up permission for normal users to use the Linux `sudo` command on page 101

**Related references**

- Prerequisites for managing Linux or Solaris hosts on page 96

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

Before HCSM 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-ID managed-host-name =NOPASSWD: /usr/sbin/dmidecode
   
   normal-user-ID managed-host-name =NOPASSWD: /usr/sbin/smartctl
   
   normal-user-ID managed-host-name =NOPASSWD: /sbin/ethtool
   
   normal-user-ID managed-host-name =NOPASSWD: /sbin/shutdown
   
   For Red Hat Linux, Oracle Linux and SUSE Linux 11 SP1 only, also add:
   
   normal-user-ID managed-host-name =NOPASSWD: /usr/sbin/exportfs
   
   For SUSE Linux only, also add:
   
   normal-user-ID managed-host-name =NOPASSWD: /bin/cat
   
   normal-user-ID 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 HCSM management server:
   - IP address: host IP address
   - Port number: host SSH port number
   - User name: normal user ID
   - Password: normal user password
   - su Password: blank

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

Result

Normal users can now log in to the Linux host and use the sudo command.
Setting up permission for normal users to use the Solaris \texttt{pfexec} command

Before HCSM 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 \texttt{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.

\textbf{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 \texttt{su} command.

To set up normal users to log in and use the \texttt{pfexec} command:

\textbf{Procedure}

1. Add the following profile definition to the \texttt{/etc/security/prof_attr}:
   \begin{verbatim}
   HCSM::::
   \end{verbatim}

2. Add the following execution-rights definitions to \texttt{/etc/security/exec_attr}:
   \begin{verbatim}
   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
   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
   \end{verbatim}
3. Execute the following command to apply the profile definition to a normal user:
   ```bash
   usermod -p HCSM ID-of-normal-user
   ```

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 HCSM management server:
   - IP address: host IP address
   - Port number: host SSH port number
   - User name: normal user ID
   - Password: normal user password
   - su Password: blank

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

   **Related concepts**
   - [About permissions for logging into a Linux or Solaris managed host](#) on page 99

   **Related tasks**
   - [Setting up an account on the Linux or Solaris host for use with Hitachi Compute Systems Manager](#) on page 97
   - [Setting up an IP connection with a Linux or Solaris host](#) on page 98

   **Related references**
   - [Prerequisites for managing Linux or Solaris hosts](#) on page 96

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

If you want HCSM 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 6.2 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 HCSM server, **community-name** is a proper SNMP community name, and optional **port-number** is the port number of the HCSM server trap listening port. If the port number of the HCSM 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 HCSM 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 HCSM 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:
• 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 HCSM server
   • community-name is a proper SNMP community name
   • port-number is the port number of the HCSM server trap listening port (optional). If the port number of the HCSM 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 HCSM 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 Compute Systems Manager User Guide*.

**Related tasks**

- [Adding resources to Hitachi Compute Systems Manager](#) on page 57

### 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 Compute Systems Manager User Guide*.
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
- 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 (HCSM) network communication. SSL or TLS enable HCSM 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.

HCSM 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 an external authentication server (LDAP directory server)
- Communication between the management server and management targets

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

Note: When you use HCSM 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 HCSM because users might not be able to connect to it.

Related concepts
- About secure communications for management clients on page 110
- About secure communications for the SMTP server on page 119

Related tasks
- Setting up SSL on the server for secure client communication on page 111
- Setting up SSL on web-based management clients on page 117
- Setting up SSL on management clients running the CLI on page 118
- Setting up SSL on web-based management clients on page 117
- Configuring SSL for a secure LDAP server connection on page 135

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 (HCSM) 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 111
- [Setting up SSL on web-based management clients](#) on page 117
- [Setting up SSL on management clients running the CLI](#) on page 118

**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 HCSM.
- 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 HCSM.
2. To create a private key (httpsdkey.pem), a certificate signing request
   (httpsd.csr), and a self-signed certificate (httpsd.pem) for the HCS
   Common Component, use the following command:
   - In Windows:
     
     ```
     HCS-Common-Component-installation-folder\bin
     \hcmds64ssltool /key HCS-Common-Component-installation-
     folder\uCPSB\httpsd\ssl\bin\demoCA\httpsdkey.pem /csr HCS-
     ```
In Linux:

```
HCS-Common-Component-installation-directory/bin/hcmds64ssltool -key HCS-Common-Component-installation-directory/uCPSB/httpsd/sslc/bin/demoCA/httpsd.key.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, HCSM.
- 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.
5. Stop HCSM.

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

      #</VirtualHost>

   with the exception of #SSLCA CertificateFile, 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 SSLv3 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
SSLPProtocol SSLv3 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 HCSM.

10. Update the HCSM 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 HCSM server.

Related concepts
- About secure communications for management clients on page 110

Related tasks
- Setting up SSL on web-based management clients on page 117
- Setting up SSL on management clients running the CLI on page 118
- Closing the non-SSL communication port on page 115

Related references
- Properties related to web server communication including SSL settings (user_httpsd.conf) on page 263

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 HCSM.

6. Verify that you can log in to the Hitachi Compute Systems Manager user
   interface.

Related concepts

- [About secure communications for management clients](#) on page 110

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 HCSM management clients
that access the HCSM 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 110

Related tasks

- Setting up SSL on the server for secure client communication on page 111
- Setting up SSL on management clients running the CLI on page 118

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 HCSM 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 HCSM server certificate that is stored in the following directory to a temporary directory on the HCSM 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 HCSM CLI host, import the HCSM server certificate to the truststore (cacerts) using the following command:

   - In Windows:
     jre-installation-folder\bin\keytool -importcert -trustcacerts -alias hcsm -file user-specified-folder\server-certificate-file -keystore jre-installation-folder\lib\security\cacerts -storepass changeit
   - In Linux:

     where 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 HCSM server location, use the following command:
• In Windows:
  `\csm configure`

• In Linux:
  `/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 110

**Related tasks**

- [Setting up SSL on the server for secure client communication](#) on page 111
- [Setting up SSL on web-based management clients](#) on page 117

### 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 119
- [About secure communications for management clients](#) on page 110

### 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 (HCSM) 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 110
- [About Hitachi Compute Systems Manager security settings](#) on page 110

**Related tasks**

- [Setting up SSL for communicating with the SMTP server](#) on page 120
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 issuing the following command:
   - In Windows:
     `HCS-Common-Component-installation-folder\bin\hcmds64keytool -import -alias hcsm -file SMTP-certificate-file (PEM-format-or-DER-format) -keystore HCS-Common-Component-installation-folder\uCPSB\jdk\jre\lib\security\jssecacerts -storepass hicommand`
   - In Linux:
     `HCS-Common-Component-installation-directory/uCPSB/jdk/bin/keytool -import -alias hcsm -file SMTP-certificate-file (PEM-format-or-DER-format) -keystore HCS-Common-Component-installation-directory/uCPSB/jdk/jre/lib/security/jssecacerts -storepass hicommand`
3. Restart HCSM.
4. From a management client, use a browser to log in to HCSM.
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 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 119
- About secure communications for management clients on page 110
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 (HCSM) 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 HCSM user interface.

Strengthening security for managed server alert communication

To increase the level of security for alert communications sent from a Hitachi 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 HCSM.
2. Create a new keystore using the following command:
   - **In Windows:**
     
     ```
     HCS-Common-Component-installation-folder\bin\hcmand64\keytool
     -genkey -keystore HCSM-installation-folder
     \ComputeSystemsManager\conf\ssl\keystore-file-name -storepass
     keystore-password -keystore-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 -keystore-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\hcmand64\keytool
     -certreq -file certificate-signing-request-file-name -keystore
     HCSM-installation-folder\ComputeSystemsManager\conf\ssl\keystore-file-name
     -storepass keystore-password -keystore-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 -keystore-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\hcmand64\keytool
     -import -file certificate-file-of-certificate-authority -
• In Linux:
  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 certificate-file-of-certificate-authority -keystore HCSM-installation-directory\ComputeSystemsManager\conf\ssl/keystore-file-name -storepass keystore-password -alias unique-name-in-keystore
• In Linux:
  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:
  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 HCSM.

13. From a management client, log in to HCSM and enable the new keystore. For details, see the Hitachi Compute Systems Manager User Guide.

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

In Windows:

```
HCS-Common-Component-installation-folder\bin\hcms64keytool -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:

```
```

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 125

About setting up secure communication for an external authentication server

Use the StartTLS protocol to implement secure communication between the Hitachi Compute Systems Manager (HCSM) 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 121

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 125

About restricting management client access to Hitachi Compute Systems Manager

You can increase Hitachi Compute Systems Manager (HCSM) security by controlling access to the HCSM 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 125

Restricting management server access from a management client

You can control access to the HCSM management server by restricting management client access. By default, all clients can access the HCSM
management server. You can configure the HCSM 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 HCSM on a management client that is not registered in the `user_httpsd.conf` file, you cannot start the HCSM GUI from the management client GUI.

To restrict management clients from accessing the management server:

**Procedure**

1. Stop HCSM.
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.
5. Start HCSM.

**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 125

**Related references**

- [Properties related to web server communication including SSL settings (user_httpsd.conf)](#) on page 263
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 (HCSM).

About using an external authentication server

When using Hitachi Command Suite (HCS) 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 HCSM, you can use the same user IDs to log in to HCSM. This means that you do not have to manage login passwords and control accounts in HCSM. HCSM 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 128
- Workflow for setting up an LDAP directory server on page 30

Related tasks

- Configuring an LDAP server connection on page 133

About using an external authorization server

If you use both an external authentication server and an external authorization server for your Hitachi Command Suite (HCS) products, you can control users' access permissions for HCSM 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 HCSM manages users by authenticating groups on the external authorization server. Set up access to the external authorization server by configuring a connection between HCSM and an LDAP directory server.

Related concepts

- About using an external authentication server on page 128
- Workflow for setting up an LDAP directory server on page 30
Related tasks

- Configuring an LDAP server connection on page 133

LDAP directory server data structure models

This module provides conceptual information about LDAP directory server data structure models, which determine the HCSM 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.

![Flat model diagram]

Legend: The user 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 an HCSM user (for example, the Windows logon ID).
• The RDN attribute value of a user ID entry includes a character that is invalid in an HCSM 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 HCSM. Therefore, if the RDN attribute value of a user entry includes an invalid HCSM 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 130
• LDAP data structure Base DN on page 131

Related tasks
• Prerequisites for determining LDAP server connection properties on page 132

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).
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 HCSM 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 HCSM are in this hierarchy.

**Related concepts**
- [LDAP server flat data structure model](#) on page 129
- [LDAP data structure Base DN](#) on page 131

**Related tasks**
- [Prerequisites for determining LDAP server connection properties](#) on page 132
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 HCSM 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 130
- [LDAP server flat data structure model](#) on page 129
- [LDAP data structure Base DN](#) on page 131

Related tasks

- [Configuring an LDAP server connection](#) on page 133

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 133
Related references

- Settings for using DNS to connect to an LDAP server on page 141
- Settings for connecting directly to an LDAP server and an authorization server on page 142

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 HCSM, 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 HCSM. If not, you must register an HCSM 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 HCSM. Specify a maximum of 256 characters using the following valid characters:
     0 to 9, A to Z, a to z, ! # $ % & ' ( ) * + - . = @ \ ^ _ |
   - In HCSM, 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 HCSM 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 HCSM 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:
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 HCSM implementation:
   - If HCSM connects to an external authentication server only, use the HCSM user interface to create user accounts, specify access control settings for management targets, and optionally, change the user authentication method for existing users.
   - If HCSM connects to an external authorization server in addition to an authentication server, use the HCSM user interface to register authorization groups and permissions.

   For details and step-by-step procedures for all of these options, see the *Hitachi Compute Systems Manager User Guide*.

Result
The HCSM management server is now connected to an external LDAP directory server for authentication.

Related tasks
- [Prerequisites for determining LDAP server connection properties](#) on page 132
- [Verifying an LDAP server connection](#) on page 136
- [Configuring SSL for a secure LDAP server connection](#) on page 135

Related references
- [Prerequisites for using a DNS server to connect to an LDAP server](#) on page 132
- [Prerequisites for registering a search user](#) on page 150
- [Settings for connecting directly to an LDAP server](#) on page 140
- [Settings for using DNS to connect to an LDAP server](#) on page 141
- [About using commands to connect to an external authentication server](#) on page 147
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 HCSM 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 HCSM 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 HCSM services. Other changes do not require restarting the services.
4. To determine whether the LDAP directory server certificate has already been set up for HCS Common Component, use the following command:
   - In Windows:
     ```
     HCS-Common-Component-installation-folder\bin\hcmandkeytool 
     -list -v keystore HCS-Common-Component-installation-folder 
     \uCPB\jdk\jre\lib\security\cacerts -storepass password-for accessing-truststore
     ```
   - In Linux:
     ```
     HCS-Common-Component-installation-directory/uCPB/jdk/bin/ 
     keytool -list -v keystore HCS-Common-Component- 
     installation-directory/uCPB/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 Common Suite (HCS) Common Component truststore.
7. Import the LDAP directory server certificate to the Hitachi Command Suite (HCS) truststore by using the following command:
   - In Windows:
     ```
     HCS-Common-Component-installation-folder\bin\hcmandkeytool 
     -import -alias unique-name-in-the-truststore -file
     ```
Certificate import and truststore configuration:

- **In Linux:**
  ```bash
  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:**
     ```bash
     HCS-Common-Component-installation-folder\bin\hcms64keytool
     -list -v -keystore truststore-filename -storepass password-
     for-accessing-truststore
     ```
   - **In Linux:**
     ```bash
     HCS-Common-Component-installation-directory/uCPSB/jdk/bin/
     keytool -list -v -keystore truststore-filename -storepass
     password-for-accessing-truststore
     ```

9. Restart HCSM.

**Result**

The HCSM management server now connects to an external LDAP directory server using a secure connection.

**Related tasks**

- Configuring an LDAP server connection on page 133
- Verifying an LDAP server connection on page 136

**Related references**

- Prerequisites for configuring a secure LDAP server connection on page 153
- Settings for connecting directly to an LDAP server on page 140
- Settings for connecting directly to an LDAP server and an authorization server on page 142
- Command format for registering a search user on page 151
- Command format for importing LDAP server certificates on page 154

**Verifying an LDAP server connection**

After you complete the required steps for configuring a connection with an LDAP server, you can use the `hcms64checkauth` 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 HCSM.

Related tasks

• Configuring an LDAP server connection on page 133
• Configuring SSL for a secure LDAP server connection on page 135

Related references

• Command format for verifying an external server connection on page 148

Connecting to a Kerberos server

This section explains how to use Kerberos with HCSM.

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:

```plaintext
auth.kerberos.default_tkt_enctypes=rc4-hmac
```

**Configuring a Kerberos server connection**

When using HCSM, 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. Identify the Kerberos server data structure model (hierarchical or flat). The property settings differ depending on the model type.
2. 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.
3. Verify that there is a registered user account on the Kerberos server for use with HCSM. If not, you must register an HCSM 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 HCSM. Specify a maximum of 256 characters using the following valid characters:
     0 to 9, A to Z, a to z, ! $ % & ’ ( ) * + - . = @ \ ^ _ |
   • In HCSM, 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 HCSM management server, edit the properties in the `exauth.properties` file to set up the Kerberos server connection parameters.

```plaintext
HCS-Common-Component-installation-directory\conf\exauth.properties
```
5. If the Kerberos server uses a hierarchical data structure or HCSM 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-componen-cent-installation-folder\bin
  \hc_md64ldapuser /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

6. Select one of the following options for configuring user accounts and permissions based on your HCSM implementation:

- If HCSM connects to an external authentication server only, use the HCSM user interface to create user accounts, specify access control settings for management targets, and optionally, change the user authentication method for existing users.

- If HCSM connects to an external authorization server in addition to an authentication server, use the HCSM user interface to register authorization groups and permissions.

For details and step-by-step procedures for all of these options, see the Hitachi Compute Systems Manager User Guide.

Result

The HCSM management server is now connected to an external Kerberos server for authentication.

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 HCSM.

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 HCSM management server. The following table lists the property values required for an implementation where you connect the HCSM management server directly to an LDAP directory server (connecting only to an external authentication server).

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>ldap</td>
</tr>
<tr>
<td>auth.server.name</td>
<td>Server identification name of the LDAP server</td>
</tr>
<tr>
<td>auth.group.mapping</td>
<td>false</td>
</tr>
<tr>
<td>auth.ocsp.enable</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>To use StartTLS communication, change the setting as required.</td>
</tr>
<tr>
<td>auth.ocsp.responderURL</td>
<td>(empty space)</td>
</tr>
<tr>
<td></td>
<td>To use StartTLS communication, change the setting as required.</td>
</tr>
<tr>
<td>auth.ldap.ServerName.protocol</td>
<td>ldap</td>
</tr>
<tr>
<td></td>
<td>To use StartTLS communication, change the setting to tls.</td>
</tr>
<tr>
<td>auth.ldap.ServerName.host</td>
<td>Host name or IP address of the LDAP server</td>
</tr>
<tr>
<td>Property</td>
<td>Setting Details</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>auth.ldap.ServerName.port</td>
<td>Port number of the LDAP server</td>
</tr>
<tr>
<td>auth.ldap.ServerName.timeout</td>
<td>Amount of time to wait before an LDAP directory server connection time-out</td>
</tr>
<tr>
<td>auth.ldap.ServerName.attr</td>
<td>Name of the attribute that defines the user ID value included in the certificate</td>
</tr>
<tr>
<td>auth.ldap.ServerName.basedn</td>
<td>DN (Base DN)</td>
</tr>
<tr>
<td>auth.ldap.ServerName.retry.interval</td>
<td>Retry interval when LDAP server communication fails</td>
</tr>
<tr>
<td>auth.ldap.ServerName.retry.times</td>
<td>Number of times to retry a connection when LDAP server communication fails</td>
</tr>
<tr>
<td>auth.ldap.ServerName.retry.dns_lookup</td>
<td>false</td>
</tr>
</tbody>
</table>

**Related tasks**
- [Configuring an LDAP server connection](#) on page 133

**Related references**
- [Properties related to LDAP directory server connections (exauth.properties)](#) on page 272
- [Example properties file for external LDAP directory server connections (exauth.properties)](#) on page 276

**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 HCSM management server. The following table lists the property values required for an implementation where you connect the HCSM management server to an LDAP directory server using DNS (connecting only to an external authentication server).

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>ldap</td>
</tr>
<tr>
<td>auth.server.name</td>
<td>Server identification name of the LDAP server</td>
</tr>
<tr>
<td>auth.group.mapping</td>
<td>false</td>
</tr>
<tr>
<td>auth.ldap.ServerName.protocol</td>
<td>ldap</td>
</tr>
<tr>
<td>auth.ldap.ServerName.timeout</td>
<td>Amount of time to wait before an LDAP directory server connection time-out</td>
</tr>
<tr>
<td>auth.ldap.ServerName.attr</td>
<td>Name of the attribute that defines the user ID value included in the certificate</td>
</tr>
<tr>
<td>auth.ldap.ServerName.basedn</td>
<td>DN (Base DN)</td>
</tr>
</tbody>
</table>
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 HCSM management server. The following table lists the property values required for an implementation where you connect the HCSM management server directly to an LDAP directory server and to an external authorization server.

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>ldap</td>
</tr>
<tr>
<td>auth.server.name</td>
<td>Server identification name of the LDAP server</td>
</tr>
<tr>
<td>auth.group.mapping</td>
<td>true</td>
</tr>
<tr>
<td>auth.ocsp.enable</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>To use StartTLS communication, change the setting as required.</td>
</tr>
<tr>
<td>auth.ocsp.responderURL</td>
<td>(empty space)</td>
</tr>
<tr>
<td></td>
<td>To use StartTLS communication, change the setting as required.</td>
</tr>
<tr>
<td>auth.ldap.ServerName.protocol</td>
<td>ldap</td>
</tr>
</tbody>
</table>
To use StartTLS communication, change the setting to tls.

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.ldap.ServerName.host</td>
<td>Host name or IP address of the LDAP server</td>
</tr>
<tr>
<td>auth.ldap.ServerName.port</td>
<td>Port number of the LDAP server</td>
</tr>
<tr>
<td>auth.ldap.ServerName.timeout</td>
<td>Amount of time to wait before an LDAP directory server connection time-out</td>
</tr>
<tr>
<td>auth.ldap.ServerName.attr</td>
<td>Name of the attribute that defines the user ID value included in the certificate</td>
</tr>
<tr>
<td>auth.ldap.ServerName.basedn</td>
<td>DN (Base DN)</td>
</tr>
<tr>
<td>auth.ldap.ServerName.retry.interval</td>
<td>Time interval for retries when LDAP server communication fails</td>
</tr>
<tr>
<td>auth.ldap.ServerName.retry.times</td>
<td>Number of times to retry a connection when LDAP server communication fails</td>
</tr>
<tr>
<td>auth.ldap.ServerName.domain.name</td>
<td>Name of the domain managed by the LDAP server</td>
</tr>
<tr>
<td>auth.ldap.ServerName.retry.dns_lookup</td>
<td>false</td>
</tr>
</tbody>
</table>

Related tasks

- [Configuring an LDAP server connection](#) on page 133

Related references

- [Properties related to LDAP directory server connections (exauth.properties)](#) on page 272
- [Example properties file for external LDAP directory server connections (exauth.properties)](#) on page 276

**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 HCSM management server. The following table lists example settings for an implementation where you connect the HCSM management server to an LDAP directory server using DNS and to an external authorization server.

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>ldap</td>
</tr>
<tr>
<td>auth.server.name</td>
<td>Server identification name of the LDAP server</td>
</tr>
<tr>
<td>auth.group.mapping</td>
<td>true</td>
</tr>
<tr>
<td>auth.ldap.ServerName.protocol</td>
<td>ldap</td>
</tr>
</tbody>
</table>
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 HCSM management server. The following table lists the property values required for an implementation where you connect the HCSM management server directly to an Kerberos server (connecting only to an external authentication server).

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>kerberos</td>
</tr>
<tr>
<td>auth.group.mapping</td>
<td>false</td>
</tr>
</tbody>
</table>

Related tasks

- [Configuring an LDAP server connection](#) on page 133

Related references

- [Prerequisites for using a DNS server to connect to an LDAP server](#) on page 132
- [Properties related to LDAP directory server connections (exauth.properties)](#) on page 272
- [Example properties file for external LDAP directory server connections (exauth.properties)](#) on page 276
<table>
<thead>
<tr>
<th>Property</th>
<th>Setting Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.ocsp.enable</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>To use StartTLS communication, change the setting as required.</td>
</tr>
<tr>
<td>auth.ocsp.responderURL</td>
<td>(empty space)</td>
</tr>
<tr>
<td></td>
<td>To use StartTLS communication, change the setting as required.</td>
</tr>
<tr>
<td>auth.kerberos.default_realm</td>
<td>Realm name</td>
</tr>
<tr>
<td>auth.kerberos.dns_lookup_kdc</td>
<td>false</td>
</tr>
<tr>
<td>auth.kerberos.default_tkt_enctypes</td>
<td>Encryption type used for Kerberos authentication</td>
</tr>
<tr>
<td>auth.kerberos.clockskew</td>
<td>Acceptable time difference range between the management server and the Kerberos server</td>
</tr>
<tr>
<td>auth.kerberos.timeout</td>
<td>Amount of time to wait before an Kerberos server connection timeout</td>
</tr>
<tr>
<td>auth.kerberos.realm_name</td>
<td>Realm identifier</td>
</tr>
<tr>
<td>auth.kerberos.auth.kerberos.realm_name-property-value.realm</td>
<td>Realm name</td>
</tr>
<tr>
<td>auth.kerberos.auth.kerberos.realm_name-property-value.kdc</td>
<td>Host name or IP address[:port-number] of the Kerberos server</td>
</tr>
</tbody>
</table>

**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 HCSM management server. The following table lists the property values required for an implementation where you connect the HCSM management server to a Kerberos server using DNS (connecting only to an external authentication server).

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>kerberos</td>
</tr>
<tr>
<td>auth.group.mapping</td>
<td>false</td>
</tr>
<tr>
<td>auth.kerberos.default_realm</td>
<td>Realm name</td>
</tr>
<tr>
<td>auth.kerberos.dns_lookup_kdc</td>
<td>true</td>
</tr>
<tr>
<td>auth.kerberos.default_tkt_enctypes</td>
<td>Encryption type used for Kerberos authentication</td>
</tr>
<tr>
<td>auth.kerberos.clockskew</td>
<td>Acceptable time difference range between the management server and the Kerberos server</td>
</tr>
<tr>
<td>auth.kerberos.timeout</td>
<td>Amount of time to wait before an Kerberos server connection timeout</td>
</tr>
</tbody>
</table>
**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 HCSM management server. The following table lists the property values required for an implementation where you connect the HCSM management server directly to an Kerberos server and to an external authorization server.

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>kerberos</td>
</tr>
<tr>
<td>auth.group.mapping</td>
<td>true</td>
</tr>
<tr>
<td>auth.kerberos.default.realm</td>
<td>Realm name</td>
</tr>
<tr>
<td>auth.kerberos.dns_lookup_kdc</td>
<td>false</td>
</tr>
<tr>
<td>auth.kerberos.clockskew</td>
<td>Acceptable range for the time difference between the management server and the Kerberos server.</td>
</tr>
<tr>
<td>auth.kerberos.timeout</td>
<td>Amount of time to wait before the Kerberos server connection times out.</td>
</tr>
<tr>
<td>auth.ocsp.enable</td>
<td>false</td>
</tr>
<tr>
<td>auth.ocsp.responderURL</td>
<td>(empty space)</td>
</tr>
<tr>
<td>auth.kerberos.realm_name</td>
<td>Realm identifier</td>
</tr>
<tr>
<td>auth.kerberos.auth.kerberos.realm_name-</td>
<td>Realm name</td>
</tr>
<tr>
<td>property-value.realm</td>
<td></td>
</tr>
<tr>
<td>auth.kerberos.auth.kerberos.realm_name-</td>
<td>Host name or IP address[:port-number] for the Kerberos server</td>
</tr>
<tr>
<td>property-value.kdc</td>
<td></td>
</tr>
<tr>
<td>auth.group.realm-name.protocol</td>
<td>ldap</td>
</tr>
<tr>
<td>auth.group.realm-name.port</td>
<td>Port number for the Kerberos server</td>
</tr>
<tr>
<td>auth.group.realm-name.basedn</td>
<td>DN (BaseDN)</td>
</tr>
<tr>
<td>auth.group.realm-name.timeout</td>
<td>Waiting time to connect to the LDAP directory server</td>
</tr>
<tr>
<td>auth.group.realm-name.retry.interval</td>
<td>Time interval for retries when LDAP directory server communication fails</td>
</tr>
<tr>
<td>auth.group.realm-name.retry.times</td>
<td>Number of retries for failed connections with the LDAP directory server</td>
</tr>
</tbody>
</table>
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 HCSM management server. The following table lists example settings for an implementation where you connect the HCSM management server to an Kerberos server using DNS and to an external authorization server.

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>kerberos</td>
</tr>
<tr>
<td>auth.group.mapping</td>
<td>true</td>
</tr>
<tr>
<td>auth.kerberos.default_realm</td>
<td>Realm name</td>
</tr>
<tr>
<td>auth.kerberos.dns_lookup_kdc</td>
<td>true</td>
</tr>
<tr>
<td>auth.kerberos.clockskew</td>
<td>Acceptable time difference range between the management server and the Kerberos server</td>
</tr>
<tr>
<td>auth.kerberos.timeout</td>
<td>Amount of time to wait before a Kerberos server connection timeout.</td>
</tr>
</tbody>
</table>

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 133
• Configuring a Kerberos server connection on page 138

Related references
• Command format for verifying an external server connection on page 148

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 147
• [Settings for connecting directly to an LDAP server](#) on page 140
• [Settings for connecting directly to a Kerberos server](#) on page 144
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`.
- 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 HCSM 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 152
Before registering a user account for searching user information using the `hcmsg64ldapuser` command, review the command format guidelines for creating the user account.

The format of the `hcmsg64ldapuser` command is as follows:

- **In Windows:**
  
  ```
  HCS-Common-Component-installation-folder\bin\hcmsg64ldapuser /set /dn LDAP-search-user-account [/pass LDAP-search-user-account-password] /name server-identification-name
  ```

- **In Linux:**
  
  ```
  HCS-Common-Component-installation-directory/bin/hcmsg64ldapuser -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.

- **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`

Note: If the DN contains one or more commas, such as in `cn=administrator,cn=admin,dc=example,com`, specify the DN as follows:

  ```
  hcmsg64ldapuser /set /dn "cn=administrator,cn=admin,dc=example,com" /pass administrator_pass /name Server-Name
  ```
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 133
- [Configuring a Kerberos server connection](#) on page 138
- [Deleting an LDAP search user](#) on page 153

**Related references**
- [Prerequisites for registering a search user](#) on page 150

**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:**
Deleting an LDAP search user

To delete an LDAP search user account, use the following command on the management server:

- In Windows:
  
  ```bash
  HCS-Common-Component-installation-folder\bin\hcmds64ldapuser /delete /name server-identification-name
  ```

- In Linux:
  
  ```bash
  HCS-Common-Component-installation-directory/bin/hcmds64ldapuser -delete -name server-identification-name
  ```

Related tasks

- Configuring SSL for a secure LDAP server connection on page 135

Related references

- Command format for registering a search user on page 151

**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 the 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 133

**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 (HCS) 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 135

Related references
- Prerequisites for configuring a secure LDAP server connection on page 153
- Command format for importing LDAP server certificates on page 154

**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 135

Related references
- Prerequisites for configuring a secure LDAP server connection on page 153
- Rules for importing LDAP directory server certificates on page 154
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
- Prerequisites for installing Deployment Manager
- Installing Deployment Manager
- Prerequisites for using Deployment Manager
- Configuring managed resources for use with Deployment Manager
- Changing the Deployment Manager port number
- Editing Deployment Manager properties and settings files when changing ports
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 HCSM installation wizard to upgrade, overwrite, or remove Deployment Manager.

**Related tasks**

- [Installing Deployment Manager](#) on page 161
- [Configuring managed resources for use with Deployment Manager](#) on page 162
- [Changing the Deployment Manager port number](#) on page 162
- [Verifying the system prerequisites](#) on page 40

**Related references**

- [Prerequisites for installing Deployment Manager](#) on page 158

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 159
- Installing .NET Framework for Deployment Manager on page 160

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.
2. Depending on the IIS version, you must also complete the following:
   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.
   For IIS 7.5 or later, 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
      • IIS 6 Metabase Compatibility
      • IIS Management Console

Related concepts

- About Deployment Manager environment settings on page 158

Related references

- Prerequisites for installing Deployment Manager on page 158
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 Server 2008 R2, run the following command to install the software:
     `DVD-drive:\HCSM_SERVER\HCSM\DPMMEDIA\dotNetFramework40\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 HCSM installation program to install Deployment Manager. The Deployment Manager installation is included within the main HCSM installation.

   Note: If Deployment Manager is already installed, the removal option is available.

2. Follow the online prompts to install Deployment Manager.
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 HCSM.

When you finish the Deployment Manager installation, you are returned to the main HCSM 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 162

Related references

- Prerequisites for installing Deployment Manager on page 158

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 161

---

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 158

---

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 HCSM, 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 HCSM.
  2. In the properties file, change the Deployment Manager port number.
  3. Start HCSM.

Related concepts

- [About Deployment Manager environment settings](#) on page 158

Related references

- [Editing Deployment Manager properties and settings files when changing ports](#) on page 163

**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:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BackupRestoreUnicast</td>
<td>This port is used for managed resource disk backup and restoration.</td>
</tr>
<tr>
<td></td>
<td>The default value is 26501.</td>
</tr>
<tr>
<td></td>
<td>If an attempt to change this port number fails, the system uses the default value 56020/tcp.</td>
</tr>
<tr>
<td>BOOTNIC</td>
<td>This port is used for managed resource PXE booting.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>The default value is 26502. If an attempt to change this port number fails, the system uses the default value 56022/tcp.</td>
</tr>
<tr>
<td>FSC</td>
<td>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.</td>
</tr>
<tr>
<td>FTUnicast</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Port number</th>
<th>Location to edit</th>
</tr>
</thead>
</table>
| 26500/tcp   | `<Port>port-number-to-change</Port>`  
For example: `<Port>26500</Port>` |

Related tasks
- [Changing the Deployment Manager port number](#) on page 162

Related references
- [Properties related to Deployment Manager ports (port.ini)](#) on page 287
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 (HCSM), which is required for many administrative tasks.

About starting and stopping Hitachi Computer Systems Manager

When you start a machine where you installed Hitachi Compute Systems Manager (HCSM), HCSM starts automatically. At the same time, other Hitachi Command Suite (HCS) products are also started.

To change the HCSM settings, you must manually stop and start HCSM. You can choose whether to stop and start HCSM only, or stop and start HCSM in addition to all other HCS products.

Related tasks

- Starting Hitachi Compute Systems Manager on page 166
- Stopping Hitachi Compute Systems Manager on page 167
- Checking the status of Hitachi Compute Systems Manager services on page 170

Related references

- Hitachi Compute Systems Manager services and processes on page 168

Starting Hitachi Compute Systems Manager

You can start HCSM from the Windows desktop or from the command line.

To start HCSM 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 HCSM from the command line, use the following command:

```
HCS-Common-Component-installation-folder\bin\hcmds64srv /start
```

To start HCSM from the Linux command line, enter the following command:

```
HCS-Common-Component-installation-directory/bin/hcmds64srv -start
```

The HCSM services start. Other HCS products installed on the same machine, including HCS common component, also start.

Related concepts

- About starting and stopping Hitachi Computer Systems Manager on page 166
Stopping Hitachi Compute Systems Manager

You can stop HCSM from the Windows desktop or from the command line.

**Note:** You must stop all HCS services before making configuration changes. Therefore, do not stop only the HCSM service unless there is a specific reason to do so (for example, when troubleshooting an issue).

In Windows:

To stop HCSM 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 HCSM from the command line, use the following command:
  ```
  HCS-Common-Component-installation-folder\bin\hcmds64srv /stop /server ComputeSystemsManagerWebService
  ```

In Linux:

To stop HCSM from the command line, use the following command:

```
HCS-Common-Component-installation-directory/bin/hcmds64srv -stop
```

To stop only HCSM but not other Hitachi Command Suite products, use the following command:

```
HCS-Common-Component-installation-directory/bin/hcmds64srv -stop -server ComputeSystemsManagerWebService
```

Only the HCSM service stops.

**Related concepts**

- About starting and stopping Hitachi Computer Systems Manager on page 166

**Related tasks**

- Starting Hitachi Compute Systems Manager on page 166
- Checking the status of Hitachi Compute Systems Manager services on page 170
Hitachi Compute Systems Manager services and processes

When viewing HCSM status or messages, the system displays information for the Windows HCSM services and processes listed in the following table:

<table>
<thead>
<tr>
<th>Process name</th>
<th>Service Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cjstartweb.exe</td>
<td>HCS Compute Systems Manager Web Service</td>
<td>Hitachi Compute Systems Manager servlet service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>hcmdssvctl.exe</td>
<td>HBase 64 Storage Mgmt SSO Service</td>
<td>Hitachi Command Suite servlet service for single sign-on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>httpsd.exe</td>
<td>HBase 64 Storage Mgmt Web Service</td>
<td>Hitachi Command Suite common web service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multiple instances of this process might be running.</td>
</tr>
<tr>
<td>httpsd.exe</td>
<td>HBase 64 Storage Mgmt Web SSO Service</td>
<td>Hitachi Command Suite common web service for single sign-on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multiple instances of this process might be running.</td>
</tr>
<tr>
<td>rotatelogs.exe</td>
<td>None.</td>
<td>Log partitioning utility for web services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multiple instances of this process might be running.</td>
</tr>
<tr>
<td>hntr2mon.exe</td>
<td>Hitachi Network Objectplaza Trace Monitor 2</td>
<td>Hitachi Command Suite common trace information collection.</td>
</tr>
<tr>
<td></td>
<td>Hitachi Network Objectplaza Trace Monitor 2 (x64)</td>
<td>(Integrated trace information is collected.)</td>
</tr>
<tr>
<td>hntr2srv.exe</td>
<td>None.</td>
<td>Hitachi Command Suite common trace service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(This service processes events from the Services window.)</td>
</tr>
<tr>
<td>pdservice.exe</td>
<td>HiRDB/EmbeddedEdition_HD1</td>
<td>Database process server server control.</td>
</tr>
</tbody>
</table>

When viewing HCSM Deployment Manager status or messages, the system displays information for the services and processes listed in the following table:
<table>
<thead>
<tr>
<th>Process name</th>
<th>Service Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apiserv.exe</td>
<td>DeploymentManager APIService</td>
<td>Deployment Manager Common Component service</td>
</tr>
<tr>
<td>bkressvc.exe</td>
<td>DeploymentManager Backup/Restore Management</td>
<td>Backup/restore task execution service</td>
</tr>
<tr>
<td>depssvc.exe</td>
<td>DeploymentManager Get Client Information</td>
<td>Deployment Manager service for collecting information from the target server</td>
</tr>
<tr>
<td>pxesvc.exe</td>
<td>DeploymentManager PXE Management</td>
<td>Network (PXE) boot control service</td>
</tr>
<tr>
<td>pxemtftp.exe</td>
<td>DeploymentManager PXE Mtftp</td>
<td>TFTP server functionality</td>
</tr>
<tr>
<td>rupdssvc.exe</td>
<td>DeploymentManager Remote Update Service</td>
<td>Deployment Manager service for executing remote updates for the target server</td>
</tr>
<tr>
<td>schwatch.exe</td>
<td>DeploymentManager Schedule Management</td>
<td>Schedule management service</td>
</tr>
<tr>
<td>ftsvc.exe</td>
<td>DeploymentManager Transfer Management</td>
<td>File transfer service</td>
</tr>
<tr>
<td>sqlservr.exe</td>
<td>SQL Server (DPMDBI)</td>
<td>Database service</td>
</tr>
<tr>
<td>sqlagent.exe</td>
<td>SQL Server Agent (DPMDBI)</td>
<td>Database job management service</td>
</tr>
</tbody>
</table>

Note: This service is registered during the Deployment Manager installation, but it does not run as a resident process.

When viewing HCSM status or messages, the system displays information for the Linux HCSM processes listed in the following table:

<table>
<thead>
<tr>
<th>Process name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cjstartweb</td>
<td>Hitachi Compute Systems Manager servlet service.</td>
</tr>
<tr>
<td>hcs_csm</td>
<td>Hitachi Command Suite servlet services for single sign-on.</td>
</tr>
<tr>
<td>hcs_hss0</td>
<td>Hitachi Command Suite common web service. Multiple instances of this process might be running.</td>
</tr>
<tr>
<td>httpsd</td>
<td>Hitachi Command Suite common web service for single sign-on. Multiple instances of this process might be running.</td>
</tr>
<tr>
<td>histr2mon</td>
<td>Hitachi Command Suite common trace information collection.</td>
</tr>
</tbody>
</table>

(Integrated trace information is collected.)
<table>
<thead>
<tr>
<th>Process name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pdprcd</td>
<td>Database process server process.</td>
</tr>
</tbody>
</table>

**Related concepts**

- [About starting and stopping Hitachi Computer Systems Manager](#) on page 166

**Related tasks**

- [Checking the status of Hitachi Compute Systems Manager services](#) on page 170

**Checking the status of Hitachi Compute Systems Manager services**

You can check HCSM status from the desktop or from the command line.

**In Windows:**

To check HCSM 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 HCSM from the command line, use the following command:
  
  
  ```
  HCS-Common-Component-installation-folder\bin\hcmds64srv /statusall
  ```

**In Linux:**

To check HCSM 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 HCSM services.

**Related concepts**

- [About starting and stopping Hitachi Computer Systems Manager](#) on page 166

**Related references**

- [Hitachi Compute Systems Manager services and processes](#) on page 168

**Managing the database**

This module provides information about managing the HCSM database.
About database management

Managing the Hitachi Compute Systems Manager (HCSM) database includes maintaining a backup copy of the database. If a database-related failure occurs on the HCSM management server, the system uses the backup to restore the database.

- To back up and restore the HCSM 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 HCSM to another server by exporting the current database and importing it to a new server. When you use HCSM over a long time period, HCSM software upgrades and increases in managed resources might require you to implement servers with higher performance. In this case, you can migrate HCSM 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 HCSM installation directory.
  - Migrate to servers with a more recent HCSM version.

    If you are running more than one Hitachi Command Suite (HCS) product on the same management server as HCSM, 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 HCSM 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.
Prerequisites for database backup

Before you back up the HCSM database, you must create a directory for storing the backup files. When you create the directory, ensure that you follow the HCSM path naming conventions. Also ensure that the directory size is equal to or greater than the required space specified by the following formula:

\[
\text{Database directory required space: } (\text{total-size-of-all-Hitachi-Command-Suite-product-databases-to-back-up} + 4.6\text{GB}) \times 2
\]

where the size of the HCSM 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 171

Related tasks

- **Backing up the database** on page 172

Backing up the database

You must maintain a backup copy of the database so that the 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.
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

To specify the directory for the dir option, use 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 file specified for dir is
empty.

The auto option 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 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 HCSM database.

Postrequisites

⚠️ Note: The system backs up the Hitachi Command Suite (HCS) setting files in
a different location than the database backup directory. If an error occurs in
the management server and you must reinstall the HCS products, use the
backup setting files to obtain the previous settings.

Related concepts
- About database management on page 171

Related tasks
- Restoring the database on page 174

Related references
- Prerequisites for database backup on page 172

Prerequisites for restoring the database

Before you restore the HCSM 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 (HCS) products versions and revisions, including
  the installed HCSM
Installation locations for HCS products including HCSM, 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 171

**Related tasks**
• [Backing up the database](#) on page 172
• [Restoring the database](#) on page 174

**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
     ```

     To specify the file location for the `restore` option, use the absolute path to the database backup file (`backup.hdb`) created by the `hcmds64backups` command.

     HCSM stops automatically.

2. Start HCSM.

**Result**

The HCSM database is now restored.

If other Hitachi Command Suite (HCS) products run on the same host, those products are also restored. If the command restores other HCS products, you might need to complete additional tasks for those products. For details, see the Hitachi Command Suite product documentation.
Prerequisites for database migration

To migrate the HCSM database to another server, export the existing database from the source HCSM server and import it to the target HCSM server.

Before you start the migration process, complete the following prerequisite tasks:

- Verify that the HCSM 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 (HCS) product
  - Database storage directory for the HCS Common Component database (excluding the SYS directory and SYS subdirectories)

Note: HCSM exports databases as archive files. If the total database capacity exceeds 2 GB, the archive file creation fails. In this case, you must manually transfer the exported database data to the migration destination.

Exporting the database

To migrate the HCSM 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. 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 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 you run the `hcmds64dbtrans` command in the preceding format, HCSM will start.

2. For migrations, transfer the exported files to the migration target server.

If the system cannot create an archive file (such as when the total database capacity exceeds 2 GB), manually transfer all files stored in the directory specified for the `workpath` directory option to the migration target server. Do not change the file structure in the directory specified by the `workpath` option.

**Result**

The database is exported. For migration, the exported database is ready for you to import to the target HCSM server.

**Related concepts**

- [About database management](#) on page 171

**Related tasks**

- [Importing the database](#) on page 176

**Related references**

- [Prerequisites for database migration](#) on page 175

**Importing the database**

After you export the HCSM database from an existing server, you can import it to another HCSM 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\hcms64dbtrans /import /workpath working-folder /file archive-file /type {ALL|product-name} /auto
     ```
   - In Linux:
     ```
     HCS-Common-Component-installation-directory/bin/hcms64dbtrans -import -workpath working-directory -file archive-file -type {ALL|product-name} -auto
     ```

   where
   - **working-directory** is the absolute path of a directory in which you want to temporarily store your database information. Ensure that this directory is empty.
   - **archive-file** is the absolute path of the database archive file that you transferred from the original server.
   - **product-name** is the product for which you want to import the database. To import all Hitachi Command Suite (HCS) product databases, specify ALL. To import the HCSM database only, specify HCSM. To import other HCS product databases individually, see the documentation for the applicable Hitachi Command Suite product.
   - **auto** specifies whether 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\hcms64dbtrans /import /workpath working-folder /type {ALL|product-name} /auto
     ```
   - In Linux:
     ```
     HCS-Common-Component-installation-directory/bin/hcms64dbtrans -import -workpath working-directory -type {ALL|product-name} -auto
     ```
where

- **working-directory** is the absolute path of a directory where you want to temporarily store your database information. Ensure that this directory is empty.

- **product-name** is the product whose database you want to import. To import all Hitachi Command Suite (HCS) product databases, specify `ALL`. To import the HCSM database only, specify `HCSM`. To import other HCS product databases individually, see the documentation for the applicable Hitachi Command Suite product.

- **auto** sets whether 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 executing, the Hitachi Command Suite products and the database services are changed to the stop status.

4. Start HCSM 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 HCSM database is now running on the new server.

**Related concepts**

- [About database management](#) on page 171

**Related tasks**

- [Exporting the database](#) on page 175

**Related references**

- [Prerequisites for database migration](#) on page 175
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 and using HCSM in a cluster environment
- HCSM services used in a cluster environment
- Prerequisites for implementing HCSM in a cluster environment
- Installing Hitachi Compute Systems Manager in a cluster environment
- Upgrading Hitachi Compute Systems Manager in a cluster environment
- Migrating Hitachi Compute Systems Manager (HCSM) to a cluster environment
- Configuring HCSM within a cluster environment
- Starting and stopping services in a cluster environment
- Managing the database in a cluster environment
- Removing Deployment Manager from a cluster environment
- Removing the software in a cluster environment
About implementing and using HCSM in a cluster environment

When using Hitachi Compute Systems Manager (HCSM), you can increase reliability by setting up a failover management server using Microsoft clustering services.

When you use HCSM in a cluster environment, you designate one HCSM 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 Windows Server Failover Clustering.

**Related concepts**

• [HCSM services used in a cluster environment](#) on page 181

**Related tasks**

• [Setting up a new instance of HCSM on an active node](#) on page 187
• [Upgrading or overwriting HCSM on an active node](#) on page 193
• [Migrating Hitachi Compute Systems Manager (HCSM) to a cluster environment](#) on page 197
• [Removing Deployment Manager from a cluster environment](#) on page 215

**Related references**

• [Determining which method to use when implementing HCSM in a cluster environment](#) on page 181
• [Verifying the free disk space of a management server in a cluster environment](#) on page 185
• [Checking the cluster environment configuration using the cluster management software](#) on page 186
HCSM services used in a cluster environment

The following list identifies the Hitachi Compute Systems Manager (HCSM) services and Hitachi Command Suite Common Component services that you use to set up and run the HCSM software 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

When using Deployment Manager, you use the following additional services:
- DeploymentManager PXE Management
- DeploymentManager PXE Mtftp
- DeploymentManager Transfer Management

Prerequisites for implementing HCSM in a cluster environment

Before installing or configuring Hitachi Compute Systems Manager (HCSM) in a cluster environment, you must verify that your environment meets all prerequisites. This includes verifying your existing HCSM installation status, verifying required free disk space, and verifying the installation of your other Hitachi Command Suite (HCS) products.

Determining which method to use when implementing HCSM in a cluster environment

The setup process for installing and configuring Hitachi Compute Systems Manager (HCSM) in a cluster environment, differs depending on the management server status and your environment. Before you set up HCSM, 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 and HCSM has not been installed:

<table>
<thead>
<tr>
<th>Executing Node</th>
<th>Standby Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify the prerequisites for using a cluster environment</td>
</tr>
<tr>
<td></td>
<td>Prepare the environment for installation</td>
</tr>
<tr>
<td></td>
<td>Install HCSM</td>
</tr>
<tr>
<td></td>
<td>Change the URL used to access the GUI to point to the logical host name</td>
</tr>
<tr>
<td></td>
<td>Create a cluster settings file</td>
</tr>
<tr>
<td></td>
<td>Configure the services to start manually</td>
</tr>
<tr>
<td></td>
<td>Register resources in the cluster software</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Install HCSM</td>
</tr>
<tr>
<td></td>
<td>Create a cluster settings file</td>
</tr>
<tr>
<td></td>
<td>Configure the services to start manually</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>End</td>
</tr>
</tbody>
</table>
• If the management server is in a cluster environment and HCSM is already installed:
• If the management server is not in a cluster environment:

![Diagram](image)

**Note:** When installing HCSM 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.

**Related concepts**
- [About implementing and using HCSM in a cluster environment](#) on page 180

**Related tasks**
- [Setting up a new instance of HCSM on an active node](#) on page 187
- [Setting up a new instance of HCSM on a standby node](#) on page 190
- [Upgrading or overwriting HCSM on an active node](#) on page 193
- [Upgrading or overwriting HCSM on a standby node](#) on page 195
Setting up a cluster within Windows Server Failover Clustering on page 202
Temporarily stopping HCSM in a cluster environment on page 208
Restarting HCSM in a cluster environment on page 209
Migrating Hitachi Compute Systems Manager (HCSM) to a cluster environment on page 197

Related references
- Verifying the free disk space of a management server in a cluster environment on page 185
- Checking the cluster environment configuration using the cluster management software on page 186

Verifying the free disk space of a management server in a cluster environment

When setting up HCSM in a cluster environment, you must migrate or back up the database to a shared disk.

Before you set up HCSM 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 HCSM)*
  - If you are using Deployment Manager, free space required to migrate image files
  - Free space required to store the work folder used by HCSM

For details about the HCSM work folder, see the description of the hcsm.shared.directory located in the following properties file:
\HCSM-installation-folder\ComputeSystemsManager\conf\user.properties

*The size of the HCSM 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 references
- Determining which method to use when implementing HCSM in a cluster environment on page 181
- Checking the cluster environment configuration using the cluster management software on page 186
Checking the cluster environment configuration using the cluster management software

When setting up HCSM in a cluster environment, you must use the cluster management software to verify the current environment settings and to configure additional settings.

Use the cluster management software to check the following items before setting up HCSM in a cluster environment:

- Check whether a group exists in which other Hitachi Compute Systems Manager product services are registered.
  - If a group in which HCS 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 HCS services are registered exists, use the cluster management software to create a group in which you plan to register the HCSM services.
- 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 references

- Determining which method to use when implementing HCSM in a cluster environment on page 181
- Verifying the free disk space of a management server in a cluster environment on page 185

Installing Hitachi Compute Systems Manager in a cluster environment

This module provides information about installing and configuring a new installation of Hitachi Compute Systems Manager (HCSM) in a cluster environment.
Setting up a new instance of HCSM on an active node

You can complete a new installation of Hitachi Compute Systems Manager (HCSM) on the management server on an active node in a cluster configuration.

Procedure

1. Bring online the cluster management IP address and shared disk.
2. If you created the cluster environment using another Hitachi Command Suite product, use the cluster management software to take offline the Hitachi Command Suite product services and groups in which services are registered. Then disable failover for the same services and groups.
   a. Right-click a service, and then click Properties. On the Policies tab, select do not restart
   b. Right-click the group in which the services are registered, and then click Properties. On the Failover tab, enter 0 for Maximum failures in the specified period.

   For details about services or groups that you must take offline and disable failover, see the documentation for each Hitachi Command Suite product.

   Do not take the following resources offline:
   • Shared disk
   • Cluster management IP address
   • Logical host name
3. Complete a new installation of HCSM on the active node.
   If another Hitachi Command Suite product already exists in the cluster environment, verify the following before installing HCSM:
   • 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 there no other Hitachi Command Suite products exist in the cluster environment, verify the following before installing HCSM:
   • 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.
4. Using the HCSM 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. Change the HCSM URL to access the logical host name.
Verify whether the URL points to the logical host name by using the following command:

```
HCS-Common-Component-installation-folder\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-folder\bin
\hcmds64chgurl /change http://IP-address-or-host-name-of-active-node:port-number http://logical-host-name:port-number
```

5. If you already have an HCS product configured within the cluster, skip to the next step. If HCSM is the first HCS product in the cluster, do the following:

   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-folder\conf`.

   b. Back up the HCSM database by using the following command:

   ```
   HCS-Common-Component-installation-folder\bin
   \hcmds64backups /dir local-disk-folder-for-data-storage-backup /auto
   ```

   **Note:** We recommend that you back up the database in case an error occurs.

   c. If you changed the database port from the default (22032/tcp), take note of the port number that you are using.

   d. Migrate the database to the shared disk by using the following command:

   ```
   HCS-Common-Component-installation-folder\bin
   \hcmds64dbclustersetup /createcluster /databasepath folder-on-shared-disk-for-database-recreation /exportpath local-disk-folder-for-data-storage-backup /auto
   ```
Caution: When you run the `hcmandbclustersetup` command, the database port number and 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.

6. Use the following command to ensure that the HCS product services are stopped:

   `HCS-Common-Component-installation-folder\bin\hcmandbclustersetup /status`

7. In the Services window, open the properties for each of the following services and change Startup Type from Automatic to Manual.
   - 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

8. Create a work folder on the shared disk.
   a. Create a folder on the shared disk to use as the Hitachi Compute Systems Manager (HCSM) work folder.
   b. Access the following properties file and enter the work folder path as the value for the `hcsm.shared.directory` property:

   `HCSM-installation-folder\ComputeSystemsManager\conf\user.properties`

9. If you installed Deployment Manager, run the following batch file and specify settings so that the Deployment Manager services start correctly:

   `HCSM-installation-folder\ComputeSystemsManager\DeploymentManager\hcsm_setting\set_cluster.bat`

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. In the cluster management software, move the groups in which you plan to register HCSM services to the standby node.

Right-click the group that registers the services, select Move, and then select either **Select Node** or **Move this service or application to another node**.

**Related tasks**

- Setting up a new instance of HCSM on a standby node on page 190
- Setting up a cluster within Windows Server Failover Clustering on page 202
- Taking HCSM services offline from cluster management software on page 207
- Backing up the database in a cluster environment on page 210

**Related references**

- Command format for migrating to a cluster environment on page 214
- Synchronizing settings in a cluster environment on page 201
- Settings requirements for virus scanning programs in a cluster environment on page 201

**Setting up a new instance of HCSM on a standby node**

You can complete a new installation of Hitachi Compute Systems Manager (HCSM) on the management server on a standby node in a cluster configuration.

**Procedure**

1. Complete a new installation of HCSM on the standby node.

   For details on how to install HCSM, see the *Hitachi Compute Systems Manager Installation and Configuration Guide*.

   Before installing HCSM on the standby node, be aware of the following requirements:
   - You must install HCSM in the same location as on the active node.
   - If Deployment Manager is installed on the active node, install Deployment Manager on the standby node.
• If other HCS 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 HCS 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 an HCS product configured within the cluster, skip to the next step. If HCSM is the first HCS 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-folder\conf`.

      **Note:** On a standby node, you must specify `standby` for `mode`.

   b. If you changed the port used by the database from the default (22032/tcp), take note of the port number you are using.
   c. Migrate the database to the shared disk by using the following command:
      
      ```
      HCS-Common-Component-installation-folder\bin\hcmds64dbclustersetup /createcluster /databasepath shared-disk-folder-for-database-recreation /exportpath local-disk-folder-for-data-storage-backup /auto
      ```
      
      For the `databasepath` option, specify the same folder as the one used by the active node to re-create the database.

      **Caution:** When you run the `hcmds64dbclustersetup` command, the database port number and 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.

4. Use the following command to ensure that the HCS product services are stopped:
   
   ```
   HCS-Common-Component-installation-folder\bin\hcms64srv /status
   ```
5. In the Services window, open the properties for each of the following services and change Startup Type from Automatic to Manual.
   - 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

6. Access the following properties file and verify that the work folder path created on the active node is specified as the value for the hcsm.shared.directory property:

   `HCSM-installation-folder\ComputeSystemsManager\conf \user.properties`

   If not, modify the value to match the value specified on the active node.

7. If you installed Deployment Manager, run the following batch file and specify settings so that the Deployment Manager services start correctly:

   `HCSM-installation-folder\ComputeSystemsManager\DeploymentManager\hcsm_setting\set_cluster.bat`

8. 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-folder\ComputeSystemsManager\conf \user.properties`

9. Register the HCSM services in the group by using the cluster management software.

   If you installed the deployment manager, you must also register the Deployment Manager services as resources.

10. On the active node, bring online the services and groups of any other Hitachi Command Suite product that you took offline previously. Also, enable failover for the same services and groups.

Related concepts
- [About implementing and using HCSM in a cluster environment](#) on page 180

Related tasks
- [Setting up a new instance of HCSM on an active node](#) on page 187

Related references
- [Command format for migrating to a cluster environment](#) on page 214
- [Settings requirements for virus scanning programs in a cluster environment](#) on page 201
Upgrading Hitachi Compute Systems Manager in a cluster environment

This module provides information about upgrading or completing an overwrite installation of Hitachi Compute Systems Manager (HCSM) in a cluster environment.

Note: The procedure to upgrade from version 7.x is different from the standard upgrade procedure explained in the following sections. The procedure for upgrading from version 7.x is located in "Upgrading from HCSM in a cluster environment" in Appendix C.

Upgrading or overwriting HCSM on an active node

You can complete an upgrade or overwrite installation of Hitachi Compute Systems Manager (HCSM) on a management server that is an active node in a cluster environment.

Before completing an upgrade or overwrite installation, stop cluster operation temporarily.

Procedure

1. In the cluster management software, bring online the group containing the Hitachi Compute Systems Manager services.
2. In the cluster management software, take the following services offline:
   - 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
   - Any Hitachi Command Suite product resources not mentioned above

Note: You take the HiRDB/ClusterService _HD1 services offline in step 4.

3. Run the following command to stop the services for Hitachi Command Suite products.

   \HCS-Common-Component-installation-folder\bin\hcms64srv /stop

4. In the cluster management software, take the following service offline:

Implementing Hitachi Compute Systems Manager in a cluster environment

Hitachi Compute Systems Manager Installation and Configuration Guide
5. In the cluster management software, disable failover of the group in which the services are registered by changing the settings for the following resources:
   - 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
   - Any other services you took offline in step 2

   If you are using Deployment Manager, change the resource settings of the following services:
   - DeploymentManager PXE Management
   - DeploymentManager PXE Mtftp
   - DeploymentManager Transfer Management

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

6. Ensure that the shared disk is accessible.

7. Complete an overwrite or upgrade installation of HCSM.

   In the Pre-installation Confirmation, ensure that the setting for Back up the database prior to the installation is Yes.

   If the setting is No, click Advanced Settings to open the Advanced Installation Settings dialog box. Select Backup from the setup menu, and then select Back up the database prior to the installation.

8. Run the following command to back up the database after the upgrade or overwrite installation is complete:

   HCS-Common-Component-installation-folder\bin\hcmds64backups /dir local-disk-folder-for-data-storage-backup /auto

9. If any Hitachi Command Suite products are running, use the Windows menu to stop Hitachi Compute Systems Manager.

   If you use the Windows menu to stop Hitachi Compute Systems Manager, the other Hitachi Compute Systems Manager products also stop at the same time.

10. In the Services window, open the properties for the following services. If Startup Type is Automatic, change it to Manual.

    - 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

11. Access the following properties file and verify that the hcsm.shared.directory property value specifies the HCSM work folder path:
If the value is not specified, create a folder on the shared disk, and then specify the path of that folder.

12. If you are using Deployment Manager, run the following batch file and specify settings so that the deployment manager services start correctly:

```
HCSM-installation-folder\ComputeSystemsManager\DeploymentManager\hcsm_setting\set_cluster.bat
```

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.

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.

14. In the cluster management software, move the group containing the HCSM resources to the standby node.

Right-click the group in which the services are registered, and select **Move** and then either **Select Node** or **Move this service or application to another node**.

**Related tasks**
- [Upgrading or overwriting HCSM on a standby node](#) on page 195

### Upgrading or overwriting HCSM on a standby node

You can complete an upgrade or overwrite installation of Hitachi Compute Systems Manager (HCSM) on a management server that is a standby node in a cluster environment.

Restart the cluster environment that you stop temporarily on the active node after an upgrade or overwrite installation.
Procedure

1. Use the following command to stop the Hitachi Command Suite product services on the standby node.
   
   ```
   HCS-Common-Component-installation-folder\bin\hmcs64srv /stop
   ```

2. Complete an overwrite or upgrade installation of HCSM.
   
   If you complete a new installation of Deployment Manager during an upgrade or overwrite installation on an active node, ensure that you also complete a new installation of Deployment Manager on the standby node.

3. If any Hitachi Command Suite products are running, use the Windows menu to stop Hitachi Compute Systems Manager (HCSM).
   
   If you use the Windows menu to stop Hitachi Compute Systems Manager, the other Hitachi Command Suite products also stop at the same time.

4. In the Services window, open the properties for the following services. If the Startup Type is Automatic change it to Manual.
   
   - 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

5. In the cluster management software, enable failover for the group in which the services are registered by changing the settings of the following resources:
   
   - 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
   - Any Hitachi Command Suite product resources not mentioned above

   If you are using Deployment Manager, also change the resource settings of the following services:
   
   - DeploymentManager PXE Management
   - DeploymentManager PXE Mtftp
   - DeploymentManager Transfer Management

   The resource settings can be changed by the following method:

   In Windows Server Failover Clustering, right-click the resource name, select Properties > Policies tab, and enable the If resource fails, attempt restart on current node option and the If restart is unsuccessful, fail over all resources in this service or application or If restart in unsuccessful, fail over all resources in this service or application options.
6. Access the following properties file and verify that the HCSM work folder path created on the active node is listed as the value for the `hcsm.shared.directory` property:

   HCSM-installation-folder\ComputeSystemsManager\conf\user.properties

   If not, change the property to reflect the correct work folder path.

7. If you are using Deployment Manager, run the following batch file and specify settings so that Deployment Manager services start correctly:

   HCSM-installation-folder\ComputeSystemsManager\DeploymentManager\hcsm_setting\set_cluster.bat

8. 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-folder\ComputeSystemsManager\conf\user.properties

9. In the cluster management software, bring online the group containing the HCSM services.

10. In the cluster management software, migrate the group containing the HCSM services to the active node.

11. If you completed a new installation of Deployment Manager during an HCSM upgrade or overwrite installation, configure the cluster environment so that you can use Deployment Manager.

Related tasks

- [Upgrading or overwriting HCSM on an active node](#) on page 193

---

**Migrating Hitachi Compute Systems Manager (HCSM) to a cluster environment**

You can migrate Hitachi Compute Systems Manager (HCSM) to a management server that is an active node in a cluster environment.

**Prerequisites**

Before migrating Hitachi Compute Systems Manager (HCSM) to a cluster environment, you must complete the following tasks:

- Check whether the work folder used by HCSM contains any subfolders or files. If it does, move the Hitachi Compute Systems Manager (HCSM) work folder to the shared disk.

  For details about the Hitachi Compute Systems Manager (HCSM) work folder, see the description of the `hcsm.shared.directory` property defined in the following file:
If you are using Deployment Manager and plan to migrate Hitachi Compute Systems Manager (HCSM) to a cluster environment, you must move the Deployment Manager image file to the shared disk and register it again before migrating to a cluster environment as follows:

1. In the Deployment Manager settings, delete the image file that is moving.
2. Move the image file to the shared disk.
3. In the Deployment Manager settings, register the image file that you moved to the shared disk.

For details on registering, deleting, and managing the image file in the Deployment Manager settings, see the Hitachi Compute Systems Manager User Guide.

You can change the environment of a Hitachi Compute Systems Manager (HCSM) system from a non-cluster to a cluster configuration. Before you can migrate to a cluster configuration, you must ensure that HCSM is installed and operational on the active node in the new cluster.

Procedure

1. Install HCSM 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 HCSM user interface to point to the logical host name:

   HCS-Common-Component-installation-folder\bin\hcmds64chgu /change http://active-node-IP-address-or-host-name:port-number http://logical-host-name:port-number

4. Create a cluster configuration file on the active and the standby nodes.

   This procedure is not necessary if the cluster environment was constructed 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.

```plaintext
mode=standby
virtualhost=logical-host-name
onlinehost=active-node-host-name
standbyhost=standby-node-host-name
```

Save the file as `cluster.conf` in `installation-folder-of-Common-Component\conf`.

5. On the active node, use the following command to back up the database:

```
HCS-Common-Component-installation-folder\bin\hcmds64backups /dir local-disk-folder-for-data-storage-backup /auto
```

6. If you have changed the port used by the database from the default (22032/tcp), take note of the port number you are using.

7. Use the following command on the active node to migrate the database to the shared disk:

```
HCS-Common-Component-installation-folder \bin \hcmds64dbclustersetup /createcluster /databasepath folder-on-shared-disk-for-database-recreation /exportpath local-disk-folder-for-backup-storage /auto
```

8. On the standby node, use the following command to provide access to the database on the shared disk:

```
HCS-Common-Component-installation-folder\bin\hcmds64dbclustersetup /createcluster /databasepath folder-on-shared-disk-for-database-recreation /exportpath local-disk-folder-for-backup-storage /auto
```

For the `databasepath` option, specify the same folder as the one used by the active node to re-create the database.

---

Caution: When you run the `hcmds64dbclustersetup` command, the database port number and 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.

9. On the active and standby nodes, use the following command to ensure that the Hitachi Command Suite (HCS) product services are stopped:

```
HCS-Common-Component-installation-folder\bin\hcmds64srv /status
```
10. On the active and standby nodes, configure the following services to start manually:
   - 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
   In the Services window, open the properties for these services and change Startup Type from Automatic to Manual.

11. On both the active and standby nodes, set up the Hitachi Compute Systems Manager (HCSM) work folder.
   a. If you moved the Hitachi Compute Systems Manager (HCSM) work folder to the shared disk, specify the path of that folder. If you did not move the folder, create a folder on the shared disk, and then specify the path of that folder.
   b. Access the following properties file and enter the work folder path as the value for the hcsm.shared.directory property:

   HCSM-installation-folder\ComputeSystemsManager\conf\user.properties

12. If you are using the Deployment Manager, on both the active and standby nodes, run the following batch file and specify settings so that the Deployment Manager services start correctly:

   HCSM-installation-folder\ComputeSystemsManager\DeploymentManager\hcsm_setting\set_cluster.bat

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 thesvp.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.

14. Register the Hitachi Compute Systems Manager services in the cluster management software.
If you are using Deployment Manager, you must also register the Deployment Manager services as resources.

**Related references**
- [Command format for migrating to a cluster environment](#) on page 214
- [Settings requirements for virus scanning programs in a cluster environment](#) on page 201

## Configuring HCSM within a cluster environment

This module provides information about configuring Hitachi Compute Systems Manager (HCSM) within a cluster by verifying environment settings and adding resources.

**Related tasks**
- [Setting up a cluster within Windows Server Failover Clustering](#) on page 202
- [Setting up Deployment Manager in a cluster environment using Windows Server Failover Clustering](#) on page 204

**Related references**
- [Synchronizing settings in a cluster environment](#) on page 201

## 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 tasks**
- [Migrating Hitachi Compute Systems Manager (HCSM) to a cluster environment](#) on page 197
- [Setting up a new instance of HCSM on a standby node](#) on page 190

## Synchronizing settings in a cluster environment

When you use HCSM 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 HCSM in a cluster environment, when you are changing the configuration of a Hitachi Compute Systems Manager product, make sure to use the same settings on all nodes.

**Setting up a cluster within Windows Server Failover Clustering**

You can set up a cluster environment within the Windows Server Failover Clustering.

---

**Caution:** Do not access HCSM while setting up the cluster environment.

**Procedure**

1. Before configuring the cluster using the Windows Server Failover Clustering, verify that you have checked the cluster environment and completed all prerequisites.

2. In the cluster management software, add the Hitachi Compute Systems Manager (HCSM) resources to the group by right-clicking on the group and selecting **Add Resource > Generic Service**.

3. In the **Select Services** window, select the following services:
   - HiRDB/ClusterService _HD1
   - 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

   These services are now registered as resources.

4. Right-click the resource name, select **Properties**, and enter the settings provided in the following tables.

---

**Note:** There is no **Registry Replication** tab in Windows Server 2012.

The following table lists the information that you enter when setting the HiRDB/ClusterService _HD1 properties:
<table>
<thead>
<tr>
<th>Tab name</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Startup parameters: Leave this field empty (if this field contains a value, delete it).</td>
</tr>
<tr>
<td>Dependencies</td>
<td>Register the shared disk and client access point.</td>
</tr>
<tr>
<td>Advance Policies</td>
<td>Possible Owners: Add the active node and the standby node as owners of the resources.</td>
</tr>
<tr>
<td>Policies</td>
<td>Leave this field empty.</td>
</tr>
<tr>
<td>Registry Replication</td>
<td>Leave this field empty.</td>
</tr>
</tbody>
</table>

The following table lists the information that you enter when setting the HBase 64 Storage Mgmt SSO Service properties:

<table>
<thead>
<tr>
<th>Tab name</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Startup parameters: Leave this field empty (if this field contains a value, delete it).</td>
</tr>
<tr>
<td>Dependencies</td>
<td>Register HiRDB/ClusterService _HD1.</td>
</tr>
<tr>
<td>Advance Policies</td>
<td>Possible Owners: Add the active node and the standby node as owners of the resources.</td>
</tr>
<tr>
<td>Policies</td>
<td>Leave this field empty.</td>
</tr>
<tr>
<td>Registry Replication</td>
<td>Leave this field empty.</td>
</tr>
</tbody>
</table>

The following table lists the information that you enter when setting the HBase 64 Storage Mgmt Web Service properties:

<table>
<thead>
<tr>
<th>Tab name</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Startup parameters: Leave this field empty (if this field contains a value, delete it).</td>
</tr>
<tr>
<td>Dependencies</td>
<td>Register HBase 64 Storage Mgmt SSO Service.</td>
</tr>
<tr>
<td>Advance Policies</td>
<td>Possible Owners: Add the active node and the standby node as owners of the resources.</td>
</tr>
<tr>
<td>Policies</td>
<td>Leave this field empty.</td>
</tr>
<tr>
<td>Registry Replication</td>
<td>Leave this field empty.</td>
</tr>
</tbody>
</table>

The following table lists the information that you enter when setting the HBase 64 Storage Mgmt Web SSO Service properties:

<table>
<thead>
<tr>
<th>Tab name</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Startup parameters: Leave this field empty (if this field contains a value, delete it).</td>
</tr>
<tr>
<td>Dependencies</td>
<td>Register HBase 64 Storage Mgmt Web Service.</td>
</tr>
<tr>
<td>Advance Policies</td>
<td>Possible Owners: Add the active node and the standby node as owners of the resources.</td>
</tr>
<tr>
<td>Policies</td>
<td>Leave this field empty.</td>
</tr>
</tbody>
</table>
The following table lists the information that you enter when setting the HCS Compute Systems Manager Web Service properties:

<table>
<thead>
<tr>
<th>Tab name</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry Replication</td>
<td>Leave this field empty.</td>
</tr>
</tbody>
</table>

5. In the cluster management software, bring online the group to which you added the HCS services.
6. If you are using Deployment Manager, set up the Deployment Manager services within the cluster environment.

**Setting up Deployment Manager in a cluster environment using Windows Server Failover Clustering**

You can set up Deployment Manager in a cluster environment using Windows Server Failover Clustering.

**Note:** The specified resource name when the services are registered as resources can be displayed in the cluster management software by following the procedure below. Specify the resource name when operating the cluster management software.

**Prerequisites**

Before adding Deployment Manager to a cluster environment, you must first set up Hitachi Compute Systems Manager the cluster environment using Windows Server Failover Clustering.

**Caution:** When setting up clustering, ensure that you do not access HCSM for any tasks that are not related to the cluster setup process.

**Procedure**

1. In the cluster management software, take the HCS Compute Systems Manager Web Service offline.
2. Change the settings for Hitachi Command Suite Compute Systems Manager Web Service using the cluster management software.
• For Windows Server 2012:
  Start Windows Powershell and run the following command:
  `Add-ClusterCheckpoint -ResourceName HCS-Compute-Systems-Manager-Web-Service-resource-name -RegistryCheckpoint "SOFTWARE\Wow6432Node\NEC\DeploymentManager"`

  **Note:** You cannot run this command at the command prompt.

• For operating systems other than Windows Server 2012:
  In the cluster management software, right-click the resource name and choose **Properties**.
  Change the settings in the **Registry Replication** dialog box as shown in the following table:

<table>
<thead>
<tr>
<th>System architecture</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>x64</td>
<td>SOFTWARE\Wow6432Node\NEC\DeploymentManager</td>
</tr>
</tbody>
</table>

3. In the cluster management software, bring the Hitachi Command Suite Compute Systems Manager Web Service online.

4. Add the Deployment Manager services to the group where the Hitachi Compute Systems Manager service is registered.
   Right-click the name of the group, select **Add Resource > Generic Service**.
   In the **Select Services** window, select the following services:
   • DeploymentManager PXE Management
   • DeploymentManager PXE Mtftp
   • DeploymentManager Transfer Management

5. Right-click the resource name you created and select **Properties**.
   In each dialog box, enter the settings shown in the following tables.

  **Note:** There is no Registry Replication tab in Windows Server 2012.

The following tables show the settings for registering DeploymentManager PXE Management as a resource.

<table>
<thead>
<tr>
<th>Tab name</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Startup parameters: Leave this field empty. If the field contains a value, delete it.</td>
</tr>
<tr>
<td>Dependencies</td>
<td>Register HCS Compute Systems Manager Web Service.</td>
</tr>
</tbody>
</table>
Table name | Settings
---|---
Advanced Policies | Possible owners: add the active node and standby node as owners of the resource.
Policies | Leave empty.
Registry Replication | Leave empty.

The following table show the settings for registering DeploymentManager PXE Mtftp as a resource.

Table name | Settings
---|---
General | Startup parameters: Leave this field empty. If the field contains a value, delete it.
Dependencies | Register HCS Compute Systems Manager Web Service.
Advanced Policies | Possible owners: add the active node and standby node as owners of the resource.
Policies | Leave empty.
Registry Replication | Leave empty.

The following table show the settings for registering DeploymentManager Transfer Management as a resource.

Table name | Settings
---|---
General | Startup parameters: Leave this field empty. If the field contains a value, delete it.
Dependencies | Register HCS Compute Systems Manager Web Service.
Advanced Policies | Possible owners: add the active node and standby node as owners of the resource.
Policies | Leave empty.
Registry Replication | Leave empty.

6. Log in to Hitachi Compute Systems Manager. In the **Administration** tab, configure the following Deployment Manager settings:
   - Specify that images files are stored in a folder on the shared disk.
   - Specify that the Deployment Manager server IP address is the cluster management IP address.
   - Specify that the DHCP server is not installed on the same computer.

7. In the cluster management software, bring online the group to which you added the Deployment Manager services.

**Related tasks**
- [Setting up a cluster within Windows Server Failover Clustering](#) on page 202
Starting and stopping services in a cluster environment

This module provides information about starting and stopping Hitachi Compute Systems Manager (HCSM) in a cluster environment, which is required for many administrative tasks.

Bringing HCSM services online from cluster management software

When using HCSM in a cluster environment, you must bring the HCSM services online either by group in which the services are registered or by individual service. All HCSM services are registered in the same group.

- When using Windows Server Failover Clustering in Windows Server 2012:
  In Failover Cluster Manager, right-click the group in which the HCSM services are registered, and click Start Role.

- When using Windows Server Failover Clustering in a version other than Windows Server 2012:
  In Failover Cluster Manager, right-click the group in which the HCSM services are registered, and click Bring this service or application online.

To bring individual services online, right-click each service to start within the group and select Bring Online.

Related tasks

- Taking HCSM services offline from cluster management software on page 207
- Restarting HCSM in a cluster environment on page 209

Taking HCSM services offline from cluster management software

When using HCSM in a cluster environment, you take the HCSM services offline either by group in which the services are registered or by individual service. All HCSM services are registered in the same group.

- When using Windows Server Failover Clustering in Windows Server 2012:
  In Failover Cluster Manager, right-click the group in which the HCSM services are registered, and click Stop Role.

- When using Windows Server Failover Clustering in a version other than Windows Server 2012:
  In Failover Cluster Manager, right-click the group in which the HCSM services are registered, and click Take this service or application offline.

To take individual services offline, right-click each service within the group to stop and select Take Offline.

Related tasks

- Bringing HCSM services online from cluster management software on page 207
Temporarily stopping HCSM in a cluster environment

If you are using Hitachi Compute Systems Manager (HCSM) in a cluster environment, you must temporarily stop HCSM using the cluster management software. You must temporarily stop HCSM before you start doing database operations, such as restorations or backups.

Procedure

1. In the cluster management software, take the following services offline:
   - 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
   - Any additional Hitachi Command Suite product resources.

   **Note:** You take the HiRDB/ClusterService _HD1 services offline in step 3.

2. If you are using Deployment Manager, also take the following services offline:
   - DeploymentManager PXE Management
   - DeploymentManager PXE Mtftp
   - DeploymentManager Transfer Management
   These services are registered as resources.

3. Use the following command to stop the services for Hitachi Command Suite products:

   ```
   HCS-Common-Component-installation-folder\bin\hcmds64srv /stop
   ```

4. Take the HiRDB/ClusterService _HD1 offline.

5. In the cluster management software, disable failover for the group by changing the settings for the following resources:
   - 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
   - Any other services you took offline in step 1.

   If you are using Deployment Manager, also change the resource settings of the following services:
   - DeploymentManager PXE Management
   - DeploymentManager PXE Mtftp
To change the resource settings:

In Windows Server Failover Clustering, right-click the resource name, select **Properties > Policies** tab, and enable the **If resource fails, do not restart** option.

**Related tasks**
- [Taking HCSM services offline from cluster management software](#) on page 207
- [Restarting HCSM in a cluster environment](#) on page 209

**Restarting HCSM in a cluster environment**

After backing up or restoring a database in a cluster environment, you must restart HCSM services in the cluster, which were temporarily stopped.

To restart HCSM services in a cluster environment:

**Procedure**

1. In the cluster management software, enable failover by changing the settings for the resources that are registered to the group in which failover was disabled.
   
   Change the settings of the following resources:
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
   - HCSM Compute Systems Manager Web Service
   - HiRDB/ClusterService _HD1
   - Any services that were temporarily stopped
   - Any Hitachi Compute Systems Manager product resources not mentioned above

   If you are using Deployment Manager, change the resource settings of the following services as well:
   - DeploymentManager PXE Management
   - DeploymentManager PXE Mtftp
   - DeploymentManager Transfer Management

   To change the resource settings:

   In Windows Server Failover Clustering, right-click the resource name, select **Properties > Policies** tab, and enable both of the following options:
   - **If resource fails, attempt restart on current node**
• If restart is unsuccessful, fail over all resources in this Role or
  If restart is unsuccessful, fail over all resources in this service or application
2. In the cluster management software, bring online the group that contains
the HCSM services.

Related tasks
• Bringing HCSM services online from cluster management software on page 207
• Taking HCSM services offline from cluster management software on page 207
• Backing up the database in a cluster environment on page 210

Managing the database in a cluster environment

This module provides information about managing the HCSM database in a
cluster environment.

Backing up the database in a cluster environment

You must maintain a backup copy of the database in a cluster environment so
that the management server can restore the database if there is a failure.

Caution: When Hitachi Device Manager is installed on the same management
server as HCSM, and is remotely connected to Hitachi Tuning Manager, you
must temporarily stop it on the computer on which the Hitachi Tuning
Manager server is installed. You can start Hitachi Tuning Manager again after
backing up the database. For details on how to stop and restart Hitachi
Tuning Manager, see the documentation for the version of Hitachi Tuning
Manager installed in your system.

Procedure
1. In the cluster management software, temporarily stop HCSM within the
cluster.
2. Use the following command to start the Hitachi Command Suite Common
Component services.
   
   HCS-Common-Component-installation-folder\bin\hcmds64srv /start

3. On the active node, back up the database by using the following
command:
   
   HCS-Common-Component-installation-folder\bin\hcmds64backups /dir local-disk-folder-for-backup-storage
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.

4. Use the following command to stop the Hitachi Command Suite Common Component services.

   \texttt{HCS-Common-Component-installation-folder\bin\hmcs64srv /stop}

5. In the cluster management software, restart HCSM within the cluster.

Result

You now have a backup copy of the latest HCSM database.

Related tasks

- Restoring the database in a cluster environment on page 211
- Temporarily stopping HCSM in a cluster environment on page 208
- Restarting HCSM in a cluster environment on page 209

Restoring the database in a cluster environment

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 \texttt{hmcs64backups} command.

Caution:

- When Hitachi Device Manager is installed on the same management server as HCSM, and is remotely connected to Hitachi Tuning Manager, you must temporarily stop it on the computer where the Hitachi Tuning Manager server is installed. You can start Hitachi Tuning Manager again after the database has been restored. For details on how to stop and restart Hitachi Tuning Manager, see the documentation for the version of Hitachi Tuning Manager installed in your system.
- The \texttt{hmcs64db} 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. In the cluster management software, temporarily stop HCSM within the cluster.

2. On the active node, restore the database by using the following command:

   \texttt{HCS-Common-Component-installation-folder\bin\hmcs64db /restore backup-file /type ALL}

   where
backup-file is the absolute path to the backup file (backup.hdb) saved on the shared disk.

3. In the cluster management software, restart HCSM within the cluster.
4. Use the HCSM user interface to check the status of the HCSM tasks. If a task is incomplete or failed, recreate the task or reschedule it.
5. If Hitachi Device Manager is remotely connected to Hitachi Tuning Manager, the settings are reset when you restore the database. You must set up your Hitachi Tuning Manager connection again.

Related tasks
- Backing up the database in a cluster environment on page 210
- Temporarily stopping HCSM in a cluster environment on page 208
- Restarting HCSM in a cluster environment on page 209

Exporting the database in a cluster environment

To migrate the HCSM database 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.

Caution: When Hitachi Device Manager is installed on the same management server as HCSM, and is remotely connected to Hitachi Tuning Manager, you must temporarily stop it on the computer on which the Hitachi Tuning Manager server is installed. You can start Hitachi Tuning Manager again after exporting the database. For details on how to stop and restart Hitachi Tuning Manager, see the documentation for the version of Hitachi Tuning Manager installed on your system.

Procedure
1. In the cluster management software, temporarily stop HCSM within the cluster.
2. Use the following command to start the Hitachi Command Suite products.
   
   ```
   HCS-Common-Component-installation-folder\bin\hcmds64srv /start
   ```

3. Use the following command to export the databases:
   
   ```
   HCS-Common-Component-installation-folder\bin\hcmds64dbtrans /export /workpath working-folder /file archive-file
   ```

   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.

4. For migrations, transfer the exported files to the migration target server.
If the system cannot create an archive file (such as when the total database capacity exceeds 2 GB), manually transfer all files stored in the folder specified for the workpath directory option to the migration target server. Do not change the file structure in the folder specified by the workpath option.

5. Use the following command to stop the Hitachi Command Suite products.

   ```
   HCS-Common-Component-installation-folder\bin\hcmds64srv /stop
   ```

6. In the cluster management software, restart HCSM within the cluster.

Related tasks

- Importing the database in a cluster environment on page 213
- Temporarily stopping HCSM in a cluster environment on page 208
- Restarting HCSM in a cluster environment on page 209

## Importing the database in a cluster environment

After you export the HCSM database from an existing server in the cluster, you can import it to another HCSM server. You can also use an exported database to restore an existing database after a failure.

**Caution:** When Hitachi Device Manager is installed on the same management server as HCSM, and is remotely connected to Hitachi Tuning Manager, you must temporarily stop it on the computer on which the Hitachi Tuning Manager server is installed. You can start Hitachi Tuning Manager again after importing the database. For details on how to stop and restart Hitachi Tuning Manager, see the documentation for the version of Hitachi Tuning Manager installed on your system.

### Procedure

1. 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.

2. In the cluster management software, temporarily stop HCSM within the cluster.

3. Use the following command to start the database service:

   ```
   HCS-Common-Component-installation-folder\bin\hcmds64dbsrv /start
   ```

4. 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|HCSM}
   ```

   When specifying the command options, use the following descriptions:
• workpath
  Specify the working-folder using the absolute path of a folder where you want to temporarily store your database information. Ensure that this folder is empty.

• file
  Specify the archive-file using the absolute path of the database archive file that you transferred from the original server.

• type
  To import all Hitachi Command Suite (HCS) product databases, specify the type as ALL. To import the HCSM database only, specify HCSM. To import other HCS product databases individually, see the documentation for the applicable Hitachi Command Suite product.

5. Use the following command to start the HCS services.

   HCS-Common-Component-installation-folder\bin\hcmds64srv /start

6. In the cluster management software, restart HCSM within the cluster.

7. Back up the databases.
   As a precaution, we recommend that you immediately back up the databases you imported.

8. If Hitachi Device Manager is remotely connected to Hitachi Tuning Manager, the settings are reset when you restore the database. You must set up your Hitachi Tuning Manager connection again.

Related tasks

• Backing up the database in a cluster environment on page 210
• Exporting the database in a cluster environment on page 212
• Temporarily stopping HCSM in a cluster environment on page 208
• Restarting HCSM in a cluster environment on page 209

Command format for migrating to a cluster environment

You can use the hcmds64dbclustersetup command to migrate HCSM to a cluster environment. You use the cluster setup migration command as follows:

   HCS-Common-Component-installation-folder\bin\hcmds64dbclustersetup /createcluster /databasepath folder-on-shared-disk-for-database-recreation /exportpath local-disk-folder-for-data-storage-backup /auto

where

• databasepath specifies a folder for recreating the database. Specify an absolute path that is 63 characters or less for a folder on the shared disk. You can use the following characters A~Z a~z 0~9 . _ and you can also use backslash (\), colon (:), and the forward slash (/) as delimiters.
• exportpath specifies the destination folder in which to store the data that you are backing up. Specify an absolute path that is 63 characters or less
for a folder 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 `<backup-data-storage-folder>` already exists, delete the entire content of the folder, or delete the folder.

- 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 tasks**

- [Migrating Hitachi Compute Systems Manager (HCSM) to a cluster environment](#) on page 197

---

**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. Move the group in which the HCSM services are registered from the standby node to the active node.

2. In the cluster management software, take the following services offline:
   - 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
• DeploymentManager PXE Management
• DeploymentManager PXE Mtftp
• DeploymentManager Transfer Management

3. In the cluster management software, remove the Hitachi Command Suite Compute Systems Manager Web Service settings that you set for Deployment Manager.
   • When using Windows Failover Clustering on Windows Server 2012, start Windows Powershell and run the following command:
     `Remove-ClusterCheckpoint -ResourceName HCS-Compute-Systems-Manager-Web-Service-resource-name -RegistryCheckpoint`

   **Note:** You cannot run this command at the command prompt.

   • When using Windows Failover Clustering on operating systems other than Windows Server 2012:

     In the cluster management software, right-click the resource name, choose **Properties**, and change the settings in the **Registry Replication** dialog box as follows:

     | Tab name            | Settings         |
     |---------------------|------------------|
     | Registry Replication| Leave empty.     |

   4. To stop HCS product services, use the Windows menu to stop Hitachi Compute Systems Manager.

   If you use the Windows menu to stop Hitachi Compute Systems Manager, the other HCS products also stop at the same time.

   5. In the cluster management software, take the **HiRDB/ClusterService_HD1** service offline.

   6. Use the cluster management software to delete the following services:

     • DeploymentManager PXE Management
     • DeploymentManager PXE Mtftp
     • DeploymentManager Transfer Management

   7. In the cluster management software, disable failover of the group in which the deleted services were registered.

     In Windows Failover Clustering, right-click the resource name, choose **Properties > Policy** tab and select **If the resource fails, do not restart**.

   8. Back up the database.

   9. Run the following command to stop the Hitachi Command Suite product services:

      `HCS-Common-Component-installation-folder\bin\hcmds64srv /stop`
10. Remove Deployment Manager from the active node.
11. On the active node, delete any files and folders that are no longer required.
12. In the cluster management software, move the group in which the HCSM services are registered to the standby node.
13. Remove Deployment Manager from the standby node.
14. On the standby node, delete any files and folders that are no longer required.
15. Enable failover for the group in which the services are registered, and complete the following steps to configure the resources for which you previously disabled failover:

   In Windows Server Failover Clustering, right-click the resource name and choose Properties. On the Policies tab, select the following check boxes:
   - If resource fails, attempt restart on current node
   - If restart is unsuccessful, fail over all resources in this Role or
   - If restart is unsuccessful, fail over all resources in this service or application

Related tasks
- Taking HCSM services offline from cluster management software on page 207
- Temporarily stopping HCSM in a cluster environment on page 208

Removing the software in a cluster environment

You can remove the Hitachi Compute Systems Manager (HCSM) software from the server in a cluster environment if you want to migrate to a different server or stop HCSM operation.

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

Procedure

1. Move the group in which the HCSM services are registered from the standby node to the active node. On the active node, use the cluster management software to bring the HCS group online.
2. On the active node, use the cluster management software to take the following services offline:
   - 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
If you have been using the Deployment Manager, you must also take the following services offline:
- DeploymentManager PXE Management
- DeploymentManager PXE Mtftp
- DeploymentManager Transfer Management

3. To stop the Hitachi Command Suite products, use the Windows menu to stop HCSM.
   If you use the Windows menu to stop Hitachi Compute Systems Manager, the other Hitachi Command Suite products also stop at the same time.

4. Use the cluster management software to take the HiRDB/ClusterService _HD1 service offline.

5. In the cluster management software, delete the following services unless other applications are using them:
   - 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

   If you are using the Deployment Manager, you must also delete following services:
   - DeploymentManager PXE Management
   - DeploymentManager PXE Mtftp
   - DeploymentManager Transfer Management

6. In the cluster management software, disable failover for the HCS services group where the services that you did not delete in step 5 are registered.

   To change the resource settings:
   In Windows Server Failover Clustering, right-click the resource name, and choose Properties. On the Policies tab, select If resource fails, do not restart.

7. Back up the database.

8. Use the following command to stop the Hitachi Command Suite Common Component services.
   \[ HCS-Common-Component-installation-folder\bin\hcmds64srv /stop \]

9. Remove HCSM from the active node.

10. 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).

11. In the cluster management software, move the HCSM services group to the standby node.

12. Remove HCSM from the standby node.
13. 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).

14. If the following resources are not in use by other applications, use the cluster management software to take them offline, and then delete them.
   • IP address
   • shared disk

15. If the HCSM services group is no longer needed, delete it.

16. If you want to continue using the group, enable failover for the following resources for which you disabled failover in step 6:

   In Windows Server Failover Clustering, right-click the resource name and select **Properties > Policies** tab, and enable the **If resource fails, attempt on the current node** option and the **If restart is unsuccessful, fail over all resources in this Role** or **If restart is unsuccessful, fail over all resources in this service or application** options.

**Related tasks**

- [Taking HCSM services offline from cluster management software](#) on page 207
- [Removing Deployment Manager from a cluster environment](#) on page 215
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 (HCSM), follow the instructions that appear in the error messages generated by HCSM.

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 222
- Troubleshooting example: management server does not start on page 223
- Troubleshooting example: database corruption on page 223
- Troubleshooting example: database corruption in a cluster environment on page 224

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, HCSM generates an error message. The following is an example of the troubleshooting information HCSM might generate when no login window opens even though the user specified the correct URL.

Possible cause

HCSM is not running or is in the process of starting on the management server.

Countermeasure

Check the HCSM 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 222
**Troubleshooting example: management server does not start**

If HCSM does not start as expected, HCSM generates an error message. The following is an example of the troubleshooting information HCSM might generate when the HCSM service or the Hitachi Command Suite (HCS) 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 222

**Troubleshooting example: database corruption**

If you cannot restore a database using the `hcmds64db` or `hcmds64dbtrans` command, HCSM 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 HCSM.
3. To restore the database, use the following command:
   - In Windows:
     ```
     \hcmds64dbrepair /trans exported-database-archive-files-folder
     ```
   - In Linux:
You must use the absolute path to the location of the database archive files.

4. Start HCSM.
5. Change the HCSM System account password. This step is required because the \( \text{hcmds64dbrepair} \) command resets the System account back to the default password.

Related concepts
- [Troubleshooting overview](#) on page 222

### Troubleshooting example: database corruption in a cluster environment

If you cannot restore a database using the \( \text{hcmds64db} \) or \( \text{hcmds64dbtrans} \) command in a cluster environment, HCSM generates an error message. The following example describes how to use \( \text{hcmds64dbrepair} \) command to restore a database that was exported with the \( \text{hcmds64dbtrans} \) command.

#### Possible cause
The database in a cluster environment might be corrupted.

#### Countermeasure
1. Verify that the available capacity in the following directory is greater than the size of the database:
   
   \[ \text{HCS-Common-Component-installation-folder\tmp} \]
   
   When restoring the database, the archived database files are extracted to this directory.

2. In the cluster management software, temporarily stop HCSM within the cluster.

3. To restore the database, use the following command on the HCSM active node:
   
   \[ \text{HCS-Common-Component-installation-folder\bin} \ \text{\( \text{hcmds64dbrepair} \) /trans exported-database-archive-file} \]
   
   You must use the absolute path to the location of the database archive files.

4. In the cluster management software, restart HCSM within the cluster.

5. Using the HCSM interface, check the status of the HCSM 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 HCSM 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 222

---

**Collecting maintenance information**

This module provides information about collecting maintenance information for troubleshooting HCSM issues.

**About collecting maintenance information**

If your Hitachi Compute Systems Manager (HCSM) 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 HCSM login window is not displayed even though the GUI is running.
- The HCSM main window is not displayed after you log in to HCSM.

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 222

**Related tasks**
- [Collecting management server maintenance information](#) on page 226
- [Collecting maintenance information for a managed host on Windows](#) on page 231
- [Collecting maintenance information for a managed host on Linux or Solaris](#) on page 232
- [Collecting Java VM thread information on Windows](#) on page 228

**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:**

```
```

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 (HCS) products.

To collect maintenance information for HCSM 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 HCSM, see the manual for the applicable product.  
  - All printable ASCII characters 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 HCS 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 HCS product names, see the documentation for each product. To specify multiple product names, separate them by a space.  
  - To obtain maintenance information for HCSM, 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 HCS 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 `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 225

**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:
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 HCSM:
   - HCS-Common-Component-installation-folder\uCPSB\CC\web
     \containers\HBase64StgMgmtSSOService\javacorexxx.xxxx.txt
   - HCS-Common-Component-installation-folder\uCPSB\CC\web
     \containers\ComputeSystemsManagerWebService
     \javacorexxx.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:](WarningIcon) 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 225
- Collecting Java VM thread information on Linux on page 229

**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 HCSM.

   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 HCSM:
   
   - `HCS-Common-Component-installation-folder/uCPSB/CC/web/
     containers/HBase64StgMgmtSSOService/javacorexxx.xxxx.txt`
   
   - `HCS-Common-Component-installation-folder/uCPSB/CC/web/
     containers/ComputeSystemsManagerWebService/
     javacorexxxx.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 225

Related tasks
• Collecting Java VM thread information on Windows on page 228

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 225

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 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 Solaris 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 225

Reviewing audit log information

This module provides information about reviewing audit log information.

About audit logs

When using Hitachi Compute Systems Manager (HCSM), 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 HCSM 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 233
• Viewing the audit logs on page 234

Related references

• Audit log categories and event descriptions on page 235
• Audit log message format and information on page 244
• Audit event messages for tasks on page 246
• Audit event messages for processing requests on page 246
• Audit log detailed messages for system requests on page 247

Setting up audit logs

When using HCSM, you can record user operations in audit logs. You configure audit log settings in the auditlog.conf file.

Procedure

1. Stop HCSM.
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
HCSM 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 HCSM.

**Result**

HCSM now generates user operation data and stores it in the audit logs.

**Related concepts**

- [About audit logs](#) on page 233

**Related tasks**

- [Viewing the audit logs](#) on page 234

**Related references**

- [Properties related to audit logs (auditlog.conf)](#) on page 285

**Viewing the audit logs**

When using HCSM, 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:
    `date-time server-name (or IP-address) [process-id]: message-portion`

**Related concepts**

- [About audit logs](#) on page 233

**Related tasks**

- [Setting up audit logs](#) on page 233

**Related references**

- [Audit log categories and event descriptions](#) on page 235
- [Audit log message format and information](#) on page 244
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.

<table>
<thead>
<tr>
<th>Audit log category and description</th>
<th>Type description</th>
<th>Audit event</th>
<th>Severity</th>
<th>Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>StartStop</td>
<td>Starting and stopping software</td>
<td>Successful SSO server start</td>
<td>6</td>
<td>KAPM00090-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed SSO server start</td>
<td>3</td>
<td>KAPM00091-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSO server stop</td>
<td>6</td>
<td>KAPM00092-I</td>
</tr>
<tr>
<td>Authentication</td>
<td>Administrator or end-user authentication</td>
<td>Successful login</td>
<td>6</td>
<td>KAPM01124-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Successful login (to the external authentication server)</td>
<td>6</td>
<td>KAPM02450-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed login (wrong user ID or password)</td>
<td>4</td>
<td>KAPM02291-W</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed login (logged in as a locked user)</td>
<td>4</td>
<td>KAPM02291-W</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed login (logged in as a non-existing user)</td>
<td>4</td>
<td>KAPM02291-W</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed login (no permission)</td>
<td>4</td>
<td>KAPM01095-E</td>
</tr>
<tr>
<td>Audit log category and description</td>
<td>Type description</td>
<td>Audit event</td>
<td>Severity</td>
<td>Message ID</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------</td>
<td>-------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>Failed log in</td>
<td></td>
<td>Failed login (authentication failure)</td>
<td>4</td>
<td>KAPM01125-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed login (to the external authentication server)</td>
<td>4</td>
<td>KAPM02451-W</td>
</tr>
<tr>
<td>Successful logout</td>
<td></td>
<td>Successful logout</td>
<td>6</td>
<td>KAPM08009-I</td>
</tr>
<tr>
<td>Failed logout</td>
<td></td>
<td>Failed logout</td>
<td>4</td>
<td>KAPM01126-W</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automatic account lock</td>
<td>4</td>
<td>KAPM02292-W</td>
</tr>
<tr>
<td>ExternalService</td>
<td></td>
<td>Communication with the external authentication server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events indicating the results of communication with external services such as the following:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Communication with an external server, such as NTP or DNS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Communication with a management server (SNMP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communication with the external authentication server</td>
<td>Successful communication with the LDAP directory server</td>
<td>6</td>
<td>KAPM10116-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed communication with the LDAP directory server</td>
<td>3</td>
<td>KAPM10117-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Successful communication with the Kerberos server</td>
<td>6</td>
<td>KAPM10120-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed communication with the Kerberos server (no response)</td>
<td>3</td>
<td>KAPM10121-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Successful communication with the DNS server</td>
<td>6</td>
<td>KAPM10122-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed communication with the DNS server (no response)</td>
<td>3</td>
<td>KAPM10123-E</td>
</tr>
<tr>
<td>Authentication with an external authentication server</td>
<td></td>
<td>Successful TLS negotiation with the LDAP directory server</td>
<td>6</td>
<td>KAPM10124-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed TLS negotiation with the LDAP directory server</td>
<td>3</td>
<td>KAPM10125-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Successful authentication</td>
<td>6</td>
<td>KAPM10126-I</td>
</tr>
<tr>
<td>Audit log category and description</td>
<td>Type description</td>
<td>Audit event</td>
<td>Severity</td>
<td>Message ID</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------</td>
<td>-------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>User authentication on an external authentication server</strong></td>
<td>Successful user authentication on the LDAP directory server</td>
<td>6</td>
<td>KAPM10128-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User not found on the LDAP directory server</td>
<td>4</td>
<td>KAPM10129-W</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed user authentication on the LDAP directory server</td>
<td>4</td>
<td>KAPM10130-W</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Successful user authentication on the Kerberos server</td>
<td>6</td>
<td>KAPM10133-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed user authentication on the Kerberos server</td>
<td>4</td>
<td>KAPM10134-W</td>
<td></td>
</tr>
<tr>
<td><strong>Acquisition of information from an external authentication server</strong></td>
<td>Successful acquisition of user information from the LDAP directory server</td>
<td>6</td>
<td>KAPM10135-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed acquisition of user information from the LDAP directory server</td>
<td>3</td>
<td>KAPM10136-E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Successful acquisition of the SRV record from the DNS server</td>
<td>6</td>
<td>KAPM10137-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed acquisition of the SRV record from the DNS server</td>
<td>3</td>
<td>KAPM10138-E</td>
<td></td>
</tr>
<tr>
<td><strong>ConfigurationAccess</strong></td>
<td>User registration (using a management client)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Successful user registration</td>
<td>6</td>
<td>KAPM07230-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed user registration</td>
<td>3</td>
<td>KAPM07240-E</td>
<td></td>
</tr>
<tr>
<td>Audit log category and description</td>
<td>Type description</td>
<td>Audit event</td>
<td>Severity</td>
<td>Message ID</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------</td>
<td>-------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>Audit log category and description</td>
<td>Type description</td>
<td>Audit event</td>
<td>Severity</td>
<td>Message ID</td>
</tr>
<tr>
<td>User deletion (using a management client)</td>
<td>User deletion</td>
<td>Successful single user deletion</td>
<td>6</td>
<td>KAPM07231-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed single user deletion</td>
<td>3</td>
<td>KAPM07240-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Successful multiple user deletion</td>
<td>6</td>
<td>KAPM07231-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed multiple user deletion</td>
<td>3</td>
<td>KAPM07240-E</td>
</tr>
<tr>
<td>Password change (using the Users and Permissions window)</td>
<td>Password change</td>
<td>Successful password change by the administrator</td>
<td>6</td>
<td>KAPM07232-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed password change by the administrator</td>
<td>3</td>
<td>KAPM07240-E</td>
</tr>
<tr>
<td>Password change (using the User Profile window)</td>
<td>Password change</td>
<td>Failed authentication processing for verifying old password</td>
<td>3</td>
<td>KAPM07239-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Successful change of login user's own password</td>
<td>6</td>
<td>KAPM07232-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed change of login user's own password</td>
<td>3</td>
<td>KAPM07240-E</td>
</tr>
<tr>
<td>Profile change</td>
<td>Profile change</td>
<td>Successful profile change</td>
<td>6</td>
<td>KAPM07233-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed profile change</td>
<td>3</td>
<td>KAPM07240-E</td>
</tr>
<tr>
<td>Permission change</td>
<td>Permission change</td>
<td>Successful permission change</td>
<td>6</td>
<td>KAPM02280-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed permission change</td>
<td>3</td>
<td>KAPM07240-E</td>
</tr>
<tr>
<td>Account lock</td>
<td>Account lock</td>
<td>Successful account lock</td>
<td>6</td>
<td>KAPM07235-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed account lock</td>
<td>3</td>
<td>KAPM07240-E</td>
</tr>
<tr>
<td>Account lock release</td>
<td>Account lock release</td>
<td>Successful account lock release</td>
<td>6</td>
<td>KAPM07236-I</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Audit log category and description</th>
<th>Type description</th>
<th>Audit event</th>
<th>Severity</th>
<th>Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: If an account is unlocked because a password was set for a user, the event is not recorded in the audit log.</td>
<td>Failed account lock release</td>
<td>3</td>
<td>KAPM07240-E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Successful account lock release using the <code>hcmds64unlockaccount</code> command</td>
<td>6</td>
<td>KAPM07236-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed account lock release using the <code>hcmds64unlockaccount</code> command</td>
<td>3</td>
<td>KAPM07240-E</td>
<td></td>
</tr>
<tr>
<td>Authorization method change</td>
<td>Successful authentication method change</td>
<td>6</td>
<td>KAPM02452-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed authentication method change</td>
<td>3</td>
<td>KAPM02453-E</td>
<td></td>
</tr>
<tr>
<td>Authorization group addition (using a management client)</td>
<td>Successful addition of an authorization group</td>
<td>6</td>
<td>KAPM07247-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed addition of an authorization group</td>
<td>3</td>
<td>KAPM07248-E</td>
<td></td>
</tr>
<tr>
<td>Authorization group deletion (using a management client)</td>
<td>Successful deletion of one authorization group</td>
<td>6</td>
<td>KAPM07249-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed deletion of one authorization group</td>
<td>6</td>
<td>KAPM07248-E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Successful deletion of multiple authorization groups</td>
<td>6</td>
<td>KAPM07249-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed deletion of multiple authorization groups</td>
<td>3</td>
<td>KAPM07248-E</td>
<td></td>
</tr>
<tr>
<td>Authorization group permission change (using a management client)</td>
<td>Successful change of an authorization group's permission</td>
<td>6</td>
<td>KAPM07250-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed change of an authorization group's permission</td>
<td>3</td>
<td>KAPM07248-E</td>
<td></td>
</tr>
<tr>
<td>User registration (processed on the management server)</td>
<td>Successful registration of user</td>
<td>6</td>
<td>KAPM07241-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed registration of user</td>
<td>3</td>
<td>KAPM07242-E</td>
<td></td>
</tr>
<tr>
<td>User information update</td>
<td>Successful update of user information</td>
<td>6</td>
<td>KAPM07243-I</td>
<td></td>
</tr>
<tr>
<td>Audit log category and description</td>
<td>Type description</td>
<td>Audit event</td>
<td>Severity</td>
<td>Message ID</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------</td>
<td>-------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>(processed on the management server)</td>
<td>Failed update of user information</td>
<td>3</td>
<td>KAPM07244-E</td>
<td></td>
</tr>
<tr>
<td>User deletion (processed on the management server)</td>
<td>Successful deletion of user</td>
<td>6</td>
<td>KAPM07245-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed deletion of user</td>
<td>3</td>
<td>KAPM07246-E</td>
<td></td>
</tr>
<tr>
<td>Authorization group registration (processed on the management server)</td>
<td>Successful registration of an authorization group</td>
<td>6</td>
<td>KAPM07251-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed registration of an authorization group</td>
<td>3</td>
<td>KAPM07252-E</td>
<td></td>
</tr>
<tr>
<td>Authorization group deletion (processed on the management server)</td>
<td>Successful deletion of an authorization group</td>
<td>6</td>
<td>KAPM07253-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed deletion of an authorization group</td>
<td>3</td>
<td>KAPM07254-E</td>
<td></td>
</tr>
<tr>
<td>Authorization group permission change (processed on the management server)</td>
<td>Successful change of an authorization group's permission</td>
<td>6</td>
<td>KAPM07255-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed change of an authorization group's permission</td>
<td>3</td>
<td>KAPM07256-E</td>
<td></td>
</tr>
<tr>
<td>Database backup or restore</td>
<td>Successful backup using the hcmds64backups command</td>
<td>6</td>
<td>KAPM05561-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed backup using the hcmds64backups command</td>
<td>3</td>
<td>KAPM05562-E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Successful full restore using the hcmds64db command</td>
<td>6</td>
<td>KAPM05563-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed full restore using the hcmds64db command</td>
<td>3</td>
<td>KAPM05564-E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Successful partial restore using the hcmds64db command</td>
<td>6</td>
<td>KAPM05565-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed partial restore using the hcmds64db command</td>
<td>3</td>
<td>KAPM05566-E</td>
<td></td>
</tr>
<tr>
<td>Audit log category and description</td>
<td>Type description</td>
<td>Audit event</td>
<td>Severity</td>
<td>Message ID</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------</td>
<td>-------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td>hcmds64db command</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database export or import</td>
<td>Successful database export</td>
<td>6</td>
<td>KAPM06543-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed database export</td>
<td>3</td>
<td>KAPM06544-E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Successful database import</td>
<td>6</td>
<td>KAPM06545-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed database import</td>
<td>3</td>
<td>KAPM06546-E</td>
<td></td>
</tr>
<tr>
<td>Database area creation or deletion</td>
<td>Successful database area creation</td>
<td>6</td>
<td>KAPM06348-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed database area creation</td>
<td>3</td>
<td>KAPM06349-E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Successful database area deletion</td>
<td>6</td>
<td>KAPM06350-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed database area deletion</td>
<td>3</td>
<td>KAPM06351-E</td>
<td></td>
</tr>
<tr>
<td>Authentication data input/output</td>
<td>Successful data output using the hcmds64authmove command</td>
<td>6</td>
<td>KAPM05832-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed data output using the hcmds64authmove command</td>
<td>3</td>
<td>KAPM05833-E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Successful data input using the hcmds64authmove command</td>
<td>6</td>
<td>KAPM05834-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed data input using the hcmds64authmove command</td>
<td>3</td>
<td>KAPM05835-E</td>
<td></td>
</tr>
<tr>
<td>Resource group creation</td>
<td>Successful resource group creation</td>
<td>6</td>
<td>KAPM07257-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed resource group creation</td>
<td>3</td>
<td>KAPM07258-E</td>
<td></td>
</tr>
<tr>
<td>Resource group deletion</td>
<td>Successful resource group deletion</td>
<td>6</td>
<td>KAPM07259-I</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed resource group deletion</td>
<td>3</td>
<td>KAPM07260-E</td>
<td></td>
</tr>
<tr>
<td>Editing resource group properties</td>
<td>Successful resource group property editing</td>
<td>6</td>
<td>KAPM07261-I</td>
<td></td>
</tr>
<tr>
<td>Audit log category and description</td>
<td>Type description</td>
<td>Audit event</td>
<td>Severity</td>
<td>Message ID</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------</td>
<td>-------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>Failed resource group property editing</td>
<td></td>
<td></td>
<td>3</td>
<td>KAPM07262-E</td>
</tr>
<tr>
<td>User group registration</td>
<td>Successful user group registration</td>
<td>6</td>
<td></td>
<td>KAPM07263-I</td>
</tr>
<tr>
<td></td>
<td>Failed user group registration</td>
<td>3</td>
<td></td>
<td>KAPM07264-E</td>
</tr>
<tr>
<td>User group deletion</td>
<td>Successful user group deletion</td>
<td>6</td>
<td></td>
<td>KAPM07265-I</td>
</tr>
<tr>
<td></td>
<td>Failed user group deletion</td>
<td>3</td>
<td></td>
<td>KAPM07266-E</td>
</tr>
<tr>
<td>User group update</td>
<td>Successful user group update</td>
<td>6</td>
<td></td>
<td>KAPM07267-I</td>
</tr>
<tr>
<td></td>
<td>Failed user group update</td>
<td>3</td>
<td></td>
<td>KAPM07268-E</td>
</tr>
<tr>
<td>Role registration</td>
<td>Successful registration of a role</td>
<td>6</td>
<td></td>
<td>KAPM07269-I</td>
</tr>
<tr>
<td></td>
<td>Failed registration of a role</td>
<td>3</td>
<td></td>
<td>KAPM07270-E</td>
</tr>
<tr>
<td>Role deletion</td>
<td>Successful deletion of a role</td>
<td>6</td>
<td></td>
<td>KAPM07271-I</td>
</tr>
<tr>
<td></td>
<td>Failed deletion of a role</td>
<td>3</td>
<td></td>
<td>KAPM07272-E</td>
</tr>
<tr>
<td>Role update</td>
<td>Successful update of a role</td>
<td>6</td>
<td></td>
<td>KAPM07273-I</td>
</tr>
<tr>
<td></td>
<td>Failed update of a role</td>
<td>3</td>
<td></td>
<td>KAPM07274-E</td>
</tr>
<tr>
<td>Assignment of a user account to a user group</td>
<td>Successful assignment of a user account to a user group</td>
<td>6</td>
<td></td>
<td>KAPM07275-I</td>
</tr>
<tr>
<td></td>
<td>Failed assignment of a user account to a user group</td>
<td>3</td>
<td></td>
<td>KAPM07276-E</td>
</tr>
<tr>
<td>Assignment of a permission to a role</td>
<td>Successful assignment of the permission to the role</td>
<td>6</td>
<td></td>
<td>KAPM07277-I</td>
</tr>
<tr>
<td></td>
<td>Failed assignment of the permission to the role</td>
<td>3</td>
<td></td>
<td>KAPM07278-E</td>
</tr>
<tr>
<td>Assignment of the following types of items:</td>
<td>Successful assignment of the following types of items:</td>
<td>6</td>
<td></td>
<td>KAPM07279-I</td>
</tr>
<tr>
<td>• User group and external</td>
<td>• User group and external</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

242  Troubleshooting
Hitachi Compute Systems Manager Installation and Configuration Guide
<table>
<thead>
<tr>
<th>Audit log category and description</th>
<th>Type description</th>
<th>Audit event</th>
<th>Severity</th>
<th>Message ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication group</td>
<td>authentication group</td>
<td>Failed assignment of the following types of items:</td>
<td>3</td>
<td>KAPM07280-E</td>
</tr>
<tr>
<td>• Resource group</td>
<td>• Resource group</td>
<td>• User group and external authentication group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Role</td>
<td>• Role</td>
<td>• Resource group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Role</td>
<td>• Role</td>
<td>• Role</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HCSM processing</td>
<td>Request reception</td>
<td></td>
<td>6</td>
<td>KASV27000-I</td>
</tr>
<tr>
<td></td>
<td>Response transmission (normal)</td>
<td></td>
<td>6</td>
<td>KASV27002-I</td>
</tr>
<tr>
<td></td>
<td>Response transmission (abnormal)</td>
<td></td>
<td>3</td>
<td>KASV27003-E</td>
</tr>
<tr>
<td>Task operations</td>
<td>Successful task cancellation</td>
<td></td>
<td>6</td>
<td>KASV27004-I</td>
</tr>
<tr>
<td></td>
<td>Failed task cancellation</td>
<td></td>
<td>4</td>
<td>KASV27005-W</td>
</tr>
<tr>
<td></td>
<td>Successful task registration</td>
<td></td>
<td>6</td>
<td>KASV27006-I</td>
</tr>
<tr>
<td></td>
<td>Failed task registration</td>
<td></td>
<td>4</td>
<td>KASV27007-W</td>
</tr>
<tr>
<td></td>
<td>Successful task deletion</td>
<td></td>
<td>6</td>
<td>KASV27008-I</td>
</tr>
<tr>
<td></td>
<td>Failed task deletion</td>
<td></td>
<td>4</td>
<td>KASV27009-W</td>
</tr>
<tr>
<td></td>
<td>Successful task execution</td>
<td></td>
<td>6</td>
<td>KASV27010-I</td>
</tr>
<tr>
<td></td>
<td>Failed task execution</td>
<td></td>
<td>4</td>
<td>KASV27011-W</td>
</tr>
<tr>
<td></td>
<td>Successful task rescheduling</td>
<td></td>
<td>6</td>
<td>KASV27012-I</td>
</tr>
<tr>
<td></td>
<td>Failed task rescheduling</td>
<td></td>
<td>4</td>
<td>KASV27013-W</td>
</tr>
<tr>
<td></td>
<td>Successful move to History</td>
<td></td>
<td>6</td>
<td>KASV27014-I</td>
</tr>
<tr>
<td></td>
<td>Failed move to History</td>
<td></td>
<td>4</td>
<td>KASV27015-W</td>
</tr>
</tbody>
</table>

**Related concepts**
- [About audit logs](#) on page 233
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:

```
```

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.

<table>
<thead>
<tr>
<th>Message output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>uniform-identifier</td>
<td>Fixed to CELFSS</td>
</tr>
<tr>
<td>unified-specification-revision-number</td>
<td>Fixed to 1.1</td>
</tr>
<tr>
<td>serial-number</td>
<td>Serial number of audit log messages</td>
</tr>
<tr>
<td>message-ID</td>
<td>Message ID</td>
</tr>
<tr>
<td>date-and-time</td>
<td>Date and time when the message was output</td>
</tr>
<tr>
<td>detected-entity</td>
<td>Component or process name</td>
</tr>
<tr>
<td>detected-location</td>
<td>Host name</td>
</tr>
<tr>
<td><strong>Message output</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>audit-event-type</td>
<td>Event type</td>
</tr>
<tr>
<td>audit-event-result</td>
<td>Event result</td>
</tr>
<tr>
<td>audit-event-result-subject-identification-information</td>
<td>Account ID, process ID, or IP address corresponding to the event</td>
</tr>
<tr>
<td>hardware-identification-information</td>
<td>Hardware model or serial number</td>
</tr>
<tr>
<td>location-information</td>
<td>Identification information for the hardware component</td>
</tr>
<tr>
<td>location-identification-information</td>
<td>Location identification information.</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully qualified domain name</td>
</tr>
<tr>
<td>redundancy-identification-information</td>
<td>Fully qualified domain name</td>
</tr>
<tr>
<td>agent-information</td>
<td>Agent information</td>
</tr>
<tr>
<td>request-source-host</td>
<td>Host name of the request sender</td>
</tr>
<tr>
<td>request-source-port-number</td>
<td>Port number of the request sender</td>
</tr>
<tr>
<td>request-destination-port-number</td>
<td>Port number of the request destination</td>
</tr>
<tr>
<td>request-destination-host</td>
<td>Host name of the request destination</td>
</tr>
<tr>
<td>batch-operation-identifier</td>
<td>Serial number of operations through the program</td>
</tr>
<tr>
<td>log-data-type-information</td>
<td>Fixed to BasicLog or DetailLog</td>
</tr>
<tr>
<td>application-identification-information</td>
<td>Program identification information</td>
</tr>
<tr>
<td>reserved-area</td>
<td>Not output - this is a reserved space.</td>
</tr>
<tr>
<td>message-text</td>
<td>Text describing the event</td>
</tr>
</tbody>
</table>

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 234

Related references

- [Audit event messages for processing requests](#) on page 246
- [Audit log categories and event descriptions](#) on page 235
- [Audit log detailed messages for system requests](#) on page 247
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 HCSM task event messages.

<table>
<thead>
<tr>
<th>Message text variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>unique-key</strong></td>
<td>A unique key value for a task. The key is output in the following format: uk=</td>
</tr>
<tr>
<td><strong>task-name</strong></td>
<td>The name of the task that completed the operation. The name is output in the following format: taskname=</td>
</tr>
</tbody>
</table>

Related tasks

- [Viewing the audit logs](#) on page 234

Related references

- [Audit log message format and information](#) on page 244
- [Audit log categories and event descriptions](#) on page 235
- [Audit log detailed messages for system requests](#) on page 247

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 HCSM server processing requests.

<table>
<thead>
<tr>
<th>Message text variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>unique-ID</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>detailed-message</strong></td>
<td>Detailed information about the request.</td>
</tr>
<tr>
<td><strong>error-message-ID</strong></td>
<td>The ID of the error message.</td>
</tr>
</tbody>
</table>

Related tasks

- [Viewing the audit logs](#) on page 234

Related references

- [Audit log message format and information](#) on page 244
- [Audit log categories and event descriptions](#) on page 235
Audit log detailed messages for system requests

The output format of a detailed message related to an HCSM receive request is as follows:

```
command target [parameter]
```

The variable within the brackets ([ ] ) might not appear.

Detailed HCSM 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.

<table>
<thead>
<tr>
<th>Output character string</th>
<th>Full name</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add</td>
<td>Addition</td>
</tr>
<tr>
<td>Del</td>
<td>Delete</td>
<td>Deletion</td>
</tr>
<tr>
<td>Get</td>
<td>Get</td>
<td>Acquisition</td>
</tr>
<tr>
<td>Mod</td>
<td>Modify</td>
<td>Modification</td>
</tr>
<tr>
<td>Set</td>
<td>Set</td>
<td>Setting</td>
</tr>
</tbody>
</table>

- **target**—Information that identifies the operation to perform. The following table provides detailed target output information.

<table>
<thead>
<tr>
<th>Output character string</th>
<th>Full name</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts</td>
<td>Alerts</td>
<td>Alert information reference or deletion</td>
</tr>
<tr>
<td>Chassis</td>
<td>Chassis</td>
<td>Chassis setting or reference</td>
</tr>
<tr>
<td>Server</td>
<td>Server</td>
<td>Server setting or reference</td>
</tr>
<tr>
<td>Host</td>
<td>Host</td>
<td>Host setting or reference</td>
</tr>
<tr>
<td>LGrp</td>
<td>LogicalGroup</td>
<td>Logical group setting or reference</td>
</tr>
<tr>
<td>SrvI</td>
<td>ServerInfo</td>
<td>HCSM information acquisition</td>
</tr>
<tr>
<td>User</td>
<td>User</td>
<td>User setting or reference</td>
</tr>
</tbody>
</table>

- **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.

<table>
<thead>
<tr>
<th>Output character string</th>
<th>Full name and content</th>
<th>Sequence of attribute values output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>Alert (information about the HCSM error or a managed resource error)</td>
<td>alert number</td>
</tr>
<tr>
<td>Chassis</td>
<td>Chassis (chassis information about the error)</td>
<td>chassis name, chassis IP address</td>
</tr>
<tr>
<td>Server</td>
<td>Server (server information)</td>
<td>server name, server IP address</td>
</tr>
<tr>
<td>Host</td>
<td>Host (host information)</td>
<td>host name, host IP address</td>
</tr>
<tr>
<td>User</td>
<td>User (account information of a single HCSM user)</td>
<td>user ID</td>
</tr>
</tbody>
</table>

**Related tasks**

- [Viewing the audit logs](#) on page 234

**Related references**

- [Audit log message format and information](#) on page 244
- [Audit log categories and event descriptions](#) on page 235
- [Audit event messages for processing requests](#) on page 246
- [Audit event messages for tasks](#) on page 246

**Log file settings**

This module provides information about configuring log file settings.

**About log file settings**

When using Hitachi Compute Systems Manager (HCSM), 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 HCSM Message log files:
• Maximum size of the log file
• Maximum number of log files
• Logging level

Related tasks
• Changing Hitachi Compute Systems Manager log file settings on page 249

Changing Hitachi Compute Systems Manager log file settings

You can change the HCSM log file settings based on your log file requirements.

Procedure
1. Stop HCSM.
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 HCSM.

Result
The new log file settings take effect when HCSM starts.

Related concepts
• About log file settings on page 248

Related tasks
• Starting Hitachi Compute Systems Manager on page 166
• Stopping Hitachi Compute Systems Manager on page 167
Related references

- Properties related to Hitachi Compute Systems Manager server log files (logger.properties) on page 259
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
- [ ] Hitachi Command Suite Common Component ports
- [ ] Deployment Manager ports
Hitachi Compute Systems Manager server ports

The Hitachi Compute Systems Manager server uses the ports listed in the following table:

<table>
<thead>
<tr>
<th>Port number (default)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>162/UDP</td>
<td>These ports are used for SNMP trap reception. If 162/UDP is being used by another product, 22601/UDP is recommended.</td>
</tr>
<tr>
<td>22610/TCP</td>
<td>Used for communication with the Hitachi Device Manager.</td>
</tr>
<tr>
<td>22611/TCP</td>
<td>Used for receiving alerts from a Hitachi server.</td>
</tr>
</tbody>
</table>

Related tasks
- Changing Hitachi Compute Systems Manager ports on page 74

Related references
- HCSM properties requiring updates for port number changes on page 73

Hitachi Command Suite Common Component ports

The Hitachi Command Suite (HCS) Common Component uses the ports listed in the following table:

<table>
<thead>
<tr>
<th>Port number (default)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22015/TCP</td>
<td>This port is used for access to the HCS 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 HCS products, change the port for either that product or for HCS Common Component. To block non-SSL communication to the management server from external servers, you must edit the user_httpsd.conf file.</td>
</tr>
<tr>
<td>22016/TCP</td>
<td>This port is used for access to the HCS 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 HCS products, change the port for either that product or for HCS Common Component.</td>
</tr>
<tr>
<td>22017/TCP to 22026/TCP</td>
<td>These ports are reserved.</td>
</tr>
<tr>
<td>22027/TCP</td>
<td>This port is used for internal communication with HCS Common Component (to communicate with the Web server).</td>
</tr>
</tbody>
</table>
### Port number (default)

<table>
<thead>
<tr>
<th>Port number (default)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If this port number is used by a product other than HCS products, change the port for either that product or for HCS Common Component.</td>
</tr>
<tr>
<td>22028/TCP</td>
<td>This port is used for internal communication with HCS Common Component (to receive termination messages from the Web server).</td>
</tr>
<tr>
<td></td>
<td>If this port number is used by a product other than HCS products, change the port for either that product or for HCS Common Component.</td>
</tr>
<tr>
<td>22029/TCP to 22030/TCP</td>
<td>These ports are reserved.</td>
</tr>
<tr>
<td>22031/TCP</td>
<td>This port is used for internal communication with Hitachi Command Suite Common Component (communication with the HSSO-dedicated Web server).</td>
</tr>
<tr>
<td></td>
<td>If this port number is used by a product other than HCS products, change the port for either that product or for HCS Common Component.</td>
</tr>
<tr>
<td>22032/TCP</td>
<td>This port is used for internal communication with HCS Common Component (to communicate with the database).</td>
</tr>
<tr>
<td></td>
<td>If this port number is used by a product other than HCS products, change the port for either that product or for HCS Common Component.</td>
</tr>
<tr>
<td>22033/TCP</td>
<td>This port is used for internal communication with HCS Common Component (to communicate with the Web server).</td>
</tr>
<tr>
<td></td>
<td>If this port number is used by a product other than HCS products, change the port for either that product or for HCS Common Component.</td>
</tr>
<tr>
<td>22034/TCP</td>
<td>This port is used for internal communication with HCS Common Component (to receive termination messages from the Web server).</td>
</tr>
<tr>
<td></td>
<td>If this port number is used by a product other than HCS products, change the port for either that product or for HCS Common Component.</td>
</tr>
</tbody>
</table>

**Related tasks**

- [Changing Hitachi Compute Systems Manager ports](#) on page 74

**Related references**

- [Hitachi Compute Systems Manager server ports](#) on page 252
- [HCS properties requiring updates for port number changes](#) on page 71

## Deployment Manager ports

Deployment Manager uses the ports listed in the following table:
<table>
<thead>
<tr>
<th>Port number (default)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>67/UDP</td>
<td>Used for PXE booting of managed resources. This port number cannot be changed.</td>
</tr>
<tr>
<td>69/UDP</td>
<td>Used for PXE booting of managed resources. This port number cannot be changed.</td>
</tr>
<tr>
<td>80/TCP*</td>
<td>Used for internal communication with the IIS service process. This port number can be changed.</td>
</tr>
<tr>
<td>4011/UDP</td>
<td>Used for PXE booting of managed resources. This port number cannot be changed.</td>
</tr>
<tr>
<td>26500/TCP*</td>
<td>Used for internal communication between the IIS service process and Deployment Manager. This port number can be changed.</td>
</tr>
<tr>
<td>26501/TCP or 56020/TCP*</td>
<td>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).</td>
</tr>
<tr>
<td>26502/TCP or 56022/TCP*</td>
<td>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).</td>
</tr>
<tr>
<td>26503/TCP or 56030/TCP*</td>
<td>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).</td>
</tr>
<tr>
<td>26504/TCP to 26507/TCP</td>
<td>These ports are reserved.</td>
</tr>
<tr>
<td>26508/TCP or 56023/TCP*</td>
<td>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).</td>
</tr>
<tr>
<td>56011/TCP</td>
<td>These ports are reserved.</td>
</tr>
<tr>
<td>56024/TCP</td>
<td></td>
</tr>
<tr>
<td>56028/TCP</td>
<td></td>
</tr>
<tr>
<td>56060/TCP</td>
<td></td>
</tr>
</tbody>
</table>

* 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 162

**Related references**
- [Properties related to Deployment Manager ports (port.ini)](#) on page 287
This appendix includes the Hitachi Compute Systems Manager (HCSM) and Hitachi Command Suite (HCS) Common Component properties.

- Properties for Hitachi Compute Systems Manager server
- Properties for Hitachi Command Suite Common Component
- Properties related to Deployment Manager ports (port.ini)
Properties for Hitachi Compute Systems Manager server

This module provides information about the Hitachi Compute Systems Manager (HCSM) server properties files.

About the Hitachi Compute Systems Manager server properties

The Hitachi Compute Systems Manager (HCSM) server properties define the settings for HCSM ports and logs. When you change a property, the new setting takes affect when you restart HCSM.

Related concepts

- About the Hitachi Command Suite Common Component properties on page 260

Related references

- Hitachi Compute Systems Manager server properties files on page 256
- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 257
- Properties related to Hitachi Compute Systems Manager server log files (logger.properties) on page 259

Hitachi Compute Systems Manager server properties files

HCSM settings for ports and logs are stored in the properties files listed in the following table:

<table>
<thead>
<tr>
<th>File name</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 HCSM server. |
| logger.properties | In Windows:
    \HCSM-installation-directory\ComputeSystemsManager\conf\logger.properties
    In Linux:
    \HCSM-installation-directory/ | This file includes log output-related properties. |
Related concepts

- **About the Hitachi Compute Systems Manager server properties** on page 256

Related references

- **Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties)** on page 257
- **Properties related to Hitachi Compute Systems Manager server log files (logger.properties)** on page 259

**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 HCSM server and to change the settings related to the HCSM server functions, such as the command timeout period and temperature display.

The HCSM `user.properties` file includes the port-related and function-related parameters listed in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp.trap.receive.port</code></td>
<td>Specifies the port for receiving SNMP traps.</td>
</tr>
<tr>
<td></td>
<td>Value range: 1 to 65535</td>
</tr>
<tr>
<td></td>
<td>The default value is 162 or 22601.</td>
</tr>
<tr>
<td><code>server.rmi.port</code></td>
<td>Specifies the port for receiving RMI requests from Hitachi Device Manager.</td>
</tr>
<tr>
<td></td>
<td>Value range: 1 to 65535</td>
</tr>
<tr>
<td></td>
<td>The default value is 22610.</td>
</tr>
<tr>
<td><code>server.process.timeout</code></td>
<td>Specifies the timeout period for processing commands.</td>
</tr>
<tr>
<td></td>
<td>Value range: 0 to 100000 (seconds)</td>
</tr>
<tr>
<td></td>
<td>The default value is 1800 (seconds)</td>
</tr>
<tr>
<td></td>
<td>If you do not want a command to timeout until it finishes processing, specify 0.</td>
</tr>
<tr>
<td><code>svp.alert.receive.port</code></td>
<td>Specifies the port for receiving alerts from a Hitachi server.</td>
</tr>
<tr>
<td></td>
<td>Value range: 1 to 65535</td>
</tr>
<tr>
<td></td>
<td>The default value is 22611.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>hcsm.keystore.filename</td>
<td>Specifies the name of the keystore file used by HCSM for SSL communication between the management server and a Hitachi server (including an LPAR Manager running on a blade server).</td>
</tr>
<tr>
<td>Value: character_string</td>
<td>The default value is <code>hcsm_default.keystore</code>.</td>
</tr>
<tr>
<td>powermonitoring.temperature.unit</td>
<td>Specifies the temperature measurement unit.</td>
</tr>
<tr>
<td>Value: F or C (represents Fahrenheit and Celsius)</td>
<td>The default value is F.</td>
</tr>
<tr>
<td>hcsm.shared.directory</td>
<td>Specifies the path of the HCSM work directory.</td>
</tr>
<tr>
<td>Value: character_string</td>
<td>If the specified directory does not exist, the default path is used. The default is as follows:</td>
</tr>
<tr>
<td></td>
<td>In Windows:</td>
</tr>
<tr>
<td></td>
<td><code>HCSM-installation-folder\shared</code></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• If you are using HCSM in a cluster environment, specify the path of a folder on the shared disk.</td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
</tr>
<tr>
<td></td>
<td><code>HCSM-installation-directory/shared</code></td>
</tr>
<tr>
<td>winrm.maxEnvelopeSize</td>
<td>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.</td>
</tr>
<tr>
<td>Value range: 512 to 4194304</td>
<td>The default value is 512.</td>
</tr>
<tr>
<td>hcsm.certification.verify</td>
<td>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).</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Disable: Does not check the certificate.</td>
<td>The default value is Disable.</td>
</tr>
<tr>
<td>If you specify Enable, you must register the certificate for the Hitachi server to the keystore of the management server.</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| hvm.lpar.migration.allowplaintext            | 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. |

**Related concepts**

- [About the Hitachi Compute Systems Manager server properties](#) on page 256

**Related references**

- [Hitachi Compute Systems Manager server properties files](#) on page 256

**Properties related to Hitachi Compute Systems Manager server log files (logger.properties)**

You can change the HCSM log file settings by editing the `logger.properties` file listed in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.  
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.                                                                                                               |
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 (HCS) Common Component properties define the settings for HCS Common Component functionality. When you change a property, the new setting takes affect when you restart HCSM.

Note: Any changes made to HCS Common Component properties files are applied to all HCS products that run in the same environment.

Properties files for Hitachi Command Suite Common Component

The properties files for Hitachi Command Suite (HCS) Common Component are listed in the following table:

<table>
<thead>
<tr>
<th>File name</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_httpsd.conf</td>
<td>In Windows: \ HCS-Common-Component-installation-directory\uCP\httpsd\conf \user_httpsd.conf</td>
<td>Contains properties related to the Web server.</td>
</tr>
<tr>
<td>File name</td>
<td>Location</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>usrconf.properties (SSO)</td>
<td><strong>In Windows:</strong> HCS-Common-Component-installation-directory/uCPSB/httpsd/conf getUser_httpsd.conf &lt;br&gt;<strong>In Linux:</strong> HCS-Common-Component-installation-directory/uCPSB/httpsd/conf getUser_httpsd.conf</td>
<td></td>
</tr>
<tr>
<td>usrconf.properties (HCSM)</td>
<td><strong>In Windows:</strong> HCS-Common-Component-installation-directory/uCPSB/CC/web/containers/HBase64StgMgmtSSOService/usrconf/usrcnf.usrcnf.properties &lt;br&gt;<strong>In Linux:</strong> HCS-Common-Component-installation-directory/uCPSB/CC/web/containers/HBase64StgMgmtSSOService/usrconf/usrcnf.usrcnf.properties</td>
<td></td>
</tr>
<tr>
<td>workers.properties</td>
<td><strong>In Windows:</strong> HCS-Common-Component-installation-directory/uCPSB/CC/web/redirector/ workers.properties &lt;br&gt;<strong>In Linux:</strong> HCS-Common-Component-installation-directory/uCPSB/CC/web/redirector/ workers.properties</td>
<td></td>
</tr>
<tr>
<td>user_hsst_httpsd.conf</td>
<td><strong>In Windows:</strong> HCS-Common-Component-installation-directory/uCPSB/conf/ user_hsst_httpsd.conf &lt;br&gt;<strong>In Linux:</strong> HCS-Common-Component-installation-directory/uCPSB/conf/ user_hsst_httpsd.conf</td>
<td></td>
</tr>
<tr>
<td>HiRDB.ini</td>
<td><strong>In Windows:</strong> HCS-Common-Component-installation-directory/HDB/CONF/emb/HiRDB.ini &lt;br&gt;<strong>In Linux:</strong> HCS-Common-Component-installation-directory/HDB/CONF/emb/HiRDB.ini</td>
<td>Contains properties related to the database.</td>
</tr>
<tr>
<td>File name</td>
<td>Location In Windows:</td>
<td>Location In Linux:</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>pdsys</td>
<td>HCS-Common-Component-installation-directory\HDB\CONF\pdsys</td>
<td>HCS-Common-Component-installation-directory/HDB/CONF/pdsys</td>
</tr>
<tr>
<td>def_pdsys</td>
<td>HCS-Common-Component-installation-directory\database\work\def_pdsys</td>
<td>HCS-Common-Component-installation-directory/database/work/def_pdsys</td>
</tr>
<tr>
<td>pdutsys</td>
<td>HCS-Common-Component-installation-directory\HDB\CONF\pdutsys</td>
<td>HCS-Common-Component-installation-directory/HDB/CONF/pdutsys</td>
</tr>
<tr>
<td>def_pdutsys</td>
<td>HCS-Common-Component-installation-directory\database\work\def_pdutsys</td>
<td>HCS-Common-Component-installation-directory/database/work/def_pdutsys</td>
</tr>
<tr>
<td>user.conf</td>
<td>HCS-Common-Component-installation-directory\conf\user.conf</td>
<td>HCS-Common-Component-installation-directory/conf/user.conf</td>
</tr>
<tr>
<td>exauth.properties</td>
<td>HCS-Common-Component-installation-directory\conf\exauth.properties</td>
<td>HCS-Common-Component-installation-directory/conf/exauth.properties</td>
</tr>
<tr>
<td>File name</td>
<td>Location</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>auditlog.conf</td>
<td>In Windows:</td>
<td>HCS-Common-Component-installation-directory\conf\sec\auditlog.conf</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In Linux:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HCS-Common-Component-installation-directory\conf\sec\auditlog.conf</td>
</tr>
<tr>
<td>cluster.conf</td>
<td>HCS-Common-Component-installation-directory\conf\clu ster.conf</td>
<td>Contains properties related to clustering.</td>
</tr>
</tbody>
</table>

**Related references**

- Properties related to web server communication including SSL settings (*user_httpsd.conf*) on page 263
- Properties related to the web server for HCSM (*usrconf.properties*) on page 267
- Properties related to the web server (*workers.properties*) on page 268
- Properties related to the HSSO-dedicated web server (*user_hsso_httpsd.conf*) on page 268
- Properties related to the database (*HiRDB.ini*) on page 269
- Properties related to the database (*pdsys*) on page 269
- Properties related to the database (*def_pdsys*) on page 270
- Properties related to the database (*pdutsys*) on page 271
- Properties related to the database (*def_pdutsys*) on page 271
- Properties related to System account locking (*user.conf*) on page 271
- Properties related to LDAP directory server connections (*exauth.properties*) on page 272
- Example properties file for external LDAP directory server connections (*exauth.properties*) on page 276
- Example properties file for Kerberos server connections (*exauth.properties*) on page 283
- Properties related to audit logs (*auditlog.conf*) on page 285
- Properties related to clustering (*cluster.conf*) on page 287

**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:
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ServerName host-name</strong></td>
<td>Specifies the host name or IP address of the HCSM management server.</td>
</tr>
<tr>
<td></td>
<td>By default, this is the host name set for the OS.</td>
</tr>
<tr>
<td></td>
<td>You must update this parameter if the host name or IP address of the HCSM server changes. If making a change, we recommend specifying a host name.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Listen port-number</strong></td>
<td>Specifies the port number for accessing the HBase 64 Storage Mgmt Web Service.</td>
</tr>
<tr>
<td></td>
<td>The default value is 22015.</td>
</tr>
<tr>
<td></td>
<td>If this value changes, the same port number must be specified for the <code>Listen [::]:</code> property and the <code>#Listen 127.0.0.1:</code> property.</td>
</tr>
<tr>
<td><strong>Listen [::]: port-number</strong></td>
<td>Specifies the port number for accessing the HBase 64 Storage Mgmt Web Service.</td>
</tr>
<tr>
<td></td>
<td>The default value is 22015.</td>
</tr>
<tr>
<td></td>
<td>If this value changes, the same port number must be specified for the <code>Listen</code> property and the <code>#Listen 127.0.0.1:</code> property.</td>
</tr>
<tr>
<td><code>#Listen 127.0.0.1: port-number</code></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Specifies the port number for accessing the HBase 64 Storage Mgmt Web Service.</td>
</tr>
<tr>
<td></td>
<td>The default value is 22015.</td>
</tr>
<tr>
<td></td>
<td>If this value changes, the same port number must be specified for the <code>Listen</code> property and the <code>#Listen [::]:</code> property.</td>
</tr>
<tr>
<td><code>#Listen port-number</code></td>
<td>Parameter for SSL communication. To use SSL, delete the preceding hash mark (#).</td>
</tr>
<tr>
<td></td>
<td>Specifies the port number for accessing HBase 64 Storage Mgmt Web Service using SSL.</td>
</tr>
<tr>
<td></td>
<td>The default value is 22016. If this is changed, the same port number must be specified for the <code>#Listen [::]:</code> property.</td>
</tr>
<tr>
<td><code>#Listen [::]: port-number</code></td>
<td>Parameter for SSL communication. To use SSL, do not delete the preceding hash mark (#).</td>
</tr>
<tr>
<td></td>
<td>Specifies the port number for accessing HBase 64 Storage Mgmt Web Service using SSL.</td>
</tr>
<tr>
<td></td>
<td>The default value is 22016. The port number of the <code>#Listen</code> property must be specified.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| `<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 HCSM management server.  
By default, this is the host name set for the OS.  
You must update this parameter if the host name of the HCSM 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.  
Do not specify a symbolic link and junction for the path.                                                                                               |
| `SSLCA_certificateFile` | 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. |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># &lt;/VirtualHost&gt;</td>
<td>Parameter for SSL communication. To use SSL, delete the preceding hash mark (#).</td>
</tr>
<tr>
<td>&lt;Location /ComputeSystemsManager&gt;</td>
<td>Parameter for restricting management client access. To restrict access, add this property to the last line of the user_httpd.conf file using the following format:</td>
</tr>
<tr>
<td></td>
<td>&lt;Location /ComputeSystemsManager&gt;</td>
</tr>
<tr>
<td></td>
<td>order allow, deny</td>
</tr>
<tr>
<td></td>
<td>allow from management-client [management-client...]</td>
</tr>
<tr>
<td></td>
<td>&lt;/Location&gt;</td>
</tr>
<tr>
<td></td>
<td>For additional information about how to restrict clients using this property, see the following section.</td>
</tr>
</tbody>
</table>

You can control HCSM 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 HCS 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 125
• Setting up SSL on the server for secure client communication on page 111

Related references
• Properties files for Hitachi Command Suite Common Component on page 260

Properties related to the web server for HCSM (usrconf.properties)

The usrconf.properties file includes parameters for the HCSM web server communication.

Note: The usrconf.properties file exists for each Web container service.

The following table lists the HCSM usrconf.properties file parameters:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webserver.connector.ajp13.port</td>
<td>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.</td>
</tr>
<tr>
<td>webserver.shutdown.port</td>
<td>Specifies the port used for receiving termination messages from the Web server. The default value is 22028.</td>
</tr>
</tbody>
</table>

The following table lists the usrconf.properties file parameters related to the web container server for Common Component single sign-on:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webserver.connector.ajp13.port</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webserver.shutdown.port</td>
<td>Specifies the port used for receiving termination messages from the Web server.</td>
</tr>
<tr>
<td></td>
<td>The default value is 22034.</td>
</tr>
</tbody>
</table>

**Related references**

- [Properties files for Hitachi Command Suite Common Component](#) on page 260
- [Properties related to the web server (workers.properties)](#) on page 268

### 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:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>worker.ComputeSystemsManageWebService.port</td>
<td>Specifies the port number for accessing the Web server.</td>
</tr>
<tr>
<td></td>
<td>The default value is 22027.</td>
</tr>
<tr>
<td></td>
<td>If you change this value, you must update the webserver.connector.ajp13.port property in the usrcf.properties file for HCSM so that it is the same.</td>
</tr>
<tr>
<td>worker.HBase64StgMgmtSSOService.port</td>
<td>Specifies the port number for accessing the Web server.</td>
</tr>
<tr>
<td></td>
<td>The default value is 22033.</td>
</tr>
<tr>
<td></td>
<td>If you change this value, you must update the webserver.connector.ajp13.port property in the usrcf.properties file for Common Component single sign-on so that it is the same.</td>
</tr>
</tbody>
</table>

**Related references**

- [Properties files for Hitachi Command Suite Common Component](#) on page 260
- [Properties related to the web server for HCSM (usrconf.properties)](#) on page 267

### 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:
### 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 260

### Properties related to the database (HiRDB.ini)

The Common Component `HiRDB.ini` properties file contains the database-related parameters listed in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDNAMEPORT</td>
<td>Specifies the port number used for the database.</td>
</tr>
<tr>
<td></td>
<td>The default value is 22032.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>PDHOST</td>
<td>Specifies the IP address. You usually do not change this value.</td>
</tr>
<tr>
<td></td>
<td>Change this value if the host name or IP address of the HCSM management server changes.</td>
</tr>
<tr>
<td></td>
<td>If the old IP address is specified, change the value to the loopback address 127.0.0.1.</td>
</tr>
</tbody>
</table>

**Related references**

- Properties files for Hitachi Command Suite Common Component on page 260
- Properties related to the database (pdsys) on page 269
- Properties related to the database (def_pdsys) on page 270

### Properties related to the database (pdsys)

The Common Component `pdsys` properties file contains the database-related parameters listed in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pd_name_port</td>
<td>Specifies the port number used for the database.</td>
</tr>
<tr>
<td></td>
<td>The default value is 22032.</td>
</tr>
</tbody>
</table>
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 HCSM 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 260
- [Properties related to the database (HiRDB.ini)](#) on page 269
- [Properties related to the database (def_pdsys)](#) on page 270

### 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>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pd_name_port</td>
<td>Specifies the port number used for the database.</td>
</tr>
<tr>
<td></td>
<td>The default value is 22032.</td>
</tr>
<tr>
<td></td>
<td>If you change this value, you must update the port number in the <strong>PDNAMEPORT</strong> property in the <strong>HiRDB.ini</strong> file and the <strong>pd_name_port</strong> property in the <strong>pdsys</strong> file.</td>
</tr>
<tr>
<td>pdunit -x</td>
<td>Specifies the IP address. You usually do not change this value.</td>
</tr>
<tr>
<td></td>
<td>Change this value if the host name or IP address of the HCSM management server changes.</td>
</tr>
<tr>
<td></td>
<td>If the old IP address is specified, change the value to the loopback address 127.0.0.1.</td>
</tr>
</tbody>
</table>

### Related references

- [Properties files for Hitachi Command Suite Common Component](#) on page 260
- [Properties related to the database (HiRDB.ini)](#) on page 269
- [Properties related to the database (def_pdsys)](#) on page 269
Properties related to the database (pdutsys)

The Common Component pdutdsys properties file contains the database-related parameters listed in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pd_hostname</td>
<td>Specifies the IP address. You usually do not change this value.</td>
</tr>
<tr>
<td></td>
<td>Change this value if the host name or IP address of the HCSM management server changes.</td>
</tr>
<tr>
<td></td>
<td>If the old IP address is specified, change the value to the loopback address 127.0.0.1.</td>
</tr>
</tbody>
</table>

Related references

- Properties files for Hitachi Command Suite Common Component on page 260
- Properties related to the database (HiRDB.ini) on page 269
- Properties related to the database (def_pdutsys) on page 271

Properties related to the database (def_pdutsys)

The Common Component def_pdutsys properties file contains the database-related parameters listed in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pd_hostname</td>
<td>Specifies the IP address. You usually do not change this value.</td>
</tr>
<tr>
<td></td>
<td>Change this value if the host name or IP address of the HCSM management server changes.</td>
</tr>
<tr>
<td></td>
<td>If the old IP address is specified, change the value to the loopback address 127.0.0.1.</td>
</tr>
</tbody>
</table>

Related references

- Properties files for Hitachi Command Suite Common Component on page 260
- Properties related to the database (HiRDB.ini) on page 269
- Properties related to the database (pdutsys) on page 271

Properties related to System account locking (user.conf)

The Common Component user.conf file includes the user account parameters listed in the following table:
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.lock.system</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Related tasks**

- [Enabling System account locking](#) on page 69

**Related references**

- Properties files for Hitachi Command Suite Common Component on page 260

**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 external authentication server information or use a DNS server to obtain the 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, HCSM ignores the value and uses the default.

The `exauth.properties` file parameters are listed in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>Specifies the type of external authentication server.</td>
<td>ldap or internal Default value: internal (used when not connecting to an external server)</td>
</tr>
<tr>
<td>auth.server.name</td>
<td>Specifies the server identification name of the LDAP directory server.</td>
<td>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</td>
</tr>
<tr>
<td>auth.group.mapping</td>
<td>Specifies whether to link to an external authorization server.</td>
<td>true or false Default value: false (used when not connecting to an external authorization server)</td>
</tr>
<tr>
<td>auth.ocsp.enable</td>
<td>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.</td>
<td>true or false Default value: false</td>
</tr>
<tr>
<td>auth.ocsp.responderURL</td>
<td>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</td>
<td>URL of an OCSP responder Default value: none</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Possible Values</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>auth.ldap.auth.server.name-property-value.protocol</td>
<td>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</td>
<td>ldap or tls Default value: none</td>
</tr>
<tr>
<td>auth.ldap.auth.server.name-property-value.host</td>
<td>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.</td>
<td>host name or IP address Default: none</td>
</tr>
<tr>
<td>auth.ldap.auth.server.name-property-value.port</td>
<td>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.</td>
<td>1 to 65535 Default value: 389</td>
</tr>
<tr>
<td>auth.ldap.auth.server.name-property-value.timeout</td>
<td>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.</td>
<td>0 to 120 (seconds) Default value: 15</td>
</tr>
<tr>
<td>auth.ldap.auth.server.name-property-value.attr</td>
<td>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 identifying the user. The value stored in this attribute is used as the user ID for HCSM. (This value must not include characters that are invalid for HCSM user)</td>
<td>Default value: sAMAccountName Modify this value for your configuration.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Possible Values</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>auth.ldap.auth.server.name-property-value_basedn</td>
<td>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.</td>
<td>Default value: none</td>
</tr>
<tr>
<td>auth.ldap.auth.server.name-property-value_retry.interval</td>
<td>Specifies the retry interval when an LDAP directory server connection attempt fails.</td>
<td>1 to 60 (seconds) Default value: 1</td>
</tr>
<tr>
<td>auth.ldap.auth.server.name-property-value_retry.times</td>
<td>Specifies the number of retries to attempt when an LDAP directory server connection fails. If you specify 0, no retries are attempted.</td>
<td>0 to 50 Default value: 20</td>
</tr>
<tr>
<td>auth.ldap.auth.server.name-property-value_domain.name</td>
<td>Specifies the name of the domain managed by the LDAP directory server. This property is required for the following configurations: • Using a DNS server to obtain LDAP directory server information.</td>
<td>Default value: none</td>
</tr>
</tbody>
</table>
When using HCSM, 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 HCSM 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:

```properties
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ocsp.enable=false
```

### Related concepts
- [About setting up secure communication for an external authentication server](#) on page 125

### Related tasks
- [Configuring an LDAP server connection](#) on page 133

### Related references
- [Properties files for Hitachi Command Suite Common Component](#) on page 260
- [Example properties file for external LDAP directory server connections (exauth.properties)](#) on page 276
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 authentication 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 authentication 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 110
- [About setting up secure communication for an external authentication server](#) on page 125

**Related tasks**

- [Configuring an LDAP server connection](#) on page 133
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 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, HCSM ignores the value and uses the default.

The exauth.properties file parameters are listed in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>Specifies the type of external authentication server.</td>
<td>kerberos or internal</td>
</tr>
<tr>
<td></td>
<td>Specify kerberos (to connect to an external Kerberos server).</td>
<td>Default value: internal (used when not connecting to an external server)</td>
</tr>
</tbody>
</table>

Hitachi Compute Systems Manager Installation and Configuration Guide
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.group.mapping</td>
<td>Specifies whether to link to an external authorization server.</td>
<td>true or false&lt;br&gt;Default value: false&lt;br&gt;(used when not connecting to an external authorization server)</td>
</tr>
<tr>
<td></td>
<td>Specify true to connect to an external authorization server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specify false if you do not want to connect to an external authorization server.</td>
<td></td>
</tr>
<tr>
<td>auth.ocsp.enable</td>
<td>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.</td>
<td>true or false&lt;br&gt;Default value: false</td>
</tr>
<tr>
<td></td>
<td>Specify true to validate the electronic signature certificate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specify false if you do not want to validate the electronic signature certificate.</td>
<td></td>
</tr>
<tr>
<td>auth.ocsp.responderURL</td>
<td>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.</td>
<td>URL of an OCSP responder&lt;br&gt;Default value: none</td>
</tr>
<tr>
<td>auth.kerberos.default_realm</td>
<td>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)</td>
<td>realm name&lt;br&gt;Default value: none</td>
</tr>
<tr>
<td>auth.kerberos.dns_lookup_kdc</td>
<td>Specifies whether to look up the Kerberos server using DNS. This attribute is required. Specify true&lt;br&gt;If all the following attributes values are already set, the Kerberos server will not be looked up by the DNS server.</td>
<td>true or false&lt;br&gt;Default value: false</td>
</tr>
<tr>
<td></td>
<td>• realm_name&lt;br&gt;• value-specified-for-realm_name.realm&lt;br&gt;• value-specified-for-realm_name.kdc</td>
<td></td>
</tr>
<tr>
<td>auth.kerberos.default_tkt_enctypes</td>
<td>Specifies the encryption type used for Kerberos authentication. You can use the following encryption types:</td>
<td>encryption type&lt;br&gt;Default value: none&lt;br&gt;(DES-CBC-MD5 is used for authentication.)</td>
</tr>
<tr>
<td></td>
<td>• AES128-CTS&lt;br&gt;• AES256-CTS&lt;br&gt;• RC4-HMAC&lt;br&gt;• DES3-CBC-SHA1&lt;br&gt;• DES-CBC-MD5&lt;br&gt;• DES-CBC-CRC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you want to specify multiple encryption types, use a comma to separate the encryption types.</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Possible Values</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>auth.kerberos.clockske</strong>w</td>
<td>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.</td>
<td>0 to 300 (seconds) Default: 300</td>
</tr>
<tr>
<td><strong>auth.kerberos.timeout</strong></td>
<td>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.</td>
<td>0 to 120 (seconds) Default value: 3</td>
</tr>
<tr>
<td><strong>auth.kerberos.realm_name</strong></td>
<td>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.</td>
<td>realm identification names Default value: none</td>
</tr>
<tr>
<td><strong>auth.kerberos.value-specified-for-auth.kerberos.realm_name.realm</strong></td>
<td>Specifies the name of the realm set on the Kerberos server. (required) Use the value specified in the &quot;realm-name&quot; property.</td>
<td>realm name Default value: none</td>
</tr>
</tbody>
</table>
| **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`  
  - `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:  
  - `host-name-or-IP-address[:port-number],host-name-or-IP-address[:port-number],...` | Default value: none |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.group.realm-name.protocol</td>
<td>Specifies the protocol for connecting to the LDAP directory server (required).</td>
<td>ldap or tls</td>
</tr>
<tr>
<td></td>
<td>When communicating in plain text format, specify ldap.</td>
<td>Default value: ldap</td>
</tr>
<tr>
<td></td>
<td>When using StartTLS communication, specify tls.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Before specifying tls, ensure that one of the following encryption methods is supported on the Kerberos server:</td>
<td></td>
</tr>
</tbody>
</table>
|                               | • TLS_RSA_WITH_AES_256_CBC_SHA  
|                               | • TLS_RSA_WITH_AES_128_CBC_SHA  
<p>|                               | • SSL_RSA_WITH_3DES_EDE_CBC_SHA |                 |
|                               | <strong>Note:</strong> 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. |                 |
| auth.group.realm-name.port    | Specifies port number of the LDAP directory server.                                                                                                                                                           | 1 to 65535       |
|                               | Ensure beforehand that the port you specify is set as the listen port number on the LDAP directory server.                                                                                                    | 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.                                                              | DN(BaseDN)       |
|                               | The user entries located below this DN in the hierarchy are checked during authentication.                                                                                                                     | Default value: none |
|                               | If you must escape any of the characters in the BaseDN, ensure that you escape the characters correctly because the specified                                                                               |                 |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>value is passed to the LDAP directory server without change.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Hierarchical structure model</td>
<td>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 an HCSM user ID.</td>
<td></td>
</tr>
<tr>
<td>• Flat model</td>
<td>Specify the DN of the hierarchy just the user entries required for searching.</td>
<td></td>
</tr>
<tr>
<td>When specifying the DN, follow the rules defined in RFC4514. For example, you must use a backslash () to escape each of the following characters:</td>
<td>spaces # + ; , &lt; = &gt; \</td>
<td></td>
</tr>
<tr>
<td>auth.group.realname.timeout</td>
<td>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.</td>
<td>0 to 120 (seconds)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default value: 15</td>
</tr>
<tr>
<td>auth.group.realname.retry.interval</td>
<td>Specifies the retry interval when an LDAP directory server connection attempt fails.</td>
<td>1 to 60 (seconds)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default value: 1</td>
</tr>
<tr>
<td>auth.group.realname.retry.times</td>
<td>Specifies the number of retries to attempt when an LDAP directory server connection fails. If you specify 0, no retries are attempted.</td>
<td>0 to 50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default value: 20</td>
</tr>
</tbody>
</table>

**Example properties file for Kerberos server connections (exauth.properties)**

When using HCSM, 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 HCSM 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):

```properties
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 authentication 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 authentication 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

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:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log.Facility</td>
<td>Unused - Ignored even if specified.</td>
</tr>
<tr>
<td>Log.Event.Category</td>
<td>Specifies the audit event categories that you want generated.</td>
</tr>
<tr>
<td></td>
<td>To specify multiple categories, separate them using commas, but do not</td>
</tr>
<tr>
<td></td>
<td>insert spaces between categories and commas.</td>
</tr>
<tr>
<td></td>
<td>This parameter value is required for audit logging to function.</td>
</tr>
<tr>
<td></td>
<td>Valid values: StartStop, Authentication, ConfigurationAccess,</td>
</tr>
<tr>
<td></td>
<td>ExternalService</td>
</tr>
<tr>
<td></td>
<td>If an invalid category name is specified, the specified file name is</td>
</tr>
<tr>
<td></td>
<td>ignored.</td>
</tr>
<tr>
<td></td>
<td>Default value: none</td>
</tr>
<tr>
<td>Log.Level</td>
<td>Specifies the severity level of audit events that you want generated.</td>
</tr>
<tr>
<td></td>
<td>Events with the specified severity level or lower are output to the event</td>
</tr>
<tr>
<td></td>
<td>log file.</td>
</tr>
<tr>
<td></td>
<td>If an invalid value or a non-numeric character is specified, the default</td>
</tr>
<tr>
<td></td>
<td>value is used.</td>
</tr>
<tr>
<td></td>
<td>Value range: 0 to 7 - severity level</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Default value: 6</td>
</tr>
</tbody>
</table>

The following table shows the correspondence between the audit event severity levels and event log data types.

<table>
<thead>
<tr>
<th>Audit event severity</th>
<th>Type of event log data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Error</td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Warning</td>
</tr>
<tr>
<td>5</td>
<td>Information</td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

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.

```plaintext
# 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 233
Related references
• Properties files for Hitachi Command Suite Common Component on page 260

Properties related to clustering (cluster.conf)

The Common Component cluster.conf file contains parameters related to clustering as listed in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mode</td>
<td>Specifies the node type as follows:</td>
</tr>
<tr>
<td></td>
<td>• For the active node, specify &quot;online&quot;.</td>
</tr>
<tr>
<td></td>
<td>• For the standby node, specify &quot;standby&quot;.</td>
</tr>
<tr>
<td>virtualhost</td>
<td>Specifies a logical host name.</td>
</tr>
<tr>
<td></td>
<td>• You must specify a host name. You cannot specify an IP address.</td>
</tr>
<tr>
<td></td>
<td>• You must also ensure that the logical host name is associated with an</td>
</tr>
<tr>
<td></td>
<td>access-enabled IP address.</td>
</tr>
<tr>
<td>onlinehost</td>
<td>Specifies the host name of the active node.</td>
</tr>
<tr>
<td></td>
<td>• You must specify a host name. You cannot specify an IP address.</td>
</tr>
<tr>
<td>standbyhost</td>
<td>Specifies the host name of the standby node.</td>
</tr>
<tr>
<td></td>
<td>• You must specify a host name. You cannot specify an IP address.</td>
</tr>
</tbody>
</table>

Related references
• Properties files for Hitachi Command Suite Common Component on page 260

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:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BackupRestoreUnicast</td>
<td>This port is used for managed resource disk backup and restoration.</td>
</tr>
<tr>
<td></td>
<td>• The default value is 26501.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>If an attempt to change this port number fails, the system uses the default value 56020/tcp.</td>
</tr>
<tr>
<td>BOOTNIC</td>
<td>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.</td>
</tr>
<tr>
<td>FSC</td>
<td>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.</td>
</tr>
<tr>
<td>FTUnicast</td>
<td>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.</td>
</tr>
</tbody>
</table>
Upgrading the HCSM software from v7.x

The module explains how to upgrade HCSM on the management server.

- About upgrading the HCSM software
- Prerequisites for upgrading the HCSM software
- Upgrading the HCSM software in a non-cluster environment
- Upgrading from HCSM in a cluster environment
About upgrading the HCSM software

To upgrade Hitachi Compute Systems Manager (HCSM) from v7.x on the management server, you must install HCSM v8.0 or later and complete some additional tasks, which depend on whether you are upgrading in a cluster environment.

Related tasks

- Upgrading the HCSM software in a non-cluster environment on page 291
- Upgrading the HCSM software on an active node on page 293
- Upgrading the HCSM software on a standby node on page 298

Related references

- Prerequisites for upgrading the HCSM software on page 290

Prerequisites for upgrading the HCSM software

Before beginning an upgrade from v7.x, ensure that you are aware of the following:

- HCSM v7.x is removed during the upgrade. This includes removing all files and directories that were created during the HCSM 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 HCSM software.
- Do not install any Hitachi Command Suite products v7.x or earlier on an HCSM management server that you upgraded to v8.0 or later.
- After you upgrade HCSM, 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.

- HCSM v8.0 or later management servers use the following command names and the following default installation locations:
  - Command names:
    hcmdsxxxx changes to hcmds64xxxx
  - Default HCSM 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 of 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 HCSM.

Related concepts
- About upgrading the HCSM software on page 290

Related tasks
- Upgrading the HCSM software in a non-cluster environment on page 291
- Upgrading the HCSM software on an active node on page 293
- Upgrading the HCSM software on a standby node on page 298

Upgrading the HCSM software in a non-cluster environment

You can upgrade an HCSM 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 HCS 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 HCSM v7.x during an upgrade to v8.x or later:
o Databases
o Authentication information about Hitachi Command Suite product databases including HCSM
o MIB files, including SNMP trap definitions
  The MIB files are moved to the installation directory after the upgrade.
o Properties files on the HCSM 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 HCSM 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 HCSM 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 HCSM.
7. Verify that you can access HCSM using a web browser.

**Note:**
- If HCSM 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 HCSM 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 HCSM in the web browser address bar.

Result
You can now start using the new version of HCSM.

Related concepts
- About upgrading the HCSM software on page 290
- About installing Hitachi Compute Systems Manager on page 47

Related tasks
- Verifying access to the management server on page 53
- Installing Deployment Manager on page 161
- Starting Hitachi Compute Systems Manager on page 166
- Stopping Hitachi Compute Systems Manager on page 167

Related references
- Prerequisites for upgrading the HCSM software on page 290

Upgrading from HCSM in a cluster environment
The section explains how to upgrade HCSM on the management server in a cluster environment.

Upgrading the HCSM software on an active node
You can upgrade HCSM v7.x on a management server of an active node in a cluster environment.

Before beginning an upgrade installation, you must temporarily stop cluster operation.

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 HCS 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 HCSM v7.x during an upgrade to v8.x or later:
  ○ Databases
  ○ Authentication information about Hitachi Command Suite product databases including HCSM
  ○ MIB files, including SNMP trap definitions
    The MIB files are moved to the installation directory after the upgrade.
  ○ Properties files on the HCSM 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.
• If in use, Deployment Manager is removed.

Removing Deployment Manager requires using the v7.x installation media. When you run the HCSM installation wizard, select Deployment Manager to remove it.

**Procedure**

1. Using the cluster management software, bring online the group in which the HCSM services are registered.
2. Take the following services offline:
   • HBase Storage Mgmt Common Service
   • HBase Storage Mgmt Web Service
   • HCS Compute Systems Manager Web Service
   • Any Hitachi Command Suite product resources not previously listed
   • If any HCS product v7.x and v8.x or later products coexist temporarily, take the product services for each version offline.

---

**Note:** You take the HiRDB/ClusterService _HD0 and HiRDB/ClusterService _HD1 (if already registered), offline in step 4.
If you are using Deployment Manager, also take the following services offline:

- DeploymentManager PXE Management
- DeploymentManager PXE Mtftp
- DeploymentManager Transfer Management

3. Run the following command to stop the Hitachi Command Suite product services:

```bash
HCS-Common-Component-installation-folder(v7.x)\bin\hcmdssrv /stop
```

4. In the cluster management software, take the following services offline:

- HiRDB/ClusterService _HD0
- HiRDB/ClusterService _HD1 (if already registered)

5. Change the settings of the following resources by right-clicking the resource name, choosing **Properties**, accessing the **Policies** tab, and selecting **If resource fails, do not restart**.

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HCS Compute Systems Manager Web Service
- HiRDB/ClusterService _HD0
- HiRDB/ClusterService _HD1 (if already registered)
- Any other services you took offline in step 2.

If you are using Deployment Manager, also change the resource settings of the following services:

- DeploymentManager PXE Management
- DeploymentManager PXE Mtftp
- DeploymentManager Transfer Management

6. Make sure that the shared disk is accessible.

7. If you are using Deployment Manager, remove it.

   To remove the software, use the v7.x installation media and within the HCSM installation wizard, select Deployment Manager and remove it.

8. Upgrade the HCSM software.

   The database used before the upgrade is automatically backed up during the installation.

9. Change the HCSM URL to access the logical host name.

   Verify whether the URL points to the logical host name by using the following command:

   ```bash
   HCS-Common-Component-installation-folder(v8x or later)\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.
10. If you already configured a cluster environment by using products that use the 64-bit HCS Common Component, skip to the next step. If HCSM is the first HCS product in the cluster, do the following:

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**.

b. Save the file as *cluster.conf* in *HCS-Common-Component-installation-folder(v8 x or later)\conf*.

b. Back up the HCSM database by using the following command:

```
HCS-Common-Component-installation-folder(v8 x or later)\bin
\hcmds64backups /dir local-disk-folder-for-data-storage-backup /auto
```

**Note:** We recommend that you back up the database in case an error occurs.

c. If you changed the database port from the default (22032/tcp), take note of the port number that you are using.

d. Migrate the database to the shared disk by using the following command:

```
HCS-Common-Component-installation-folder(v8 x or later)\bin
\hcmds64dbclustersetup /createcluster /databasepath folder-on-shared-disk-for-database-recreation /exportpath local-disk-folder-for-data-storage-backup /auto
```

**Caution:** When you run the *hcmds64dbclustersetup* command, the database port number and 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.

11. If any Hitachi Command Suite products are running, use the Windows menu to stop HCSM.
Using the Windows menu to stop HCSM causes all other Hitachi Command Suite products to stop at the same time.

12. In the Windows Services dialog box, open the properties for each of the following services. If the Startup Type is Automatic, change it to Manual.
   - 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

13. Verify that the hcsm.shared.directory property in the following file specifies the work path directory for HCSM:

   HCSM-installation-folder\ComputeSystemsManager\conf\user.properties

   If it has not been specified, create a directory on the shared disk, and then specify the path of that directory.

14. If you are already using Deployment Manager, run the following batch file and specify settings so that the Deployment Manager services start correctly:

   HCSM-installation-folder\ComputeSystemsManager\DeploymentManager\hcsm_setting\set_cluster.bat

15. 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.

16. Use the cluster management software to move the group in which the HCSM services are registered to the standby node.

   Right-click the group in which the services are registered, and choose Move and then select either Select Node or Move this service or application to another node.
Upgrading the HCSM software on a standby node

You can upgrade HCSM v7.x on a management server of an standby node in a cluster environment.

Before beginning the upgrade on the standby node, restart the cluster environment that you stopped temporarily on the active node during the upgrade installation.

**Procedure**

1. Run the following command to stop the Hitachi Command Suite services on the standby node:
   
   ```bash
   HCS-Common-Component-installation-folder(v7.x)\bin\hcmdssrv / stop
   ```

2. If you are using Deployment Manager, remove it.
   
   To remove the software, use the v7.x installation media and within the HCSM installation wizard, select Deployment Manager and remove it.

3. Upgrade the HCSM software.
   
   If you installed Deployment Manager during the upgrade installation on the active node, be sure to install Deployment Manager on the standby node.
4. If you already configured a cluster environment by using products that use the 64-bit HCS Common Component, skip to the next step. If HCSM is the first HCS 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
   ```

   **Note:** On a standby node, you must specify `standby` for `mode`.

   Save the file as `cluster.conf` in `HCS-Common-Component-installation-folder\v8x or later\conf`.

   b. Back up the HCSM database by using the following command:

   ```
   HCS-Common-Component-installation-folder\bin\hcmds64backups /dir local-disk-folder-for-data-storage-backup /auto
   ```

   **Note:** We recommend that you back up the database in case an error occurs.

   c. If you changed the database port from the default (22032/tcp), take note of the port number that you are using.

   d. Migrate the database to the shared disk by using the following command:

   ```
   HCS-Common-Component-installation-folder\bin\hcmds64dbclustersetup /createcluster /databasepath folder-on-shared-disk-for-database-recreation /exportpath local-disk-folder-for-data-storage-backup /auto
   ```

   **Caution:** When you run the `hcmds64dbclustersetup` command, the database port number and 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.

5. If any Hitachi Command Suite products are running, use the Windows menu to stop HCSM.

   Using the Windows menu to stop HCSM causes all other Hitachi Command Suite products to stop at the same time.
6. In the Windows Services dialog box, open the properties for each of the following services. If the Startup Type is Automatic, change it to Manual.
- 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

7. In the cluster management software, re-register the services.
Delete the following services that were registered before the upgrade:
- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HCS Compute Systems Manager Web Service
- HiRDB/ClusterService _HD0

After deleting these services, register 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/ClusterService _HD1

8. In the cluster management software, enable failover for the group in which the services are registered.
Change the settings of the resources listed in this step by right-clicking the resource name, choosing Properties, and selecting the following check boxes on the Policies tab:
- If resource fails, attempt restart on current node
- If restart is unsuccessful, fail over all resources in this Role or If restart is unsuccessful, fail over all resources in this service or application.

Change the settings of the following resources:
- 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
- Any additional Hitachi Command Suite product resources (v8x or later) not previously listed

If you are using Deployment Manager, also change the resource settings of the following services:
- DeploymentManager PXE Management
- DeploymentManager PXE Mtftp
- DeploymentManager Transfer Management
9. Change the settings of the resources listed in this step by right-clicking the resource name, choosing Properties and selecting the following check boxes on the Policies tab:
   - **If resource fails, attempt restart on current node**
   - **If restart is unsuccessful, fail over all resources in this Role** or
     - **If restart is unsuccessful, fail over all resources in this service or application.**

Change the settings of the following resources:
- 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
- Any additional Hitachi Command Suite product resources not previously listed

If you are using Deployment Manager, also change the resource settings of the following services:
- DeploymentManager PXE Management
- DeploymentManager PXE Mtftp
- DeploymentManager Transfer Management

10. Verify that the work directory path specified for the hcsm.shared.directory property in the following file matches the work path directory specified for HCSM on the active node:

    HCSM-installation-folder\ComputeSystemsManager\conf\user.properties

    If the property path does not match, change it so that it matches the path specified on the active node.

11. If you are already using Deployment Manager, run the following batch file and specify settings so that the Deployment Manager services start correctly:

    HCSM-installation-folder\ComputeSystemsManager\DeploymentManager\hcsm_setting\set_cluster.bat

12. 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-folder\ComputeSystemsManager\conf\user.properties

13. Use the cluster management software to bring online the group in which the HCSM services are registered.

14. Use the cluster management software to migrate the HCSM services group to the active node.
15. If you completed a new installation of Deployment Manager during the HCSM upgrade installation, configure the cluster environment so that you can use Deployment Manager.

Related tasks
- Installing Deployment Manager on page 161
- Setting up a cluster within Windows Server Failover Clustering on page 202
- Upgrading the HCSM software on an active node on page 293
- Stopping Hitachi Compute Systems Manager on page 167
- Setting up Deployment Manager in a cluster environment using Windows Server Failover Clustering on page 204
- Bringing HCSM services online from cluster management software on page 207

Related references
- Command format for migrating to a cluster environment on page 214
- Synchronizing settings in a cluster environment on page 201
- Properties related to Hitachi Compute Systems Manager server ports and functions (user.properties) on page 257
- Prerequisites for upgrading the HCSM software on page 290
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.
GUI

graphical user interface

HBA

See host bus adapter.

host bus adapter

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 HCSM 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 HCSM.

**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**

storage area network. A network of shared storage devices that contain disks for storing data.

**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.

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.
User Access Control (UAC)

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.

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.

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.
Symbols
.NET Framework, installing for Deployment Manager 160

A
account on the Linux host, host prerequisite 97, 99
account on the Solaris host, host prerequisite 97, 99
administrator account, creating 58
alert level, for e-mail notifications 56
assigning
  resource group to user group 59
  role to user group 59
audit events 235, 246
audit logs
  audit events for processing and launching requests 246
  auditlog.conf properties file 285
categories and audit events 235
detailed messages for HCSM requests 247
detailed messages for HCSM requests
  log message format and information 244
  overview 233
  setting up 233
  viewing 234
auditlog.conf file 285
authentication
  Base DN 131
  external server overview 128
  Kerberos server workflow 31
  LDAP server 129, 130
  LDAP server data structure models 129
  LDAP server workflow 30
attributes
  installation prerequisites 181
  cluster environment
    verifying free disk space in management server 185
  cluster environment configuration, checking 186
  cluster.conf properties file 287
  collecting maintenance information
    managed host 231
  commands
    changing the timeout period 82
  components, HCSM 19
  configuring
    audit logs 233
    basic system 20
    Deployment Manager 158
e-mail notifications 56
  JDK version 80
  LAN 21
  management server URL 78
  optional user account settings 69
  ports 74
  server host name 75
  server IP address 75
  SNMP 66
  connecting to an Kerberos server 138
  connecting to an LDAP directory server 133
  connection settings
    for an Kerberos server 144
backing up the database
  prerequisites 172

backing up the database procedure 172, 210–213
backup workflow 34
Base DN for LDAP directory servers 131
blade server chassis
  secure communication setup workflow 29
boot settings, changing 162
for an Kerberos server using DNS and an
authorization server 147
for an Kerberos server with an authorization
server 146
for an LDAP directory server 140
for an LDAP directory server using DNS and an
authorization server 143
for an LDAP directory server with an
authorization server 142
for using DNS to find an Kerberos server 145
for using DNS to find an LDAP directory server 141
creating 59
resource groups 59
creating user groups 59

D

data structure, LDAP directory server 132
database corruption in a cluster, troubleshooting 224
database corruption, troubleshooting 223
database directory, creating a new directory 45
database management
backup 172, 210–213
backup prerequisites 172
database backup workflow 34
exporting the database 175
importing the database 176
migration prerequisites 175
overview 171
restore prerequisites 173
restoring 174
database migration, prerequisites 175
DCOM, Windows host prerequisite 92
def_pdsys properties file 270
def_pdutsys properties file 271
deleting
LDAP search user 153
Deployment manager
port properties file 163, 287
Deployment Manager
configuration workflow 32
environment settings 158
installation prerequisites 161
installing 161
port, changing 162
prerequisites 158
removing from a cluster environment 215
Windows Server Failover Clustering 204
DNS, for locating an LDAP directory server 132

E

e-mail address, setting for the system account 55
e-mail notifications
setting the alert level 56
setting up 56

F

enabling
WinRM for Windows hosts 92
enabling inband events on a Windows target 94
encryption type, Kerberos directory server 137
environment settings
Deployment Manager 158
exauth.properties
file description 272, 279
file example 276, 283
exporting, database 175
external authentication server
Base DN 131
configuring a connection to an Kerberos server 138
configuring a connection to an LDAP server 133
configuring SSL for a secure connection 135
direct connection settings 140, 144
direct connection settings with an
authorization server 142, 146
DNS connection settings 141, 145
DNS connection settings with an authorization
server 143, 147
exauth.properties file 272, 279
exauth.properties file example 276, 283
identifying Kerberos encryption type 137
identifying LDAP server data structure and
authentication method 132
importing the LDAP directory server certificate 154
Kerberos authentication workflow 31
LDAP authentication method 129, 130
LDAP authentication workflow 30
LDAP data structure 129, 130
overview 128
prerequisites for a secure connection 153
prerequisites for registering an LDAP search
user 150
secure communication setup workflow 29
setting up a connection 272, 279
using DNS 132
verifying an Kerberos server connection 139
verifying an LDAP directory server connection 136

fcinfo tool, Windows host prerequisite 94
fibre channel SAN resource information, fcinfo
tool 94
firewall configuration, Windows host prerequisite 90, 91
firewall exceptions, ports 84

H

HCS Common Component
properties files list 260
properties files overview 260
Index

Hitachi Compute Systems Manager Installation and Configuration Guide
K

Kerberos
  connecting 137
  exauth.properties file 283
Kerberos directory server
  identifying encryption type 137
Kerberos directory server and authorization server settings 146
Kerberos server
  authentication workflow 31
  configuring a connection 138
  direct connection settings 144
  direct connection settings with an authorization server 146
  DNS connection settings 145
  DNS connection settings with an authorization server 147
  setup workflow 31
  verifying a connection 139
Kerberos server (DNS) and authorization server settings 147
  kernel parameters, configuring 41

L

LAN configuration 21
LDAP
  deleting search user 153
LDAP directory server
  authentication method 129–131
  authentication workflow 30, 35
  configuring a connection 133
  configuring SSL for a secure connection 135
  data structure 129, 130
  data structure Base DN 131
  direct connection settings 140
  direct connection settings with an authorization server 142
  DNS connection settings 141
  DNS connection settings with an authorization server 143
  DNS prerequisites 132
  identifying directory server data structure and authentication method 132
  prerequisites for a secure connection 153
  prerequisites for registering and LDAP search user 150
  secure communication setup workflow 29
  setup workflow 30
  verifying a connection 136
LDAP directory server (DNS) and authorization server settings 143
LDAP directory server and authorization server settings 142
license, registering 54
Linux
  files and directories 96
  host 96
  host account 97
installing HCSM 51
  overview of account on the Linux host 99
  permissions 101
  registering firewall exceptions in 42
  registering management server firewall exceptions 85
  root access 99
  setting up an IP connection 98
log files
  changing settings 249
  logger.properties file 259
  settings 248
log message format and information 244
logger.properties file 259
login window, troubleshooting 222
LOM, power management on hosts 88

M

maintenance information
  Java VM threads on Linux 229
  Java VM threads on Windows 228
Linux managed host 232
  managed host 231
  management server 226
  overview 225
  Solaris managed host 232
managed resource
  changing boot settings 162
managed resource prerequisites
  enable WoL 88
Linux files and directories 96
Linux, setting up permission for normal users (su command) 100
Linux, setting up root access 99
Linux, verifying the files and directories 96
Linux::setting up an IP connection 98
Linux::setting up permission for normal users (sudo command) 101
  setting up an account on the Linux host 97
  setting up an account on the Solaris host 97
  snmp for inband events 94
SNMP for inband events 104, 106
Solaris files and directories 96
Solaris, setting up permission for normal users (pfexec command) 103
Solaris, setting up permission for normal users (su command) 100
Solaris, setting up root access 99
Solaris, verifying the files and directories 96
Windows Server 2003::configuring the firewall 90
Windows Server 2003::installing the fcinfo tool 94
Windows Server 2008::configuring the firewall 91
Windows Server 2008::setting up a remote connection for UAC 93
  Windows: enabling DCOM 92
managed resources
adding a host 57
blade server prerequisites 89
Linux host prerequisites 96
maintenance information for Linux hosts 232
maintenance information for managed hosts 231
maintenance information for Solaris hosts 232
overview 18
rack-mounted server prerequisites 89
setup workflow 25
Solaris host prerequisites 96
updating information after replacing or modifying a host 107
Windows host prerequisites 89
management client
restricting access to the management server 125
secure communication setup workflow 27
setting up SSL on clients running the CLI 118
setting up SSL on web-based clients 117
setting up the server for secure client communication 111
management server
changing log file settings 249
changing the timeout period for commands 82, 83
importing the LDAP directory server certificate 154
information required for installation 47
maintenance information 226
migration workflow 33
properties files 260
properties files list 256
resetting the time setting 81
resetting the time setting manually 82
restricting management client access 125
setting up SSL for SMTP server secure communications 120
troubleshooting 223
verifying access 53
media for installing 47
MIB files, registering 66
migration workflow 33

O
overview
basic system configuration 20
HCSM 18
installation workflow 23
LAN configuration 21
managed resources 18
related products 21
workflows 21

P
password, changing for system account 55
path names, rules for specifying 44
pd sys properties file 269
pdutsys properties file 271
pfexec command for normal users, Solaris host prerequisite 103
planning
avoiding port conflicts 40
creating a new database directory 45
installation 40
installation information 43
management server information 47
path name rules 44
server time setting 42
system prerequisites 40
port
Deployment Manager property 163, 287
ports
avoiding conflicts 40
changing ports 74
Deployment Manager 253
HCS Common Component 252
HCSM server 252
overview of Deployment Manager 253
overview of HCS Common Component ports 252
overview of HCSM server ports 252
properties requiring updated when ports change 71, 73
user.properties file 257
workers.properties file 268
post-installation
adding a host 57
changing the system account password 55
completing the initial setup 60
creating a server administrator account 58
overview 53
registering a license 54
setting an e-mail address for the system account 55
setting up alert level for e-mail notifications 56
setting up e-mail notifications 56
verifying access to the management server 53
workflow 23
prerequisites
blade servers 89
Deployment Manager 158
implementing HCSM in a cluster environment 181
installation information 43
Linux installation 41
Linux managed hosts 96
rack-mounted servers 89
removing the software 61, 201
Solaris managed hosts 96
system 40
upgrade installation 290
Windows managed hosts 89
properties
auditlog.conf properties file 285
cluster.conf properties file 287
def_pdsys properties file 270
def_pdutsys properties file 271
exauth.properties file 272, 279
exauth.properties file example 276, 283
HCS Common Component 260
HCS Common component properties files list 260
HCSM properties files list 256
HCSM server properties file overview 256
HiRDB.ini properties file 269
logger.properties file 259
pdsys properties file 269
pdutsys properties file 271
user_hssol httpsd.conf file 268
userHttps.conf file 263
user.conf properties file 271
user.properties file 257
usrconf.properties file 267
workers.properties file 268

R
registering firewall exceptions, Linux 42
removing the software
  prerequisites 61, 201
  removal procedure 217
removing the software, Linux
  removal procedure 63
removing the software, Windows
  removal procedure 62
reseting the server time setting 81
reseting the server time setting manually 82
resource group
  assigning to user group 59
  creating 59
restarting HCSM in a cluster environment 209
restoring, database 173, 174
restricting communication to SSL 115
root access, Linux host prerequisite 99
root access, Solaris host prerequisite 99

S
search user, LDAP directory server 150
secure communications 110
  workflow for SMTP server setup 28
  workflow for increasing blade server chassis communication 29
  workflow for management clients 27
security settings
  configuring SSL for a secure LDAP server connection 135
  increasing security for chassis alert communication 121
  overview 110
  prerequisites for a secure LDAP server 153
  restricting management client access to the management server 125
secure communications between the management server and the SMTP server 119
secure communications for management clients 110
setting up:server for secure client communication 111
setting up:SSL for secure client communication 120
setting up:SSL for SMTP server secure communication 120
setting up:SSL on management clients running the CLI 118
setting up:SSL on web-based management clients 117
user_httpsd.conf file 263
user.conf properties file 271
server administrator, creating an account 58
server time setting requirements 81
service names, HCSM 168
Setting up
  blade server target 89
settings
  for virus scanning programs 52
Simple Network Management Protocol 66
SMTP server
  secure communication setup workflow 28
  secure communications 119
SNMP 94
  enabling inband events on a Linux target 104
  enabling inband events on a Solaris target 106
  registering MIB files 66
  traps 66
  workflow for configuring traps 25
software, removing with all-in-one uninstaller 63
Solaris
  files and directories 96
  host 96
  host account 97
  overview of account on the Solaris host 99
  permissions 100, 103
  root access 99
SSL
  setting up an additional certificate for chassis communication 121
  setting up on management clients running the CLI 118
  setting up on the server for secure client communication 111
  setting up on web-based management clients 117
  setting up:additional certificate for chassis communication 121
  using for secure client communication 110
starting HCSM 166
stopping HCSM 166, 167
su command for normal users, Linux host prerequisite 100
su command for normal users, Solaris host prerequisite 100
sudo command for normal users, Linux host prerequisite 101
system account
  changing the password 55
  enabling auto account locking 69
  setting an e-mail address 55
  user.conf properties file 271
system components, overview 19

changing the password 55

enabling auto account locking 69

setting an e-mail address 55

user.conf properties file 271

timeout period for commands 82

To Do list
  completing 60
  using for initial setup 53

troubleshooting
  example of database corruption 223
  example of database in a cluster 224
  example of when login windows does not display 222
  example of when management server does not start 223
  overview 222
  workflow 36

upgrading
  software on active node 293
  software on standby node 298

upgrading the software 290

upgrading the software on the management server 289

URL
  changes that require updating the URL 80
  changing the management server URL 78

user account
  optional settings 69
  unlocking accounts 70
user groups 59
user_hssd_httpsd.conf properties file 268
user_httpsd.conf properties file 263
user.conf properties file 271
user.properties file 257
usrconf.properties file 267

virus scanning
  cluster environment 201
  virus scanning setting requirements settings 52

W
  Windows firewall, enabling after installing HCSM 84
  Windows hosts 89
  Windows Server 2008, setting up a remote connection with UAC 93
  WinRM settings, applying 86
  WinRM, enabling for Windows hosts 92
  WoL, enabling on a host 88
  workers.properties file 268
workflows
  blade server chassis secure communication setup 29
  client secure communication setup 27
  Deployment Manager 32
  installation 23
  Kerberos server setup 31
  LDAP directory server setup 30
  LDAP server secure communications setup 29
  managed host setup 25
  management server migration 33
  overview 21
  post-installation 23
  server database backup 34
  server network configuration network workflow 35
  SMTP server secure communication setup 28
  troubleshooting 36

upgrading
  cluster environment 293
  non-cluster environment 291
upgrading installation, prerequisites 290
upgrading the software 290
upgrading the software on the management server 289
URL
  changes that require updating the URL 80
  changing the management server URL 78
user account
  optional settings 69
  unlocking accounts 70
user groups 59
user_hssd_httpsd.conf properties file 268
user_httpsd.conf properties file 263
user.conf properties file 271
user.properties file 257
usrconf.properties file 267

viewing, audit logs 234