HITACHI
Inspire the Next

Hitachi Command Suite

Compute Systems Manager

User Guide

Hitachi Data Systems

MK-91HC194-14

Contents

Preface

This manual describes how to use Hitachi Compute Systems Manager (HCSM) to manage resources.

Intended audience

This document provides instructions for server administrators.

Product version

This document revision applies to Hitachi Compute Systems Manager (HCSM) v8.2.1.

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.

Referenced documents

Hitachi Compute Systems Manager documents:

- *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*, MK-91HC195
- *Hitachi Command Suite Compute Systems Manager CLI Reference Guide*, MK-91HC196
- *Hitachi Command Suite Compute Systems Manager Messages*, MK-91HC197
- *Hitachi Compute Systems Manager Release Notes*, RN-91HC198

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

Document conventions

This document uses the following typographic conventions:

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

Convention	Description
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `pairdisplay -g <group>` **Note:** Italic font is also used to indicate variables.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.

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

Icon	Label	Description
	Note	Calls attention to important or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions or consequences (for example, disruptive operations).
	WARNING	Warns the user of severe conditions or consequences (for example, destructive operations).

Conventions for storage capacity values

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

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

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

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

Accessing product documentation

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

Getting help

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

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

Comments

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

Thank you!

1

Hitachi Compute Systems Manager overview

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

- ☐ About Hitachi Compute Systems Manager
- ☐ About Hitachi Compute Systems Manager components
- ☐ Hitachi Compute Systems Manager overview and basic setup workflows
- ☐ Resource management workflows
- ☐ About managed resource maintenance
- ☐ Navigating the management client user interface

About Hitachi Compute Systems Manager

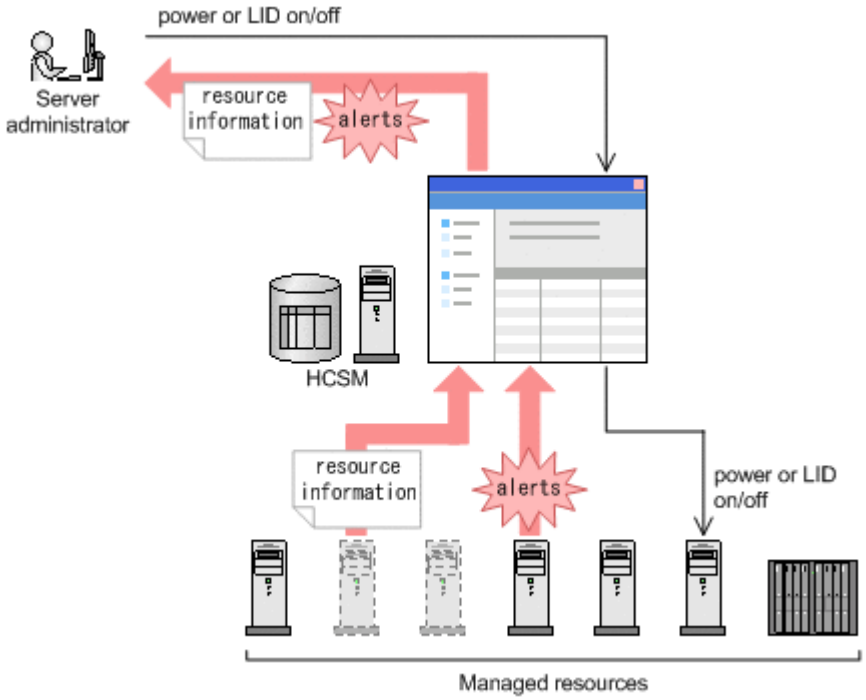
Hitachi Compute Systems Manager facilitates the management and operation of geographically remote server resources in large-scale system environments.

Compute Systems Manager enables you to manage and operate remote server resources in a large-scale system environment. Remote resources are referred to as *management targets* until you add them to the Compute Systems Manager management system. After you add a target to the system, it becomes a *managed resource*.

Server administrators use a web console or the CLI to perform tasks, such as collecting resource information, checking for errors, and controlling the power supply of managed resources, regardless of hardware model or whether the resource is physical or virtual.

Resource operations are centrally managed as tasks. Error information is provided by alerts, allowing administrative work to proceed smoothly, even when the work is shared by multiple administrators or when many tasks are being handled in parallel.

The following figure shows the management and operation of server resources by using Compute Systems Manager. Both physical (dark gray) and virtual (dashed gray) resources are shown in the environment.



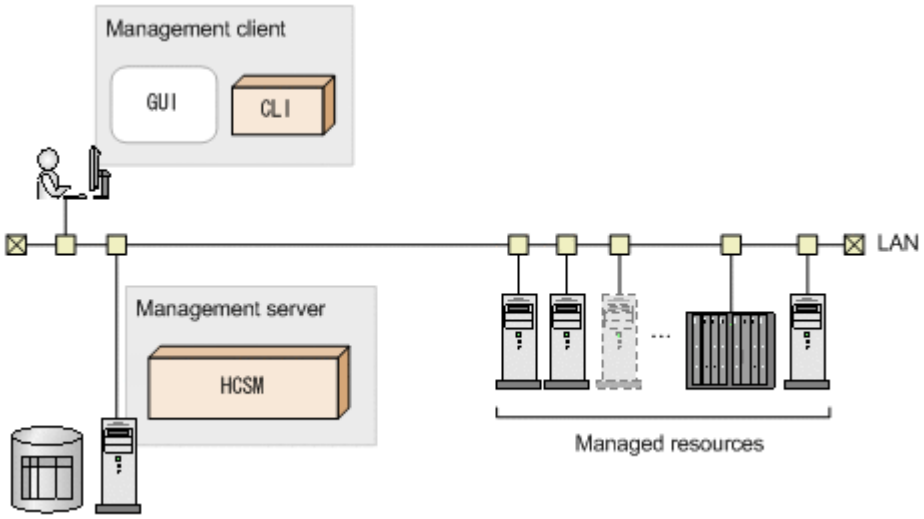
About Hitachi Compute Systems Manager components

The following components comprise the Hitachi Compute Systems Manager system:

- **Management server:** The computer on which Compute Systems Manager is installed.
- **Management client:** A computer used either to access the Compute Systems Manager Web-based GUI or the command-line interface (CLI). The GUI is accessible by using a web browser. The CLI application must be downloaded and installed on a management client.
- **Managed resources:** Resources managed by Compute Systems Manager such as hosts, Hitachi servers, virtualization resources, and so on.

For more information about these components, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

The following figure shows the components in a Compute Systems Manager system environment.



Related tasks

- Downloading the CLI on page 41

Hitachi Compute Systems Manager overview and basic setup workflows

The following modules include an overall workflow overview for Hitachi Compute Systems Manager as well as a basic setup workflow.

Hitachi Compute Systems Manager workflow overview

This manual describes how to use the management client to complete tasks that are required to use and maintain Hitachi Compute Systems Manager.

Installation and post-installation configuration of Compute Systems Manager is described in the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

The following graphic illustrates the workflow for installing, configuring, and using Compute Systems Manager.

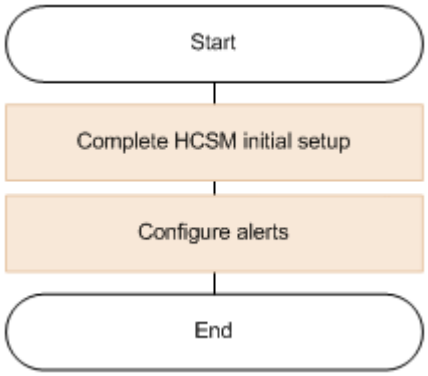
Related concepts

- Hitachi Compute Systems Manager basic setup workflow on page 19
- Management target registration workflow on page 19
- About user groups on page 208
- Resource management workflows on page 22
- Workflow for monitoring managed resources on page 25

- About managed resource maintenance on page 27
- About troubleshooting on page 218

Hitachi Compute Systems Manager basic setup workflow

The following graphic illustrates the workflow for the basic steps you must take before using Hitachi Compute Systems Manager for the first time.



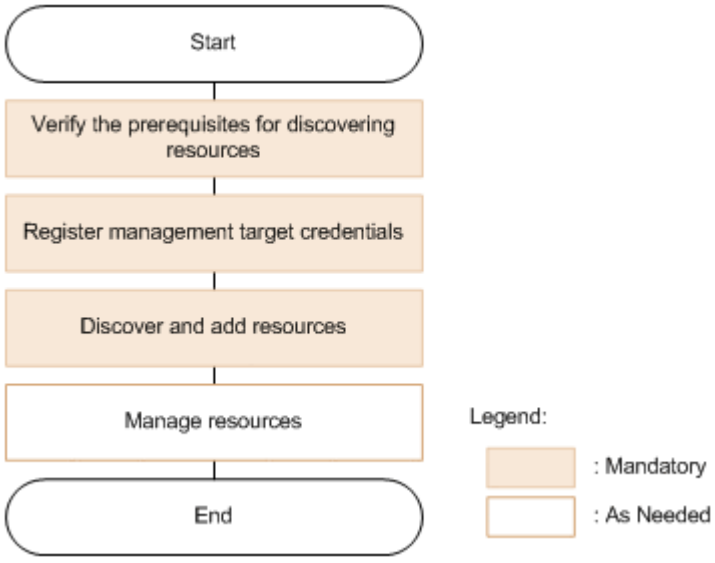
Related concepts

- About initial setup on page 34
- About alert settings on page 148

Management target registration workflow

A server administrator discovers management targets and registers them in Hitachi Compute Systems Manager as managed resources.

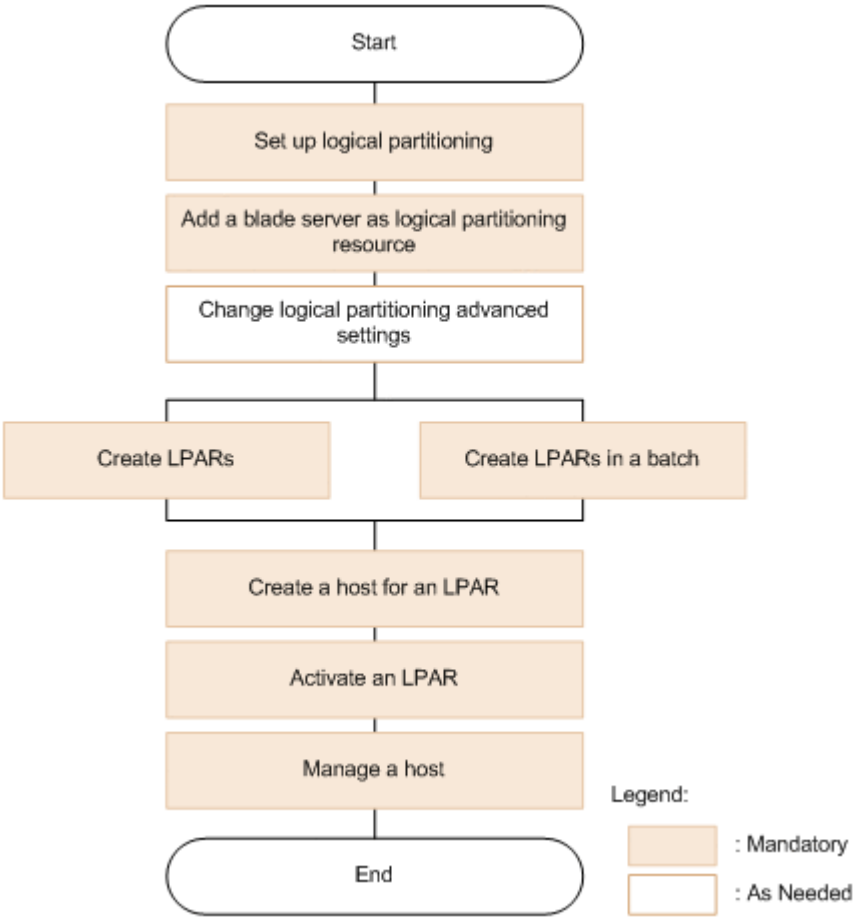
The following graphic illustrates the workflow for configuring management targets and registering them as managed resources.



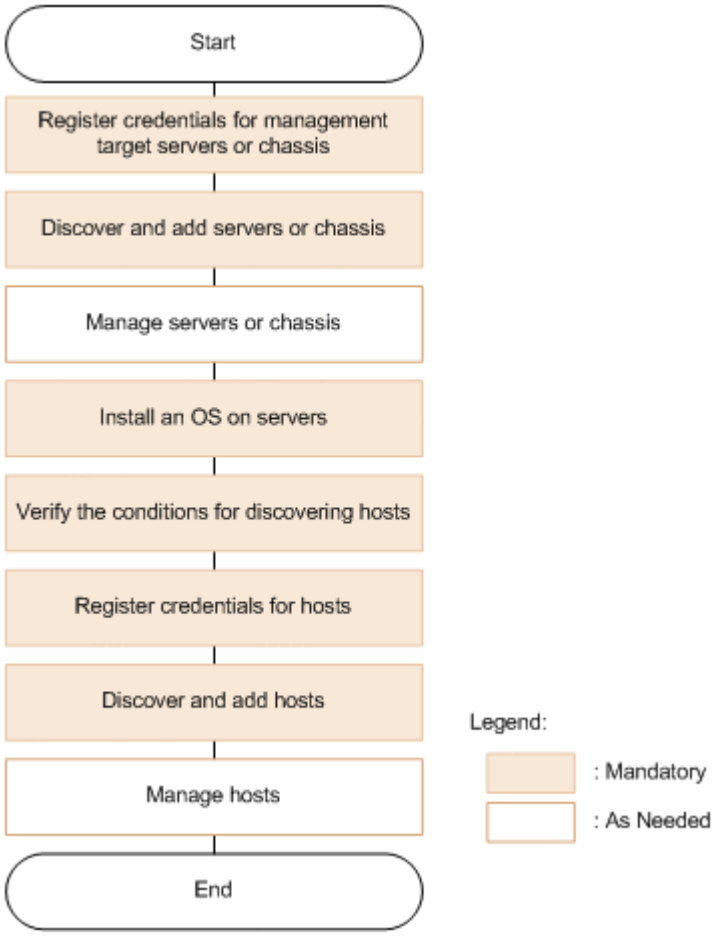
To create a new logical partitioning configuration on a managed blade server, you must complete several tasks, which include creating hosts on LPARs and

registering the hosts as managed resources. The workflow for registering the hosts created on LPARs as managed resources is the same as that described in the previous figure.

The following graphic illustrates the workflow for creating a new logical partitioning configuration.



You can register Hitachi product servers as management targets even if an operating system is not installed on the server. You can register hosts as management targets after installing an operating system on the server. The following graphic illustrates the workflow for registering management targets without an operating system.



For details on setting up the environment for management targets so Compute Systems Manager can discover the targets, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

Related concepts

- About power capping on page 117
- About viewing information summaries on page 159
- About alerts and alert resolution on page 191
- About performance and power data analyses on page 175
- Exporting information about managed resources in CSV format on page 185

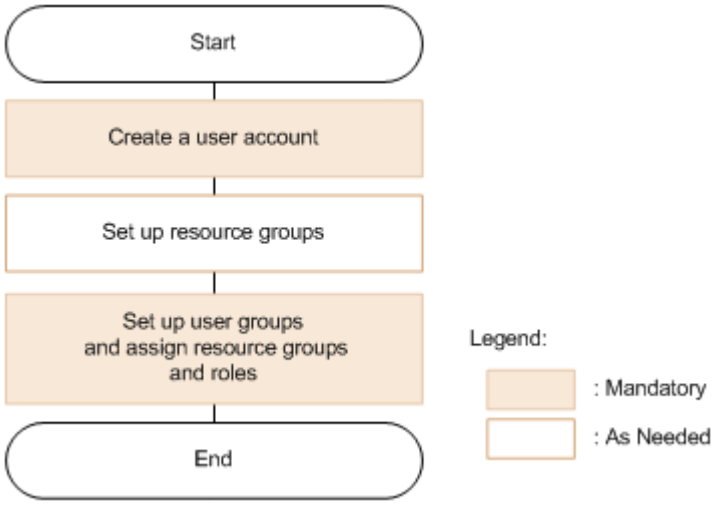
Related tasks

- Customizing performance reports displayed on the dashboard on page 162
- Resolving alerts on page 193
- Assigning an alert to a user on page 193
- Registering management target credentials on page 50

Workflow for setting up users and access controls

A server administrator creates a user account for use with Hitachi Compute Systems Manager and then sets up access controls for managed resources. By controlling access, the administrator can control which managed resources users can manage.

The following graphic illustrates the workflow for creating a user account and setting up access control for managed resources.



Related concepts

- About access control of managed resources by groups on page 198

Related tasks

- Creating resource groups on page 207
- Creating user groups on page 213
- Assigning resource groups and roles to a user group on page 214

Resource management workflows

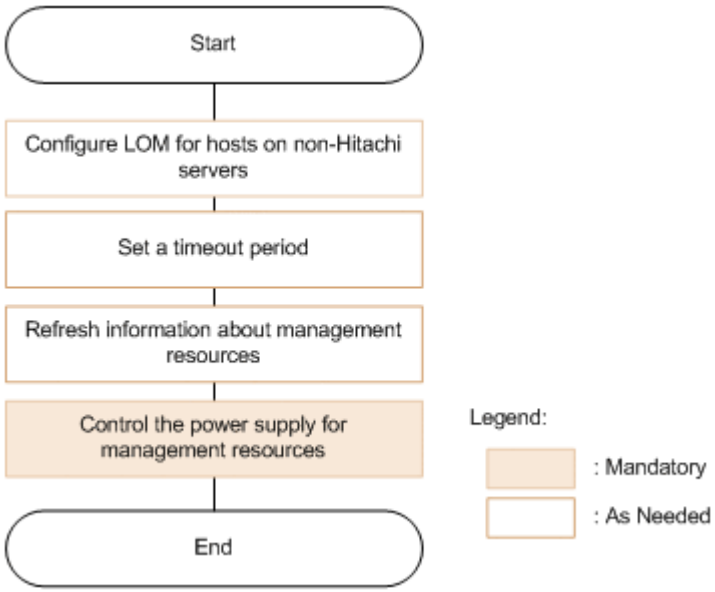
This module provides resource management workflows for configuring Hitachi Compute Systems Manager functions that enable you to:

- Manage power
- Set up automatic failover for blade servers (N+M cold standby)
- Deploy managed resources (Deployment Manager)
- Monitor the operational status of a managed resource, and analyze its performance and power monitoring data

Workflow for configuring and using power management

You can use power management to control the power supplies of managed resources.

The following graphic illustrates the workflow for managing the power supplies of managed resources.



Related tasks

- Registering LOM settings on page 78
- Setting a timeout period for power management on page 79
- Refreshing host information on page 170

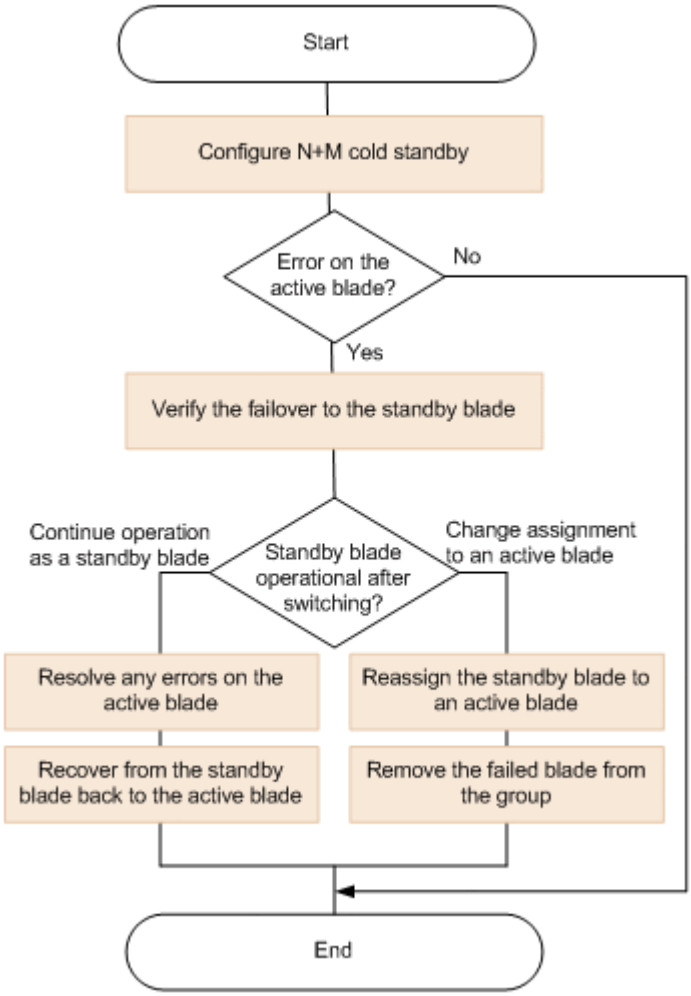
Related references

- Prerequisites for power management on page 77

Workflow for configuring and using N+M cold standby

You can use N+M cold standby to increase availability of resources and minimize any interruption in service. Before using N+M cold standby, specify the necessary settings. If an error occurs on an active blade after operation starts, confirm that the active blade failed over to the standby blade, and then take action to resolve the error.

The following graphic illustrates the workflow for configuring and using N+M cold standby.



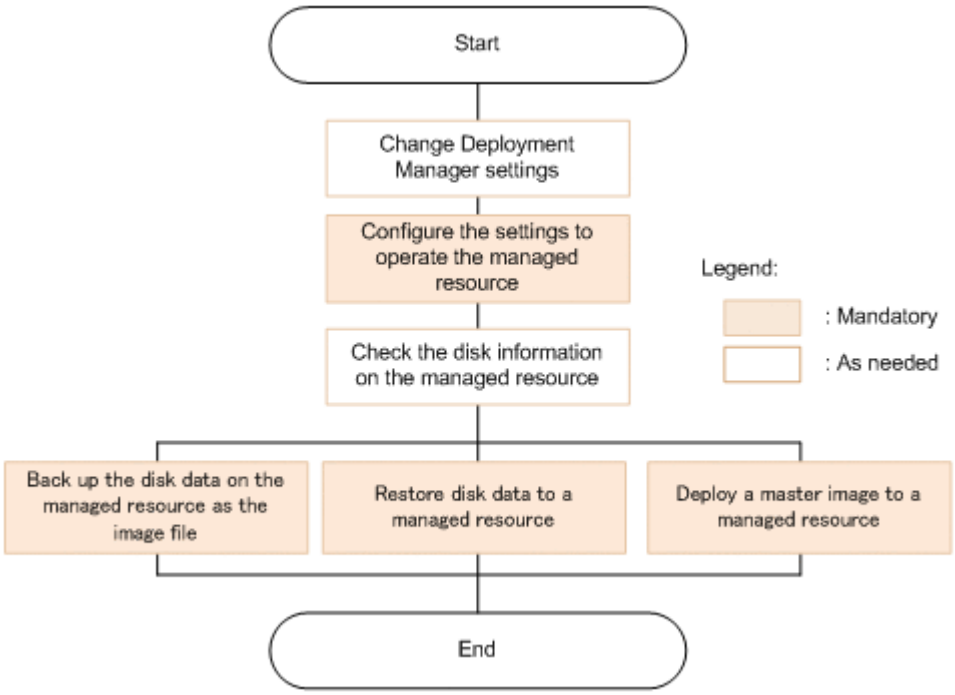
Related tasks

- Configuring N+M cold standby on page 104

Workflow for configuring and using Deployment Manager

You can use Deployment Manager to back up the disk data of a managed resource, manage image files, restore a backup image to a managed resource, and deploy a new resource by using an existing disk image (snapshot).

The following graphic illustrates the workflow for configuring and using Deployment Manager:



Related tasks

- Configuring Deployment Manager on page 132

Related references

- Prerequisites for using Deployment Manager on page 131

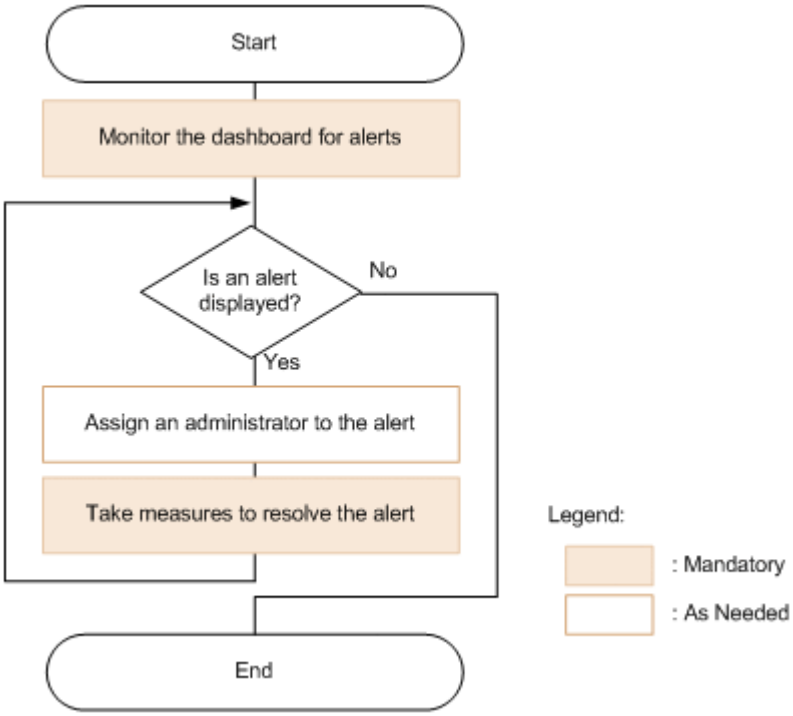
Workflow for monitoring managed resources

You can use Hitachi Compute Systems Manager to monitor the status of managed resources, and to analyze data on performance and power monitoring.

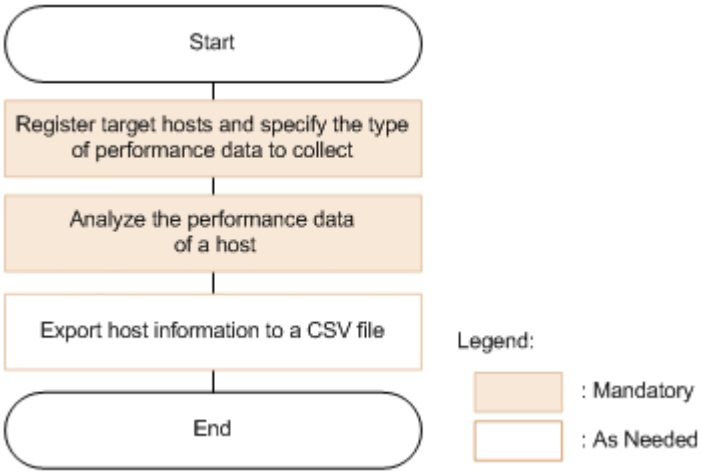
If an alert occurs while a managed resource is being monitored, you can resolve the alert or assign the task to a specific user.

The disk usage rate in performance data can be used to plan capacity re-allocation. As a result of the analysis of power monitoring data, if the power consumed by a managed resource exceeds the allowable range, you can enable power capping.

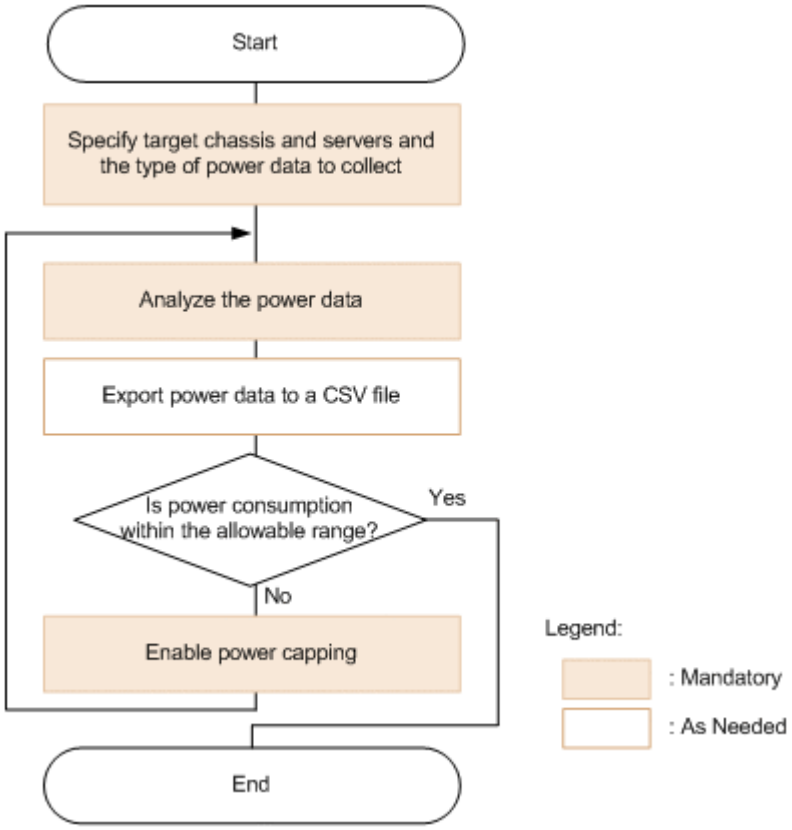
The following graphic illustrates the workflow for monitoring the status of managed resources.



The following graphic illustrates the workflow for analyzing performance data from managed hosts.



The following graphic illustrates the workflow for analyzing power monitoring data for managed servers and chassis.



Related concepts

- About power capping on page 117
- About viewing information summaries on page 159
- About alerts and alert resolution on page 191
- About performance and power data analyses on page 175
- Exporting information about managed resources in CSV format on page 185

Related tasks

- Monitoring the status of managed resources from the dashboard on page 161
- Resolving alerts on page 193
- Assigning an alert to a user on page 193

About managed resource maintenance

Using Hitachi Compute Systems Manager, you can complete the following maintenance tasks for managed resources:

- Use location identifier lamps (LID)s to locate a chassis in your network.
- Migrate LPARs to increase the availability of blade servers.
- Update firmware to ensure your chassis and blades run the latest updates.

Related concepts

- About location identifier lamps on page 100
- About migrating LPARs on page 112
- About updating firmware on page 143

Navigating the management client user interface

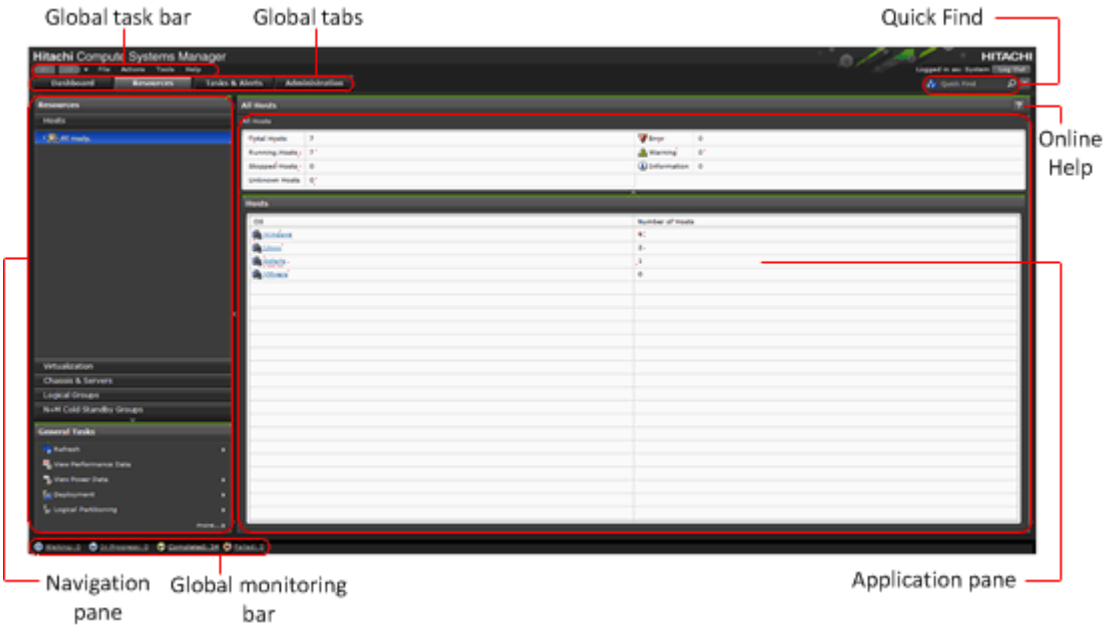
The Hitachi Compute Systems Manager management client graphical user interface provides easy access to managed resources, tasks, alerts, and administrative functions.

Navigating the Hitachi Compute Systems Manager main window

The Hitachi Compute Systems Manager main window consists of the following components:

- Global task bar
- Global tabs
- Quick Find function
- Navigation pane
- Global monitoring bar
- Application pane
- Online Help

The following figure shows the components of the main window.



Related concepts

- About the global task bar on page 29
- About the global tabs on page 29

- About the Quick Find function on page 30
- About the navigation pane on page 30
- About the application pane on page 30

Related tasks

- Viewing task status from the global monitoring bar on page 163

About the global task bar

The global task bar area of Hitachi Compute Systems Manager displays Compute Systems Manager menus and shows the name of the logged in user. This area also provides access to view Help, access to other Hitachi Command Suite products, arrow buttons for moving forward and backward through previously viewed screens, and a button for logging out.

Related tasks

- Logging out of Hitachi Compute Systems Manager on page 39

Related references

- Navigating the Hitachi Compute Systems Manager main window on page 28

About the global tabs

The global tabs area of Hitachi Compute Systems Manager displays the following tabs:

- Dashboard tab
  The Dashboard tab displays information summaries about managed resources, unresolved alerts, and other items that you define.
  If you have the applicable licenses, the dashboard displays data for performance monitoring and power monitoring.
- Resources tab
  The Resources tab displays information about the configuration of managed resources.
- Tasks & Alerts tab
  The Tasks & Alerts tab provides access to task and alert management.
- Administration tab
  The Administration tab provides access to system settings, such as user and resource management, automated event handling, and performance and power monitoring configuration.

Related tasks

- Customizing the dashboard on page 162

Related references

- Navigating the Hitachi Compute Systems Manager main window on page 28

About the Quick Find function

If you type a keyword (or partial word) in the Quick Find box, managed resources or logical group names that contain the keyword are displayed in the find results.

In the find results dialog box, you can narrow the search results by resource type or logical group or specify different search criteria if you do not find the resource or group for which you are looking.

Related references

- Navigating the Hitachi Compute Systems Manager main window on page 28

About the navigation pane

Depending on which tab is active, the navigation pane of Hitachi Compute Systems Manager displays a hierarchical tree view of managed resources, tasks, alerts, and user settings. Expand items in the navigation pane to select child objects, or to view information about those objects in the application pane.

The Resources tab also provides shortcuts to general tasks, such as discovering and refreshing resources.

Related references

- Navigating the Hitachi Compute Systems Manager main window on page 28

About the application pane

The application pane of Hitachi Compute Systems Manager displays details about items selected in the navigation pane.

You can customize the layout of this window or select items by completing the following actions:

- Click a row to select an item
  Click a check box (which selects only one line at time) or click on a specific line to select the line. To select all items in the list, click the check box on the line containing the column headers, or click Select All.
  You can select consecutive lines by holding down the Shift key and then clicking on lines.

  Note: Clicking a link in a row selects the object, not the row. To select the row, click anywhere in the row, except directly on a link.

- Sort list items by column

Click a column heading to sort the list by that column.

- Filter list results
  - Click Filter and then select attributes and values to filter the list. Use the + and - buttons to add or remove filter attributes.
  - Click On to enable filtering or click Off to disable filtering.
  - Use the Apply, Reset, and Clear buttons to apply filter values to the returned list, or to reset or clear the filter conditions.
- Display and hide columns
  Click Column Settings to specify the columns that you want to display.
- Sort columns
  Reorganize columns by dragging and dropping the column headers to the desired location.
- Copy cells or rows
  Copy selected cells or rows by right clicking in the cell or row you would like to copy and then select Copy This Cell or Copy Selected Rows, respectively, from the drop-down menu.

Related references

- Navigating the Hitachi Compute Systems Manager main window on page 28

About the global monitoring bar

The global monitoring bar of Hitachi Compute Systems Manager displays the number of tasks in a specific status.

The following task status links are displayed with a number next to them that indicates how many tasks are in that status. Click the task status link to see a list of tasks in that status.

- Waiting
- In Progress
- Completed
- Failed

Related tasks

- Viewing task status from the global monitoring bar on page 163

Related references

- Navigating the Hitachi Compute Systems Manager main window on page 28

Navigating help

The Help system provides brief explanations of the features of this product and helps you understand its capabilities. Navigating is the means by which you access the information in the Help system.

When you access **Help** > **Online Help** from the menu bar, the navigation pane displays.

If you select the help icon  from the application pane or a dialog box, click **Show All Contents** to display the navigation pane and access the Contents, Index, Search, and Glossary.

Navigating

- To navigate between topics, use the navigation pane, or right-click the topic and select Back or Forward.
- Use the breadcrumb trail at the top of each topic to see your location, or to return to a higher level topic.
- To find information for a specific topic, click the Related topics links.

Using navigation buttons

- Contents
  Open book icons in the navigation pane to reveal topic entries and subsections. As you move through Help, the current topic is highlighted.
- Index
  An alphabetical list of topics. Click an Index entry to display one or more topics that you can choose to view.
- Search
  Search for word or phrase occurrences. Click search results to display the corresponding topics.
- Glossary
  Provides brief explanations of product-related terms.

Printing topics

- To print topics, right-click the topic and select Print or click the printer icon on the button bar.

2

Initial setup

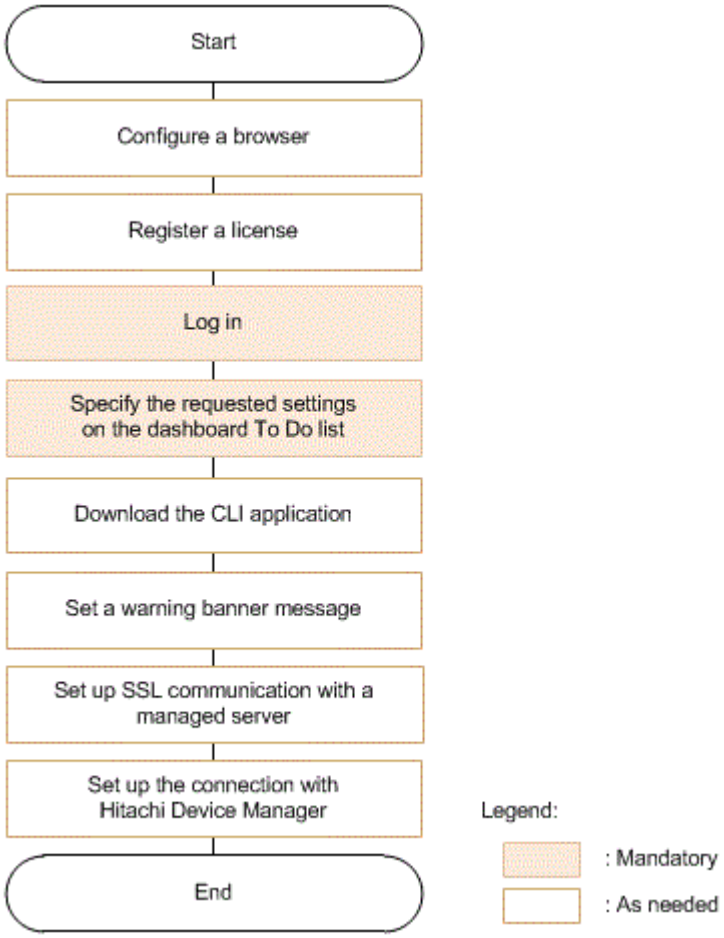
This module describes settings that are required on the management client before you can begin to use Hitachi Compute Systems Manager (HCSM).

- ☐ About initial setup
- ☐ Configuring web browser settings
- ☐ Managing licenses
- ☐ Logging in and logging out
- ☐ Configuring or changing email notification settings
- ☐ Downloading the CLI
- ☐ Setting up warning banners
- ☐ Setting up SSL secure communication for managed servers
- ☐ Setting up a connection with Hitachi Device Manager

About initial setup

The first time you log in to Hitachi Compute Systems Manager from a management client, the initial settings wizard displays in the dashboard To Do list. The wizard provides you with direct access to initial setup steps, such as editing your profile, configuring email settings, and performing discovery tasks. This wizard displays the first time you log in. For subsequent logins, after you complete the initial settings, you access these specific tasks by using the standard user interface menus and tabs. The dashboard To Do list continues to remind you of pending configuration and management tasks.

The following graphic illustrates the workflow for the initial setup of Compute Systems Manager.



For information on the settings included in the Hitachi Compute Systems Manager dashboard To Do list, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

Related tasks

- Logging in to Hitachi Compute Systems Manager on page 38

- Setting up a connection with Hitachi Device Manager on page 43

Configuring web browser settings

Hitachi Compute Systems Manager provides a web-based user interface to manage resources.

About web browser settings

Before you can log in to Hitachi Compute Systems Manager, you must verify that your web browser settings meet certain specifications.

Specify the following web browser settings when using Internet Explorer or Mozilla Firefox:

- Add-on options
- Security options
- Language options

Related tasks

- Specifying Internet Explorer settings on page 35
- Specifying Firefox settings on page 36

Specifying Internet Explorer settings

Specify the following Internet Explorer settings before logging in to Hitachi Compute Systems Manager for the first time.

Before you specify Internet Explorer settings, you must install the Adobe Flash Player. In addition, you must verify that you have not installed any browser utilities that do not allow pop-ups. The Compute Systems Manager interface requires the use of pop-ups.

Procedure

1. Open Internet Explorer.
2. Enable the Shockwave Flash Object add-on.
3. If the pop-up blocker is enabled, go to the pop-up blocker settings and add the Compute Systems Manager URL to the list of website addresses from which to allow pop-ups.
4. Add the Compute Systems Manager URL to the list of trusted sites.
5. In the security level listing for the trusted site, verify that the following scripting options are enabled:
   - **Run ActiveX controls and plug-ins**
   - **Script ActiveX controls marked safe for scripting**
   - **Active scripting**
   - **Submit non-encrypted form data** (select **Prompt** or **Enable**)
   - **File download**

6. Set English as the highest-priority language.
7. On the **Advanced** tab, do the following:
   - Select the option that allows for displaying images.
   - Clear the **Do not save encrypted pages to disk** check box.

Result

You can now access the Compute Systems Manager user interface using your browser.

Note that when using Internet Explorer on Windows Server 2008 and 2012, the browser security settings for enhanced security are enabled by default. This might cause the following conditions:

- The animation that indicates the status of the loading process does not move.
- Files cannot be downloaded from servers on which HTTPS is enabled.

To resolve either of these conditions, disable the Internet Explorer Enhanced Security Configuration.

Also note that when using Internet Explorer 9, 10, or 11, the following events might occur:

- An error message prompting the user to install Adobe Flash Player appears, even if the correct version of Adobe Flash Player is installed.
- The Help is not displayed properly.

If either of these issues occur, disable **ActiveX Filtering**, register the IP address or host name of the management server in the Internet Explorer **Compatibility View settings**, and press F5 to refresh the browser window.

Related concepts

- About web browser settings on page 35

Specifying Firefox settings

Specify the following Firefox browser settings before logging in to Hitachi Compute Systems Manager for the first time.

Before you specify Firefox settings, you must install the Adobe Flash Player. In addition, you must verify that you have not installed any browser utilities that do not allow pop-ups. The Compute Systems Manager interface requires the use of pop-ups.

Procedure

1. Open Firefox.
2. Enable the Shockwave Flash Object add-on.
3. Enable the following options:

- If the pop-up blocker is enabled, go to the pop-up blocker settings and add the Compute Systems Manager URL to the list of website addresses from which to allow pop-ups.
- Verify that English is set as the preferred language.
- Enable cookies.
- Allow automatic loading of images (for versions earlier than Firefox ESR 24).
- Enable JavaScript (for versions earlier than Firefox ESR 24).

Note: Ensure that the font size remains set at the default value. If the font size is larger than the default, text might overlap in the user interface.

Related concepts

- About web browser settings on page 35

Managing licenses

You must have a valid license to use Hitachi Compute Systems Manager.

About license management

The Hitachi Compute Systems Manager license consists of the base license for the product and plug-in licenses for specific functions. Users register the plug-in licenses as needed. The base license is automatically registered during installation of Compute Systems Manager.

If Hitachi Command Suite products other than Compute Systems Manager are used, a license is required for each product.

When the license for a Hitachi Command Suite product expires, an alert displays in the Hitachi Command Suite main window.

Related tasks

- Registering a license on page 37
- Checking the status of a license on page 38

Registering a license

You must first register a license before activating any of the Hitachi Compute Systems Manager plug-ins.

Procedure

1. Start a Web browser.
2. Specify the URL for Compute Systems Manager.

For example, `http://host-name-or-IP-address-of-management-server:22015/ComputeSystemsManager/`.

3. On the login window, click **Licenses**.

   If you are already logged in, from the **Help** menu, select **About**.
4. Register the license using one of these methods:
   - Enter the license key.
   - Specify the license key file.
5. Click **Save**.
6. Confirm that the license is successfully registered by viewing the displayed message.

   If you registered the license after you logged in, you must log out and then log in again to enable the license.

Related concepts

- About license management on page 37

Related tasks

- Checking the status of a license on page 38

Checking the status of a license

You can check the status of a Hitachi Compute Systems Manager license.

Procedure

1. On the login window, click **Licenses**.

   If you are already logged in, from the **Help** menu, select **About**.
2. Check the license status from **License Messages**.

   You can check detailed information by clicking the link for each product.

Related concepts

- About license management on page 37

Related tasks

- Registering a license on page 37

Logging in and logging out

When the installation is complete, you can log in to Hitachi Compute Systems Manager.

Logging in to Hitachi Compute Systems Manager

Before you can use Hitachi Compute Systems Manager, you must first log in to the system.

Procedure

1. Start a web browser.
2. Specify the URL for Compute Systems Manager.

   For example, `http://host-name-or-IP-address-of-management-server:22015/ComputeSystemsManager/`.
3. Type the user ID and password provided by your system administrator.
4. Click **Log In**.

Result

When you log in to Compute Systems Manager for the first time, reminders for settings that you should specify, such as registering an email address and setting the alert level for email notification are listed in a To Do list on the dashboard.

If you have items listed on the dashboard To Do list, be sure to specify the requested settings.

Related concepts

- About web browser settings on page 35

Logging out of Hitachi Compute Systems Manager

When you are done using Hitachi Compute Systems Manager, you may want to log out.

Procedure

1. In the Hitachi Compute Systems Manager menu bar, click **Log Out**.
2. Click **OK** to confirm.

Related tasks

- Logging in to Hitachi Compute Systems Manager on page 38

Configuring or changing email notification settings

Before Hitachi Compute Systems Manager can send email notifications about Compute Systems Manager system operations, such as task status and alerts, you must configure email notification settings.

About configuring email settings

You can configure Hitachi Compute Systems Manager setting so that email notifications are sent to users when a task is complete or an alert is received as follows:

- When a task is complete, an email notification is sent to the user who ran the task.

- When an alert is received from a resource, an email notification is sent to all users who belong to the user group to which the resource group containing the resource is assigned.
- Before a user can receive email notifications, you must edit the user account profile and register the email address.

Related concepts

- About alert settings on page 148

Related tasks

- Setting up email notification on page 40
- Editing a user account profile on page 201
- Editing your own profile on page 201

Setting up email notification

Before Hitachi Compute Systems Manager can send email notifications, you must specify settings that enable the management server to connect to the SMTP server. If you use authentication to connect to the SMTP server, you must also specify the user information for authentication.

To configure email notification, you need the following information:

- Host name or IP address of the SMTP server
- When using authentication, the user name and password used for authenticating connections to the SMTP server

Procedure

1. On the **Administration** tab, select **System Settings**.
2. Select **E-mail**.
3. Click **Edit Settings**.
4. To enable email notification, select the **E-mail Notification Enabled** check box and enter the required SMTP server information.
5. Optionally, to configure security settings, expand **Advanced Settings**.
6. Click **OK**.

Result

To view or confirm email notification settings, on the Administration tab, click System Settings, and then select E-mail.

Related concepts

- About configuring email settings on page 39

Downloading the CLI

Hitachi Compute Systems Manager provides a CLI for running tasks from the command line.

About downloading the CLI

To use the CLI on a management client, you must download and install the CLI application from the management server, and then set up the CLI environment.

For details about how to install and configure the CLI application, see the *Hitachi Command Suite Compute Systems Manager CLI Reference Guide*.

Related tasks

- Downloading the CLI on page 41

Downloading the CLI

Before using the CLI on a management client, you must download and install the CLI application.

Procedure

1. From the **Tools** menu, select **Download**.
2. In the **Download** dialog box, choose from the links to download the desired installation files.
3. Click **ReadMe** for installation instructions.

Related concepts

- About downloading the CLI on page 41

Setting up warning banners

This module describes how to set up login warning banners.

About warning banner settings

As a security measure during Hitachi Compute Systems Manager login, a message (warning banner) can be displayed.

A warning banner can be used to notify third parties attempting unauthorized access, and to reduce the risks from loss of data or leaked information.

Related tasks

- Logging in to Hitachi Compute Systems Manager on page 38

- Setting a warning banner message on page 42

Setting a warning banner message

Using HTML tags, edit the messages to be displayed in the Hitachi Compute Systems Manager login window.

Procedure

1. On the **Administration** tab, select **Security**.
2. Select **Warning Banner**.
3. Click **Edit Message** and type the warning message text in the **Message** box.

   You can preview the message by clicking **Preview** and viewing the message in the **Preview** box.
4. Click **OK** to save the message.
5. Confirm that the warning banner displays in the Login window.

Related concepts

- About warning banner settings on page 41

Setting up SSL secure communication for managed servers

Hitachi Compute Systems Manager registers a self-signed certificate by default so that secure SSL communication between Hitachi servers and the Compute Systems Manager management server is automatically enabled. If you want to increase security, you can create other self-signed server certificates and then use the user interface to change the SSL communication settings and enable the new certificates.

Before you enable the new self-signed certificate, you must create a keystore and register the server certificate on the management server. For details, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

Before enabling the server certificate as described in the following procedure, ensure that you have the Key Password and the Keystore Password.

Procedure

1. On the **Administration** tab, select **System Settings**.
2. Select **SSL**.
3. Click **Edit Setting**.
4. Select the **Specify the Key Password and Keystore Password** check box.
5. Type the required text in the **Key Password** and the **Keystore Password** boxes.

6. Click **OK**.

Related references

- Prerequisites for discovering blade servers and chassis on page 50

Setting up a connection with Hitachi Device Manager

Setting up a connection with Hitachi Device Manager enables you do the following:

- Automatically register Migration WWPNs when migrating an LPAR.
- View storage system information (storage system list and volume information) managed by Hitachi Device Manager. This feature requires that you install both Hitachi Device Manager and Hitachi Compute Systems Manager on the same server.

Prerequisites

Before you set up a connection with Hitachi Device Manager, confirm that you have the following required information:

- Host name or IP address
  If Compute Systems Manager and Hitachi Device Manager are installed on the same management server, Compute Systems Manager automatically connects to the local instance of Hitachi Device Manager. In this case, you cannot specify settings.
- User name
  Specify a user to which All Resources, Modify, or Admin role is assigned. If you plan to configure automatic registration for migration WWPNs, specify a user with permission to change the host group to which WWPNs for FC are registered.
- Password
- Protocol
- Port number

If you are using HTTPS, you must configure secure communications for Hitachi Device Manager before setting up the connection.

For details about how to specify these settings, refer to the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*

Procedure

1. On the **Administration** tab, select **HDvM Connection**.
2. Click **Edit Settings**.
3. To enable communication with Hitachi Device Manager, select the **Enable Device Manager Communication** check box, and enter the required information.

4. Click **Check Connection** to confirm that Compute Systems Manager can connect to Hitachi Device Manager.
5. Optionally, select the **Obtain Storage Volume information** check box.

Related tasks

- Enabling automatic registration for migration WWPNs on page 114
- Viewing a list of storage systems on page 169

3

Discovering and registering management targets

This module describes how to discover management targets, manage and unmanage resources, and specify settings for logical partitioning.

- ☐ Discovery overview
- ☐ Discovering and adding resources
- ☐ Managing and unmanaging resources
- ☐ Configuring logical partitioning
- ☐ Removing resource information from the database

Discovery overview

Hitachi Compute Systems Manager discovers management targets in your network and adds them as managed resources.

About the discovery process

The Hitachi Compute Systems Manager discovery process discovers properly configured hosts, servers, and chassis on a network within a specified IP address range. You can discover all targets within an IP address range, or by using discovery filters, narrow the discovery process to previously undiscovered targets within that range. By specifying a range of IP addresses and credentials for all the resources you want to discover, multiple resource types, such as hosts, servers, or chassis can be discovered at the same time. If you need to discover chassis resources, you can also specify an IPv6 address.

All discovered targets are automatically added as managed resources, unless you specifically disable the auto-manage feature. You can manually specify to manage or unmanage individual resources that have been discovered.

The discovery process is registered as a task in Compute Systems Manager. You can view the progress of the task on the Tasks & Alerts tab. Compute Systems Manager continues to perform the discovery task even if you log out of Compute Systems Manager.

After the discovery process is completed, if Compute Systems Manager does not discover the resources you expected to find, verify that each target resource meets the prerequisite conditions that allow the Compute Systems Manager discovery process to complete successfully.

If Hitachi Device Manager and Compute Systems Manager are run on the same management server, Compute Systems Manager automatically synchronizes the information for resources managed by Hitachi Device Manager with the information for resources managed by Compute Systems Manager. If a resource that satisfies the Compute Systems Manager discovery conditions has already been discovered in Hitachi Device Manager or if the resource is newly discovered in Hitachi Device Manager, information is automatically imported from Hitachi Device Manager and the resource is added to Compute Systems Manager and automatically managed. Similarly, if Compute Systems Manager discovers a resource that is included in a target that will be discovered by Hitachi Device Manager, that resource is automatically added to Hitachi Device Manager.

Related tasks

- Discovering and adding resources on page 51

Related references

- Prerequisites for discovering blade servers and chassis on page 50
- Prerequisites for discovering hosts on page 48

About managed resource types

Hitachi Compute Systems Manager can discover and manage the following types of resources:

- **Hosts:** Windows, Linux, and Solaris hosts can be discovered and managed.
- **Hypervisors:** Hyper-V and VMware can be discovered and managed. VMWare can also be searched for as a host.
- **Virtual machines (VMs):** When a hypervisor is discovered, virtual machines on the hypervisor are also discovered. However, the virtual machine hosts must be discovered after you configure the host environment.
- **Hitachi servers:** Hitachi blade servers and rack-mounted servers can be discovered and managed. When a chassis is discovered, all blade servers mounted on the chassis are also automatically discovered. However, the hosts on blade servers and rack-mounted servers must be discovered after you configure the host environment.
- **LPAR:** When a blade server is added as a target of a logical partitioning plug-in license, the LPARs that reside on the server automatically become managed resources. However, the LPAR hosts must be discovered after you configure the host environment.

Note: A plug-in license is required to manage LPARs.

Related tasks

- Discovering and adding resources on page 51

Related references

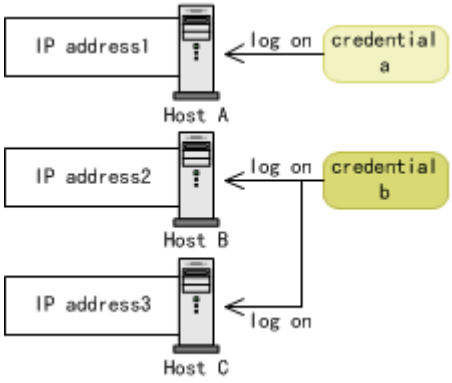
- Prerequisites for discovering blade servers and chassis on page 50
- Prerequisites for discovering hosts on page 48

About management target credentials

Information such as IDs and passwords are required for Hitachi Compute Systems Manager to access resources that you want to manage. The information for each management target is called its credentials. Credentials for all management targets must be registered before you can begin the discovery process.

If you can log into multiple resources by using the same credentials, you must register the credentials only once. For example, in the following figure, Host B and Host C have the same logon credentials. To discover all three

hosts, you must specify two credentials only; credential a (for Host A) and credential b (for Host B and Host C).



Related tasks

- Discovering and adding resources on page 51
- Registering management target credentials on page 50

Related references

- Prerequisites for discovering blade servers and chassis on page 50
- Prerequisites for discovering hypervisors and virtual machines on page 49

Discovering and adding resources

Hitachi Compute Systems Manager discovers management targets in your network and adds them to Compute Systems Manager as managed resources.

Prerequisites for discovering hosts

Before you begin the host discovery process, you must complete the following tasks for each host that you want to manage:

- Install an operating system on each host.
- Connect each host to a network that can be accessed by Hitachi Compute Systems Manager.
- Configure each host so that Compute Systems Manager can access the host by using WMI or SSH.
- Gather the following information for each host:
  - IP address of the host
  - Operating system type of the host
  - User ID and password (credentials) for the host
  - Domain name for any hosts that may be discovered by using WMI
  - SSH server port number of the hosts (when using the SSH protocol)

For more information about how to configure your targeted hosts for discovery, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

Tip: If both of the following conditions are met, information about the hosts discovered by Hitachi Device Manager is synchronized with Compute Systems Manager:

- Compute Systems Manager and Hitachi Device Manager are installed on the same management server.
- A host that meets the Compute Systems Manager discovery conditions has been discovered by Hitachi Device Manager.

Note that information about VMware discovered by Hitachi Device Manager is not synchronized with Compute Systems Manager.

Related tasks

- Registering management target credentials on page 50
- Discovering and adding resources on page 51

Prerequisites for discovering hypervisors and virtual machines

All virtual machines (VMs) and hypervisors are discovered during the Hitachi Compute Systems Manager discovery process. Before you begin the discovery process for virtual resources, you must complete the required prerequisites.

Before you begin the process of discovering hypervisors and VMs, you must complete the following tasks for each virtual resource that you want to manage:

- Verify the IP addresses of hypervisors.
- Verify the IDs and passwords required for Compute Systems Manager to access the hypervisors. For VMWare hypervisors, Compute Systems Manager requires access as the root user of the target VMware ESXi. This means you must verify the root user password.
- Set up hypervisors so that Compute Systems Manager can access them by using the appropriate protocols.
  - For Hyper-V: WMI
  - For VMware: HTTPS
- Connect hypervisors to a network that can be accessed by Compute Systems Manager.
- Verify that hypervisors are not in maintenance mode.

Related tasks

- Discovering and adding resources on page 51
- Registering management target credentials on page 50

Prerequisites for discovering blade servers and chassis

All blade servers mounted on a chassis are discovered when the chassis is discovered.

Before you begin the discovery process for blade servers and chassis, you must complete the following tasks for each chassis and blade server that you want to manage:

- Connect each chassis and blade server to a network that can be accessed by Hitachi Compute Systems Manager.
- Gather the following information for each chassis:
  - IP address of the management module
  - User ID and password (credentials) for Compute Systems Manager to access the management module
  - Port number of the management module

Related tasks

- Registering management target credentials on page 50
- Discovering and adding resources on page 51

Prerequisites for discovering rack-mounted servers

Before you begin the discovery process for rack-mounted servers, you must complete the following tasks for each rack-mounted server that you want to manage:

- Connect each rack-mounted server to a network that can be accessed by Hitachi Compute Systems Manager.
- Gather the following information for each rack-mounted server:
  - IP address of the lights-out management (LOM) module
  - Port number of the LOM

Related tasks

- Managing rack-mounted servers on page 56
- Registering management target credentials on page 50
- Discovering and adding resources on page 51

Registering management target credentials

You must register credentials for each management target before the discovery process can begin.

Before you add credentials, review the prerequisites for discovery.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. Click the **Credentials** tab.

3. Click **Add Credential**.
4. Type a credential name.

   You can use the default name.
5. Select an operating system or target type for the resource and enter the required credential information.
   - For hypervisors (VMware), enter the root user of VMware ESXi target as the user ID and enter the root user password as the password.
   - For rack-mounted servers, ensure that you do not clear the **Default Setting** check box.
6. Click **OK**.

Related tasks

- Discovering and adding resources on page 51

Related references

- Prerequisites for discovering blade servers and chassis on page 50
- Prerequisites for discovering hosts on page 48
- Prerequisites for discovering rack-mounted servers on page 50
- Prerequisites for discovering hypervisors and virtual machines on page 49

Discovering and adding resources

Management targets are discovered and added to Hitachi Compute Systems Manager as managed resources by creating a discovery task.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. On the **Discovery Settings** tab, click **Specify IP Range**.

   If the IP address range already exists for the resources you want to discover, skip to step 6.
3. Follow the instructions in the wizard to specify an IP address range and link the credentials that correspond to each resource.

   Note: To discover blade servers, specify the IP address range and credentials of the chassis on which the blade servers are mounted. All blade servers mounted on the discovered chassis are discovered.
4. Check the **Enable** check box if you want to use ping.

   Before using this option, check if your data center allows it.
5. Verify the information that you typed and click **Submit**.

   The IP address range is added to the list on the **Discover Settings** tab.
6. From the list of IP address ranges, select the IP address range you want to include in the discovery process, and then click **Discover Resources**.

7. In the **Discover Resources** window, verify the settings.
8. Optionally, select **Advanced Settings** and set the email notification settings.

   To specify additional settings:
   - **Discovery Type Criteria**: Filters the target criteria. Choose **All** or **Previously Undiscovered**.
   - **Discovery Type**: These options are available when filtering for previously undiscovered hosts. Choose **First attempt**, **Unresponsive in last discovery**, or **Failed in last discovery**.
   - By default, all discovered resources are automatically managed by Compute Systems Manager. To disable the auto-manage feature, clear **Discovered resources are automatically managed**.
9. Click **Show Plan** and confirm that the information in the plan summary is correct.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run immediately or scheduled for later. The default setting is **Now**.
10. Click **Submit** when you are ready to run the plan.

    If you selected **Now**, the discovery process begins.
11. You can check the progress and the result of the discovery task on the **Tasks & Alerts** tab.

    You can verify the discovery results for each resource by viewing the details of the task.

Postrequisites

Note: The discovery process continues even if you log out of Compute Systems Manager.

After the discovery process completes, you can view a list of the resources that were discovered on the Discovered Resources tab. For a more specific list of resource types discovered, click the resource type tabs under Discovered Resources, or view resource details on the Resources tab.

Related concepts

- About managing and unmanaging resources on page 53

Related references

- Prerequisites for discovering blade servers and chassis on page 50
- Prerequisites for discovering rack-mounted servers on page 50
- Prerequisites for discovering hosts on page 48
- Prerequisites for discovering hypervisors and virtual machines on page 49

Managing and unmanaging resources

Management targets that are discovered by Hitachi Compute Systems Manager during the discovery process are automatically managed. In some cases you might want to manually specify resources to manage or unmanage.

About managing and unmanaging resources

By default, discovered resources are automatically managed.

If you disabled the auto manage feature during the discovery process, or if you previously chose to unmanage a resource, you can manually specify a resource to manage from the discovered resources window without having to discover resources again.

Note: To manage LPARs, you must add a blade server as a logical partitioning resource by assigning a plug-in license.

To manage a previously unmanaged resource again, note the following:

- You cannot view performance data for the resource that was obtained before the resource was unmanaged.
- You must re-register the tasks that were registered before the resource was unmanaged.
- If event handling is automated, you must set up the resource again by applying the commands that you applied before the resource was unmanaged.

Related tasks

- Removing host information from the database on page 70
- Managing hosts on page 53
- Managing blade servers and chassis on page 55
- Managing hypervisors and virtual machines on page 54
- Managing rack-mounted servers on page 56
- Specifying scripted commands to run when an alert occurs on page 157

Managing hosts

By default, discovered hosts are automatically managed. If you disabled the auto-manage feature during the discovery process, or you previously chose to unmanage a host, you can manually specify hosts to manage.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. On the **Discovered Resources** tab, click the **Hosts** tab.

3. From the list of hosts, select the host you want to manage.
   To identify unmanaged hosts, sort the list by the **Managed** column.
4. Click **Manage Resources**.
5. Verify the hosts and related resources to manage and click **OK**.

Result

The value in the Managed column for each selected resource changes to Yes.

The selected resources are now being managed by Hitachi Compute Systems Manager. Any hypervisors on those hosts are also managed.

Note: Managing a host in Compute Systems Manager does not affect Hitachi Device Manager, even if the host is synchronized with Hitachi Device Manager.

Related concepts

- About managing and unmanaging resources on page 53

Related tasks

- Unmanaging hosts on page 57

Related references

- Prerequisites for discovering hosts on page 48

Managing hypervisors and virtual machines

By default, discovered hypervisors are automatically managed. In addition, all virtual machines running on the hypervisor are also managed automatically. If you disabled the auto-manage feature during the discovery process or if you chose to unmanage a specific hypervisor, you can manually specify a hypervisor to manage. When you add the hypervisor, all associated virtual machine targets are also managed. However, virtual machine hosts are not managed automatically, so you must manage them manually as needed.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. On the **Discovered Resources** tab, click the **Hypervisors** tab.
3. From the list of hypervisors, select the hypervisor that you want to manage.
4. Click **Manage Resources**.
5. Verify the hypervisors and the related resources to manage and click **OK**.

Result

The value in the Managed column for the selected hypervisor changes to Yes, and the hypervisor is now managed by Hitachi Compute Systems Manager. Hosts containing hypervisors that are managed and virtual machines that run

on the hypervisor are also managed. You can verify managed virtual machines information by using the VMs tab on the Discovered Resources tab.

Related concepts

- About managing and unmanaging resources on page 53

Related tasks

- Unmanaging hypervisors and virtual machines on page 58

Related references

- Prerequisites for discovering hypervisors and virtual machines on page 49

Managing blade servers and chassis

By default, discovered chassis are automatically managed. All blade servers mounted on a managed chassis are also automatically managed. If you disabled the auto-manage feature during the discovery process, or if you previously chose to unmanage a chassis, all blade servers mounted on that chassis are also unmanaged. You can manually specify a chassis to manage.

If you add a blade server as managed resource and also add the blade server as a logical partitioning resource by applying a plug-in license, the LPARs running on the server automatically become managed resources.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. On the **Discovered Resources** tab, click the **Chassis** tab.
3. From the list of chassis, select the chassis you want to manage.
   To identify unmanaged chassis, sort the list by the **Managed** column.
4. Click **Manage Resources**.
5. Verify the chassis and the related resources to manage and click **OK**.

Result

The value in the Managed column for each selected chassis changes to Yes.

The selected resources are now being managed by Hitachi Compute Systems Manager. You can verify which blade servers are being managed on the Blades tab in the Discovered Resources tab.

Related concepts

- About managing and unmanaging resources on page 53

Related tasks

- Unmanaging blade servers and chassis on page 58
- Adding blade servers as logical partitioning resources on page 56

Related references

- Prerequisites for discovering blade servers and chassis on page 50

Adding blade servers as logical partitioning resources

Before you can manage an existing LPAR or create a new LPAR, you must add the blade server as a managed resource by assigning an LPAR Manager license.

Prerequisites

Before adding a blade server, ensure that logical partitioning is enabled and LPAR manager is running.

Procedure

1. On the **Administration** tab, select **Logical Partitioning > Licensed Blades**.
2. Click **Add Licensed Blades** and select the blade server for which you want to add a logical partitioning plug-in license.
3. Click **OK**.

Result

The blade server is added as an LPAR managed resource and is displayed in the Licensed Blades list.

Related concepts

- About LPAR host configuration on page 67

Related tasks

- Creating an LPAR host on page 68

Managing rack-mounted servers

By default, discovered rack-mounted servers are automatically managed. If you disabled the auto-manage feature during the discovery process, or you previously chose to unmanage a rack-mounted server, you can manually specify a rack-mounted server to manage. You can manage rack-mounted servers by using the discovered servers list.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. On the **Discovered Resources** tab, click the **Rack-mounted** tab.
3. From the list of servers, select the rack-mounted servers you want to manage.

   To identify unmanaged rack-mounted servers, sort the list by the **Managed** column.

4. Click **Manage Resources**.
5. Verify the rack-mounted servers to manage and click **OK**.

Result

The value in the Managed column for each selected rack-mounted server changes to Yes.

The selected resources are now managed by Hitachi Compute Systems Manager.

Related concepts

- About managing and unmanaging resources on page 53

Related tasks

- Unmanaging rack-mounted servers on page 59

Related references

- Prerequisites for discovering rack-mounted servers on page 50

Unmanaging hosts

By default, discovered hosts are automatically managed. You can manually specify hosts to unmanage.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. On the **Discovered Resources** tab, click the **Hosts** tab.
3. From the list of hosts, select the host you want to unmanage.
4. Click **Unmanage Resources**.
5. Verify the hosts and the related resources to unmanage and click **OK**.

   The value in the **Managed** column for each selected resource changes to **No**.

Result

The selected hosts are no longer managed by Hitachi Compute Systems Manager. Any hypervisors and associated virtual machines on those hosts are also no longer managed.

Postrequisites

Note: Unmanaging a host in Compute Systems Manager does not affect Hitachi Device Manager, even if the host is synchronized with Hitachi Device Manager.

Unmanaging hypervisors and virtual machines

By default, discovered hypervisor and the virtual machines running on the hypervisor and automatically managed. If you do not want to manage a specific hypervisor, you can manually remove it from management. When you unmanage a hypervisor, all associated virtual machines are also unmanaged.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. On the **Discovered Resources** tab, click the **Hypervisors** tab.
3. From the list of hypervisors, select the hypervisor that you want to unmanage.
4. Click **Unmanage Resources**.
5. Verify the hypervisors and the related resources to unmanage and click **OK**.

Result

The value in the Managed column for the selected hypervisor changes to No, and the hypervisor is no longer managed by Hitachi Compute Systems Manager. Hosts containing hypervisors that are no longer managed and virtual machines that run on the hypervisor are also no longer managed. The virtual machines that are no longer managed can be verified by using the VMs tab on the Discovered Resources tab.

Unmanaging blade servers and chassis

By default, discovered blade servers and chassis are automatically managed. You can manually specify chassis to unmanage. When you unmanage a chassis, all blade servers and the LPARs on the blade servers mounted on the chassis are also unmanaged.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. On the **Discovered Resources** tab, click the **Chassis** tab.
3. From the list of chassis, select the chassis you want to unmanage.
4. Click **Unmanage Resources**.
5. Verify the chassis and the related resources to unmanage and click **OK**.

   The value in the **Managed** column for each selected resource changes to **No**.

Result

The selected resources are no longer managed by Hitachi Compute Systems Manager.

You can check unmanaged blade servers in the Blades tab of the Discovered Resources tab and unmanaged LPARs in the LPARs tab of the Discovered Resources tab.

Removing logical partitioning resources

You can remove the managed resources for which you are no longer managing logical partitioning.

Prerequisites

Before removing a blade server, ensure that you enabled logical partitioning and that LPAR manager is running.

Procedure

1. On the **Administration** tab, select **Logical Partitioning > Licensed Blades**.
2. Select the blade server from which to remove the logical partitioning plug-in license, and then click **Remove Licensed Blades**.
3. Click **OK**.

Result

The blade server is removed as an LPAR managed resource and is no longer displayed in the Licensed Blades list.

Related concepts

- About LPAR host configuration on page 67

Unmanaging rack-mounted servers

By default, discovered rack-mounted servers are automatically managed. You can manually specify rack-mounted servers to unmanage.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. On the **Discovered Resources** tab, click the **Rack-mounted** tab.
3. From the list, select the rack-mounted servers you want to unmanage.
4. Click **Unmanage Resources**.
5. Verify the rack-mounted servers and the related resources to unmanage and click **OK**.

   The value in the **Managed** column for each selected resource changes to **No**.

Result

The selected resources are no longer managed by Hitachi Compute Systems Manager.

Configuring logical partitioning

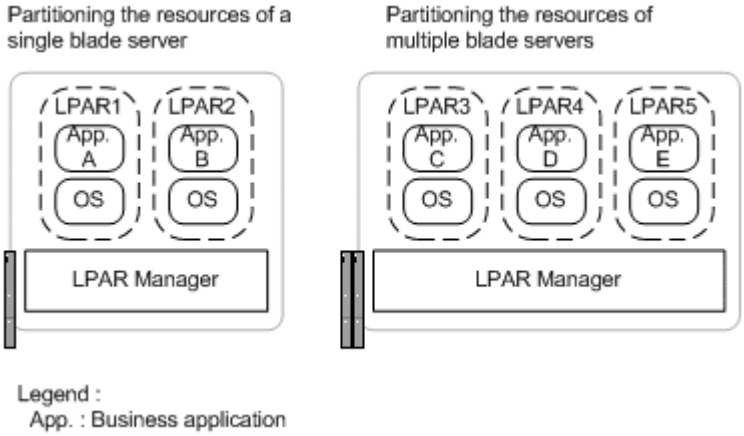
You can configure logical partitioning for Hitachi blade servers and create LPARs.

About logical partitioning settings

Logical partitioning enables you to logically divide (partition) a blade server of one or more blades into individual, independent server environments. You can use Hitachi Compute Systems Manager to logically partition a physical resource into separate Logical Partitions called LPARs. Each LPAR can run a different operating system or business application. LPARs are managed by an LPAR Manager on the blade server.

A plug-in license is required to use logical partitioning functions in Hitachi Compute Systems Manager.

The following figure shows examples of logical-partitioning-based server configurations.



You can use Hitachi Compute Systems Manager to configure the logical partitioning requirements and create LPARs. You can also use Hitachi Compute Systems Manager to change logical partitioning configuration and LPAR settings as needed.

Related concepts

- About LPAR host configuration on page 67
- Management target registration workflow on page 19

Related tasks

- Adding blade servers as logical partitioning resources on page 56

Configuring logical partitioning

Prerequisites

Before configuring logical partitioning, verify the following:

- Blade servers are not running.
- All running hosts are unmanaged before enabling or disabling logical partitioning.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers**.
2. Expand the tree and select **Blade**.
3. From the server list, select the server that you want to configure.
4. From the **More Actions** menu, select **Configure Logical Partitioning**.
5. To enable logical partitioning, select the **Enable Logical Partitioning** check box and fill out the values for the LPAR Manager ID, LPAR Manager IP address, virtual NIC system number, and other items.

   To disable logical partitioning, clear the check box.

   After configuring these items, you can also choose to activate LPAR Manager or a server.
6. Click **Show Plan** and verify that the task information displayed in the summary is correct.
7. Click **Submit**.

Result

You can view task progress and results on the Tasks & Alerts tab.

You can also view the logical partitioning settings on the Logical Partitioning tab of the window displaying the blade server information.

Related concepts

- About logical partitioning settings on page 60

Related tasks

- Configuring logical partitioning advanced settings on page 61
- Viewing logical partition configuration on page 63

Configuring logical partitioning advanced settings

Using Hitachi Compute Systems Manager, you can configure advanced settings for logical partitioning, including PCI device settings and auto shutdown.

Before changing the logical partitioning advanced settings, ensure that LPAR manager is running and that you added the blade server as a logical partitioning resource by assigning a plug-in license.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers**.
2. Expand the tree and select **Blade**.
3. From the server list, click the **Server Name** that you want to configure. The configuration information for the managed server appears.
4. Select **Logical Partitioning** and then select **LPAR Manager Information**.
5. Click **Edit Logical Partitioning Advanced Settings**.
6. Read the on-screen instructions and set the values for the LPAR Manager ID, LPAR Manager IP address, virtual NIC system number, and other items.
7. Click **Show Plan** and verify that the task information displayed in the summary is correct.
8. Click **Submit**.

Result

You can view the task progress and result on the Tasks & Alerts tab.

You can also view the logical partitioning settings on the Logical Partitioning tab of the window displaying the blade server information.

Related concepts

- About logical partitioning settings on page 60

Related tasks

- Configuring logical partitioning on page 61
- Viewing logical partition configuration on page 63

Changing the USB auto assignment setting

When you enable USB auto assignment, the reserved USB is automatically assigned at the time the LPAR is activated.

Specify either of the following options:

- All LPARs
  Each activated LPAR is assigned a reserved USB.
- Specific LPAR
  A specific USB is assigned to a single target LPAR.

To disable auto assignment of a USB to an LPAR, do not specify any LPARs to which the USB is assigned.

Before changing the USB auto assignment setting, ensure that:

- LPAR Manager is running.
- The blade server is logical partitioning resource with an assigned plug-in license.
- If you are specifying a particular LPAR for USB auto-assignment, ensure that the USB is reserved on the target LPAR.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers**.
2. Expand the tree and select **Blade**.
3. From the server list, click the **Server Name** link of the server containing the LPAR that you want to change.
   The configuration information for the managed server appears.
4. Click **Logical Partitioning > USB > Specify LPAR USB Auto Assignment**.
5. Read the on-screen instructions and configure the required settings.
6. Click **Show Plan** and verify that the task information displayed in the summary is correct.
7. Click **Submit**.

Result

You can view the tasks progress and result on the Tasks & Alerts tab.

You can also view USB auto assignment information from the blade server information window by selecting the Logical Partitioning tab and then selecting the USB tab.

Related concepts

- About logical partitioning settings on page 60
- About LPAR USB assignments on page 128

Related tasks

- Viewing detailed server information on page 167

Viewing logical partition configuration

Using Hitachi Compute Systems Manager, you can view basic logical partitioning configuration information including the LPAR Manager ID and IP address, along with advanced setting information such as the PCI settings.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers**.
2. Expand the tree and select **Blade**.
3. From the server list, click the **Server Name** that you want to view.
   The configuration information for the managed server appears.
4. Select **Logical Partitioning**.

Related concepts

- About logical partitioning settings on page 60

Related tasks

- Configuring logical partitioning on page 61

Creating LPARs

To create an LPAR, you can specify settings related to the CPU, memory, NIC, FC, and USB assignment.

Before you create an LPAR, ensure that LPAR manager is running and the blade server is a logical partitioning resource with an assigned plug-in license.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers**.
2. Expand the tree and select **Blade**.
3. From the server list, click the **Server Name** link of the server on which you want to create the LPAR.
   The configuration information for the managed server opens.
4. Click the **Logical Partitioning** tab, and then select **LPAR**.
5. From the **LPAR Management** menu, select **Create LPAR**.
   Follow the wizard to set up the details for the new LPAR.
6. In the LPAR basic information settings window, set the LPAR name and related details.
   In this window, you can also set the activation order.
7. In the CPU settings window, set the CPU allocation, number of logical CPUs, and other related settings.
8. In the memory settings window, set the memory size and related settings.
9. In the NIC settings window, set the shared NIC and related settings.
   To change settings for each shared NIC, select the target NIC, and then click **Edit Virtual NIC**.
10. In the FC settings window, set the shared FC and related settings.
11. In the USB settings window, set the USB to reserve on the LPAR.
    To use web remote KVM on an LPAR or on a host on the LPAR, or to use USB on an LPAR, you must first reserve a USB on the LPAR, and then assign the USB to the LPAR.
12. In the confirmation window, expand **Plan Details**, and then verify the task information.
13. Click **Submit**.

Result

You can view the progress and execution result of the task on the Tasks & Alerts tab.

The newly created LPAR automatically becomes a managed resource.

You can view the LPAR settings by accessing the LPAR list and clicking the LPAR Name link.

Related concepts

- About LPAR host configuration on page 67

Related tasks

- Changing LPAR settings on page 65
- Creating multiple LPARs on page 66
- Viewing detailed LPAR information on page 169
- Adding blade servers as logical partitioning resources on page 56

Changing LPAR settings

You can use Hitachi Compute Systems Manager to change LPAR settings, such as CPU, memory, NIC, FC, and USB assignment settings.

Prerequisites

Before changing LPAR settings, ensure the following:

- The LPAR Manager is running.
- The blade server is a logical partitioning resource with an assigned plug-in license.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Logical Partitions > LPAR**.
2. In the list of LPARs, click the **LPAR Name** link of the LPAR for which you want to change settings.
   The configuration information for the managed LPAR is displayed.
3. Select the tab that contains the settings that you want to change.
4. Click the edit button and then change the settings.
5. Click **Show Plan** and verify that the task information displayed in the summary is correct.
6. Click **Submit**.

Result

You can view the progress and execution result of the task on the Tasks & Alerts tab.

You can view the LPAR settings in the LPAR details window.

Related concepts

- About LPAR host configuration on page 67

Related tasks

- Creating LPARs on page 64
- Creating multiple LPARs on page 66
- Viewing detailed LPAR information on page 169
- Adding blade servers as logical partitioning resources on page 56

Creating multiple LPARs

You can use Hitachi Compute Systems Manager to create multiple LPARs simultaneously on a specific blade server or LPAR Manager.

When you create multiple LPARs simultaneously, the system uses default values for certain parameters such as the LPAR number and name. After creating the LPARs, you must check the settings for each LPAR and change them as necessary.

Prerequisites

Before creating multiple LPARs, ensure that the LPAR manager is running and that the blade server is a logical partitioning resource with an assigned plug-in license.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Use either of the following methods to display a list of LPARs:
   - Select **All Logical Partitions** and then select **LPAR**.
   - Select **All Servers > Blade** and then from the server list, click the **Server Name** link of the server on which to create LPARs. When the server configuration information window appears, select **Logical Partitioning** and then select **LPAR**.
3. On the **LPAR Management** menu, click **Quick Create Multiple LPARs**.
4. Read the on-screen instructions and configure the necessary settings.

   You can enter the **LPAR Manager ID** by clicking **Select**, and then in the **Select LPAR Manager** window, select the LPAR Manager for the LPAR that you want to create.

   When creating multiple LPARs simultaneously by selecting a specific blade server, the **Select** button is not displayed, because the LPAR Manager is identified.
5. Click **Show Plan** and verify that the task information displayed in the summary is correct.
6. Click **Submit**.

Result

You can view the progress and execution result of the task on the Tasks & Alerts tab.

You can also change settings for the new LPARs.

Related concepts

- About LPAR host configuration on page 67

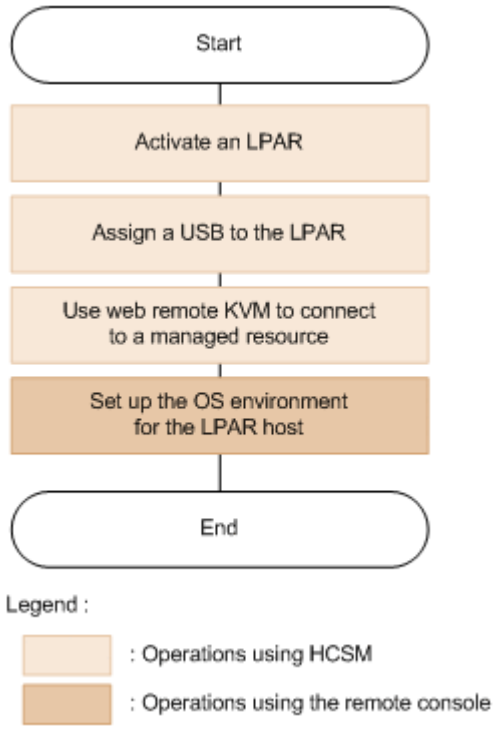
Related tasks

- Creating LPARs on page 64
- Changing LPAR settings on page 65
- Adding blade servers as logical partitioning resources on page 56

About LPAR host configuration

To create a host on an LPAR, you must use web remote KVM. The remote console is used to operate the LPAR when setting up an operating system environment for the LPAR host during host creation.

The following flowchart shows the steps to create a host on an LPAR. These steps are required for each LPAR.



You can take a snapshot of an LPAR and use Deployment Manager to deploy a new LPAR. The new LPAR includes any hosts that were running on the source LPAR.

Related concepts

- About Deployment Manager on page 130
- Management target registration workflow on page 19

Related tasks

- Creating an LPAR host on page 68

Related references

- Prerequisites for LPAR host configuration on page 68

Prerequisites for LPAR host configuration

Before configuring a host for an LPAR, complete the following tasks:

- Ensure that the FC WWN is set for the LPAR by reviewing the information in the LPAR details window.
- Assign devices to specify when setting up an operating system environment for the LPAR.
  Use Hitachi Device Manager to allocate storage system volumes to the LPAR as devices available for booting. When allocating such volumes, use the FC WWN information set for the LPAR.
  For details about using Hitachi Device Manager, see the *Hitachi Command Suite User Guide*.
- Set the FC for the LPAR.
  When installing on operating system, set only one port that is bootable. If two or more ports are enabled, they may not be recognized correctly. If using two or more ports for redundancy, change the FC setting for the LPAR after installing the operating system.
- Activate the LPAR and assign a USB to it.
  By enabling USB auto assignment, you can assign a USB automatically when the LPAR is activated.

Related concepts

- About LPAR host configuration on page 67

Related tasks

- Creating an LPAR host on page 68

Creating an LPAR host

You can create a host on an LPAR.

Procedure

1. Use Web remote KVM to connect to the LPAR on which you want to create the host.
2. Use the remote console to set up the operating system environment:

a. Select the device to use for booting.

   Specify the boot priority of the devices according to the installation environment.

b. Install the operating system.

c. Shut down the operating system.

For information about using the remote console to set up an operating system environment, see the relevant blade server manual.

Result

After completing the steps for all the LPARs on which you want to create a host, disable USB auto assignment.

If USB auto assignment is left enabled, USB may be assigned unintentionally.

Related concepts

- About LPAR host configuration on page 67

Related references

- Prerequisites for LPAR host configuration on page 68

Removing resource information from the database

When managing a resource is no longer necessary, you can remove the resource and all information about the resource from the Hitachi Compute Systems Manager database.

About removing resource information from the database

All information about a resource previously discovered by Hitachi Compute Systems Manager is stored in the Compute Systems Manager database for both managed and unmanaged resources. Resource information can be removed from the Compute Systems Manager database, regardless of whether the resources are managed.

If you physically remove a resource from your network, you should also remove information about the resource from the Compute Systems Manager database. Unmanaging a resource does not automatically remove the information from the database.

Related tasks

- Removing host information from the database on page 70
- Removing blade server and chassis information from the database on page 71
- Removing hypervisor and virtual machine information from the database on page 70

- Removing rack-mounted server information from the database on page 72

Removing host information from the database

You can remove a host and all information about the host from the Hitachi Compute Systems Manager database.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. On the **Discovered Resources** tab, click the **Hosts** tab.
3. From the list of hosts, select the host to remove.
4. Click **Remove Resources**.
5. Verify the hosts and related resources to remove and click **OK**.

Result

The host and all information about the host is removed from the Compute Systems Manager database. The removed resources no longer appear in Compute Systems Manager. Information about the hypervisors on the hosts is also deleted.

Postrequisites

Note: Removing resources and resource information from Compute Systems Manager does not affect Hitachi Device Manager, even if the resource is synchronized with Hitachi Device Manager.

Related concepts

- About removing resource information from the database on page 69

Related tasks

- Removing hypervisor and virtual machine information from the database on page 70
- Removing blade server and chassis information from the database on page 71
- Removing rack-mounted server information from the database on page 72

Removing hypervisor and virtual machine information from the database

When you remove a hypervisor, all the information about the hypervisor and associated virtual machines is also removed from the database.

Procedure

1. On the **Administration** tab, select **Managed Resources**.

2. On the **Discovered Resources** tab, click the **Hypervisors** tab.
3. From the list of hypervisors, select the hypervisor that you want to remove from the database.
4. Click **Remove Resources**.
5. Verify the hypervisors and related resources to remove, and then click **OK**.

Result

The removed hypervisor is no longer displayed in the list of hypervisors. The hypervisor is no longer managed, and is no longer in the Hitachi Compute Systems Manager database. Information about the virtual machines that run on the hypervisor and information about hosts containing hypervisors is also removed. The removed virtual machines are no longer displayed in the virtual machine list of the VMs tab on the Discovered Resources tab.

Related concepts

- About removing resource information from the database on page 69

Related tasks

- Removing host information from the database on page 70
- Removing blade server and chassis information from the database on page 71
- Removing rack-mounted server information from the database on page 72

Removing blade server and chassis information from the database

When you remove a chassis, all information about the chassis and the associated blade servers is also removed from the Hitachi Compute Systems Manager database.

Note: Because blade server information is managed by chassis, you do not need to make any changes within Compute Systems Manager if you are only removing a specific blade. When you physically remove a single blade from a chassis, information about the blade server remains in the database as long as the chassis is managed. If you remove a blade that is associated with a plug-in license such as Logical Partitioning Manager, Deployment Manager, or N+M Cold Standby, remove the resource from the list of licensed resources or N+M Cold Standby groups.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. On the **Discovered Resources** tab, click the **Chassis** tab.
3. From the list of chassis, select the chassis to remove.
4. Click **Remove Resources**.
5. Verify the chassis and related resources to remove and click **OK**.

All information about the chassis is removed from the Compute Systems Manager database. All blade servers mounted on the chassis and the LPARs on the blade servers are also removed.

Result

The removed resources no longer appear in Compute Systems Manager.

The removed blade servers are no longer listed in the Blades tab of the Discovered Resources tab, and removed LPARs are not listed in the LPARs tab of the Discovered Resources tab.

Related concepts

- About removing resource information from the database on page 69

Related tasks

- Removing hypervisor and virtual machine information from the database on page 70
- Removing host information from the database on page 70
- Removing rack-mounted server information from the database on page 72
- Removing logical partitioning resources on page 59
- Removing managed resources from Deployment Manager on page 133
- Removing a blade from an N+M cold standby group on page 106

Removing rack-mounted server information from the database

When you remove a rack-mounted server, all information about that server is also removed from the Hitachi Compute Systems Manager database.

Procedure

1. On the **Administration** tab, select **Managed Resources**.
2. On the **Discovered Resources** tab, click the **Rack-mounted** tab.
3. From the list of servers, select the rack-mounted servers to be removed.
4. Click **Remove Resources**.
5. Verify the rack-mounted servers to remove and click **OK**.

   All information about the rack-mounted server is removed from the Compute Systems Manager database.

Result

The removed resources no longer appear in Compute Systems Manager.

Related concepts

- About removing resource information from the database on page 69

Related tasks

- Removing blade server and chassis information from the database on page 71
- Removing host information from the database on page 70
- Removing hypervisor and virtual machine information from the database on page 70

4

Using Compute Systems Manager to manage resources

This module describes the management operations available for managed resources.

- Managing power settings for managed resources
- Using location identifier lamps to locate hardware
- Configuring and using N+M cold standby
- Migrating LPARs
- Capping resource power consumption
- Managing tasks
- Using related Hitachi management software
- Setting up Virtual Machine Manager connections for managing virtual resources
- Configuring and using Deployment Manager
- Updating firmware

Managing power settings for managed resources

This module describes how to configure Hitachi Compute Systems Manager to perform remote power management of managed resources.

About power management

You can control the power to resources managed by Hitachi Compute Systems Manager by registering a resource's management interface information for lights-out management (LOM) or enabling Wake-on-LAN (WoL).

Power management options for managed resources include:

- Turning on the power of or starting a managed resource
  - Turning on the power
    Turns on the power of the host, the server, or the virtual machine.
    When you turn on the power of a host, the operating system starts.
    When you turn on the power of a server or a virtual machine, and an operating system or guest operating system is installed on the host, the operating system also starts.
    LPAR Manager also starts on the blade server if logical partitioning is in use. Depending on the LPAR settings, the related LPARs also start.
  - Starting
    If an operating system is installed on the host of an LPAR, the operating system starts.
- Turning off the power of or stopping a managed resource
  - Forcibly turning off the power
    Turns off the power without shutting down the host, the server, the operating system on the virtual machine, or the guest operating system.
  - Stopping
    Stops the operating system of the LPAR host without shutting down the operating system.
  - Shutting down
    Shuts down the operating system on the host, and then turns off the power.
    On LPAR Manager, this action shuts down the operating system on the LPARs, and then shuts down the managed resource.
- Restarting a managed resource
  - Rebooting
    Shuts down the operating system on the host, and then turns on the power again.
  - Resetting
    Forcibly turns off the power of the virtual machine or the server, and then turns on the power again.

- Restarting
  Shuts down LPAR Manager or stops the LPAR, and then restarts it. When LPAR Manager is restarted, depending on the LPAR settings, the LPARs on LPAR Manager also start.

Note: Power supplies for virtual machines are managed according to the hypervisor settings for the host running as a hypervisor.

You can also manage power by scheduling power management tasks. For example, you could set up the following management tasks:

- Turning off power to a host every weekend
- Restarting a host on the first Saturday of every month
- Shutting down the server every weekend

Related tasks

- Turning on power to a host on page 79
- Turning on a server on page 85
- Turning off power to a host on page 80
- Turning on power to a virtual machine on page 83
- Refreshing chassis information on page 172
- Refreshing host information on page 170
- Refreshing server information on page 173

Related references

- Example host power management schedules on page 91
- Prerequisites for power management on page 77

Prerequisites for power management

Before you can configure power management, you must complete the following tasks for the resources for which you want to manage power:

- Collect the name and IP address of each host you want to manage.
- Collect the name of the blade server for which you want to manage the power supply, the name of the chassis that contains the blade server, and the slot number of the blades.
- Collect the name of the rack-mounted server for which you want to manage the power supply, and the LOM IP address.
- Collect the name of the virtual machine for which you want to manage the power supply and the name of the hypervisor on which the virtual machine is mounted.
- Collect the name or number of the LPAR for which you want to manage power.
- Collect the ID of the LPAR Manager associated with the LPARs.
- Specify auto shutdown and other settings for logical partitioning (when managing the power supply for LPAR Manager).

- Specify activation order for LPARs (when managing the power supply for LPARs).
- Assign the resource groups that contain the resources running on the target resources to the user group. This means that in addition to assigning the resource group containing the resource targets to the user group, you must also assign the resource groups that contain all the resources running on the targets.
- Set up power management for a hypervisor by using the hypervisor interface to set up power management for the all associated virtual machines. You must set up power management for all virtual machines if you want to manage power for a hypervisor.
- Specify a timeout period for power management (if changing the default settings).
- Set lights-out management (LOM) for hosts (if managing the power supply for a physical host mounted on a non-Hitachi server).
- Refresh resource information to see the most recent power supply status updates (optional).
- Register LOM settings for each host.
  Gather the following LOM settings information for each host connected to a non-Hitachi server:
  - LOM IP address
  - IPMI login ID and password of the user with Administrator permission for LOM

Related tasks

- Registering LOM settings on page 78
- Setting a timeout period for power management on page 79
- Refreshing host information on page 170
- Assigning resource groups and roles to a user group on page 214

Registering LOM settings

To power on or force power off to a physical host mounted on a non-Hitachi server, you must configure access to the management interface of the host by registering LOM settings. You must register LOM settings before starting power management tasks.

Note: If the LOM settings of the host are not registered, Hitachi Compute Systems Manager attempts to power on the host by using Wake-on-LAN (WoL). WoL must be enabled on the host network adapter. For information about enabling WoL, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

Procedure

1. On the **Resources** tab, select the host for which you want to set LOM settings.

2. From the **More Actions** menu, click **Specify LOM Address**.
3. Enter the required information.

> **Note:** In some cases, the use of a password or user name is not supported when connecting to a host management interface. In this case, select **User ID not required** or **Password not required**.

4. Click **OK**.

Result

The LOM IP address appears in the LOM Address column for the host for which you registered LOM settings. Compute Systems Manager can now manage the power supply for this host.

Related references

- Prerequisites for power management on page 77

Setting a timeout period for power management

You can specify a timeout period for each type of power management setting.

Procedure

1. On the **Administration** tab, select **System Settings**.
2. Click **Timeouts**.
3. Click **Edit Timeout Settings**.
4. Specify a timeout period (in seconds), and click **OK**.

Result

To confirm the new settings, click the Administration tab, and then select System Settings > Timeouts.

Related references

- Prerequisites for power management on page 77

Turning on power to a host

You can turn on power for a managed host and schedule the task to be performed either immediately or at a later time. You can also schedule the task to repeat at specified intervals.

> **Note:** Power supplies for virtual machines are managed according to the hypervisor settings for the host running as a hypervisor.

Procedure

1. On the **Resources** tab, access the list of hosts and select the hosts that you want to turn on.
2. Click **Power Management** and select **Power On**.
3. Optionally, expand **Advanced Settings** to set email notification preferences.
4. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
5. Click **Submit**.

   The power-on process begins.

Result

You can verify the progress and execution results on the Tasks & Alerts tab.

Note: The power-on process continues even if you log out of Hitachi Compute Systems Manager.

You can check the status of the power supply for the managed host on the Resources tab.

Related tasks

- Turning off power to a host on page 80

Related references

- Prerequisites for power management on page 77

Turning off power to a host

You can turn off power to a managed host.

Note: Power supplies for virtual machines are managed according to the hypervisor settings for the host running as a hypervisor.

Procedure

1. On the **Resources** tab, access the list of hosts and select the hosts that you want to turn off.
2. Click **Power Management** and select **Shutdown OS**.
3. Optionally, expand **Advanced Settings** to set email notification preferences.

4. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
5. Click **Submit**.

   The shutdown process starts.

Result

You can check the progress and execution results on the Tasks & Alerts tab.

Note: The shutdown process continues even if you log out of Hitachi Compute Systems Manager.

You can check the status of the power supply for the managed host on the Resources tab.

Related tasks

- Turning on power to a host on page 79

Related references

- Prerequisites for power management on page 77

Forcing shutdown of a host

You can force a host to power off if an alert is generated indicating that the operating system cannot be controlled or if an attempt to shut down the host fails.

Procedure

1. On the **Resources** tab, access the list of hosts and select the hosts for which you want to force off the power.
2. Click **Power Management**, then select **Force Power Off**.
3. Optionally, expand **Advanced Settings** to set email notification preferences.
4. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
5. Click **Submit**.

   The power-off process begins at the scheduled time. You can verify the progress and execution results on the **Tasks & Alerts** tab.

Result

You can check the status of the power supply for the managed host on the Resources tab.

Note: The shutdown process continues even if you log out from Hitachi Compute Systems Manager.

Related tasks

- Turning on a server on page 85

Related references

- Prerequisites for power management on page 77

Restarting a host

You can restart a managed host.

Note: Power supplies for virtual machines are managed according to the hypervisor settings for the host running as a hypervisor.

Procedure

1. On the **Resources** tab, select the hosts you want to reboot from the list of hosts.
2. Click **Power Management** and select **Reboot OS**.
3. Optionally, expand **Advanced Settings** to set email notification preferences.
4. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.
      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
5. Click **Submit**.
   The restart process starts.

Result

You can verify the progress and execution results on the Tasks & Alerts tab.

Note: The reboot process continues even if you log out from Hitachi Compute Systems Manager.

Related references

- Prerequisites for power management on page 77

Turning on power to a virtual machine

You can turn on power for one or more virtual machines. This task is usually run on virtual machines with no mounted hosts, but if there are hosts mounted on the virtual machine, the guest operating system also starts.

Procedure

1. On the **Resources** tab, select **Virtualization**.
2. Select **All Virtual Machines**.
3. Expand the tree, and select the type of virtual machine that you want to power on.
4. From the list of virtual machines, select one or more virtual machines that you want to power on.
5. Click **Power Management** and select **Power On**.
6. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.
      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
7. Click **Submit**.
   The power-on processing starts. In the **Tasks & Alerts** tab, you can check the task progress and results.

> **Note:** Hitachi Compute Systems Manager continues the processing to turn power on even if you log out from Compute Systems Manager during the processing.

Result

On the Resources tab, you can check the power status of virtual machines.

Related tasks

- Forcing a virtual machine to power off on page 84

Related references

- Prerequisites for power management on page 77

Resetting a virtual machine

You can reset one or more virtual machines without shutting down the operating system. Resetting a virtual machine consists of forcing the power off and then powering it on. If you are unable to restart a mounted host, you can use this task to restart the host operating system.

Procedure

1. On the **Resources** tab, select **Virtualization**.
2. Select **All Virtual Machines**.
3. Expand the tree, and select the type of virtual machine for which you want to reset the power.
4. From the list of virtual machines, select one or more virtual machines for which you want to reset the power. You can select multiple virtual machines.
5. Click **Power Management** and select **Power Reset**.
6. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
7. Click **Submit**.

   The power-reset processing starts. In the **Tasks & Alerts** tab, you can check the task progress and results.

Note: Hitachi Compute Systems Manager continues the power-reset process even if you log out from Compute Systems Manager during the processing.

Result

On the Resources tab, you can check the power status of virtual machines.

Related references

- Prerequisites for power management on page 77

Forcing a virtual machine to power off

You can force power off to one or more virtual machines. If a failure occurs in which the virtual machine cannot be controlled and the power cannot be turned off using standard methods, you can force the power to turn off on the managed virtual machines.

Procedure

1. On the **Resources** tab, select **Virtualization**.
2. Select **All Virtual Machines**.
3. Expand the tree, and select the type of virtual machine for which you want to forcibly turn off power.
4. From the list of virtual machines, select one or more virtual machines for which you want to forcibly turn off power.

   You can select multiple virtual machines.

5. Click **Power Management** and select **Force Power Off**.
6. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.
      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
7. Click **Submit**.
   The forced-power-off processing starts. In the **Tasks & Alerts** tab, you can check the task progress and results.

Note: Hitachi Compute Systems Manager continues the process of forcibly turning off the power even if you log out from Compute Systems Manager during the processing.

Result

On the Resources tab, you can check the power status of virtual machines.

Related tasks

- Turning on power to a virtual machine on page 83

Related references

- Prerequisites for power management on page 77

Turning on a server

You can turn on power for a managed server. When a server contains multiple blades, the power is turned on at the server level. LPAR Manager and virtual machines on the server also start. LPARs on LPAR Manager also start according to the settings specified for LPARs.

Note: If there are hosts mounted on the server, the operating system also starts.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Click **All Servers**.
3. Expand the tree and select the type of server you want to turn on.
4. From the list of servers, select the servers you want to turn on.
   You can select multiple servers.
5. Click **Power Management** and select **Power On**.
6. Optionally, expand **Advanced Settings** to set email notification preferences.

7. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
8. Click **Submit**.

   The power-on process begins.

Result

You can verify the task progress and results on the Tasks & Alerts tab.

Note: The power-on process continues even if you log out of Hitachi Compute Systems Manager.

You can check the status of the power supply for the managed server on the Resources tab.

Related tasks

- Forcing a server to power off on page 87

Related references

- Prerequisites for power management on page 77

Resetting the power for a server

You can reset the power for a managed server without shutting down the operating system. Resetting a server consists of forcing the power off and then powering it on. When a server contains multiple blades, the power is reset at the server level.

Note: If you are unable to restart a mounted host, you can use this task to restart the host operating system.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Click **All Servers**.
3. Expand the tree and select the type of server for which you want to reset power.
4. From the list of servers, select the servers for which you want to reset power.

   You can select multiple servers.
5. Click **Power Management** and select **Power Reset**.
6. Optionally, expand **Advanced Settings** to set email notification preferences.

7. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
8. Click **Submit**.

   The power-reset process begins.

Result

You can verify the progress and execution results on the Tasks & Alerts tab.

Note: The power-reset process continues even if you log out of Hitachi Compute Systems Manager.

You can check the status of the power supply for the managed server on the Resources tab.

Related references

- Prerequisites for power management on page 77

Forcing a server to power off

You can force a server to power off if an alert is generated indicating that the server cannot be controlled or if an attempt to turn off the server fails. When a server contains multiple blades, the power is forced to turn off at the server level.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Click **All Servers**.
3. Expand the tree and select the type of server you want to turn off.
4. From the list of servers, select the servers you want to turn off.

   You can select multiple servers.
5. Click **Power Management**, then select **Force Power Off**.
6. Optionally, expand **Advanced Settings** to set email notification preferences.
7. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
8. Click **Submit**.

The power-off process begins at the scheduled time. You can verify the progress and execution results on the **Tasks & Alerts** tab.

Result

You can check the status of the power supply for the managed server on the Resources tab.

Note: The power-off process continues even if you log out from Hitachi Compute Systems Manager.

Related tasks

- Turning on a server on page 85

Related references

- Prerequisites for power management on page 77

Shutting down LPAR Manager

You can shut down LPAR Manager. When you shut down LPAR Manager, the LPAR hosts shut down, the LPARs are deactivated, the LPAR Manager shuts down, and then the server powers off.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers > Blade**.
2. From the list of servers, select a server on which to shut down LPAR Manager.
3. Click **Power Management** and then select **Shutdown LPAR Manager**.
4. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.
      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
5. Click **Submit**.

Result

On the Tasks & Alerts tab, you can check the task progress and results.

On the Resources tab, you can check LPAR Manager power status.

Related tasks

- Restarting LPAR Manager on page 89

Related references

- Prerequisites for power management on page 77

Restarting LPAR Manager

You can restart LPAR Manager. Depending on the LPAR settings, the LPARs on the LPAR Manager and the hosts on the LPARs also restart.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers > Blade**.
2. From the list of servers, select a server on which you want to restart LPAR Manager.
3. Click **Power Management** and then select **Restart LPAR Manager**.
4. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.
      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
5. Click **Submit**.

Result

On the Tasks & Alerts tab, you can check the task progress and the results.

On the Resources tab, you can check LPAR power status.

Related tasks

- Shutting down LPAR Manager on page 88

Related references

- Prerequisites for power management on page 77

Activating LPARs

Using Hitachi Compute Systems Manager, you activate LPARs that are not currently active. Before activating an LPAR, ensure that you start LPAR Manager.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Logical Partitions > LPAR**.
2. From the list of LPARs. select the LPAR that you want to activate.
3. Click **Power Management** and then select **Activate**.

4. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
5. Click **Submit**.

Result

On the Tasks & Alerts tab, you can check the task progress and results.

On the Resources tab, you can check LPAR power status.

Related tasks

- Deactivating LPARs on page 90
- Reactivating LPARs on page 91

Related references

- Prerequisites for power management on page 77

Deactivating LPARs

You can deactivate LPARs in certain cases, such as when the host on an LPAR abnormally stops.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Logical Partitions > LPAR**.
2. From the list of LPARs. select an LPAR that you want to deactivate.
3. Click **Power Management** and then select **Deactivate**.
4. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
5. Click **Submit**.

Result

On the Tasks & Alerts tab, you can check the progress and the execution results.

On the Resources tab, you can check the power status of LPARs.

Related tasks

- Activating LPARs on page 89
- Reactivating LPARs on page 91

Related references

- Prerequisites for power management on page 77

Reactivating LPARs

You can reactivate LPARs in certain cases, such as when the host on an LPAR stops unexpectedly.

Procedure

1. In the **Resources** tab, select **Chassis & Servers > All Logical Partitions > LPAR**.
2. From the list of LPARs, select the LPAR that you want to reactivate.
3. Click **Power Management** and then select **Reactivate**.
4. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
5. Click **Submit**.

Result

On the Tasks & Alerts tab, you can check the task progress and results.

On the Resources tab, you can check LPAR power status.

Related tasks

- Activating LPARs on page 89
- Deactivating LPARs on page 90

Related references

- Prerequisites for power management on page 77

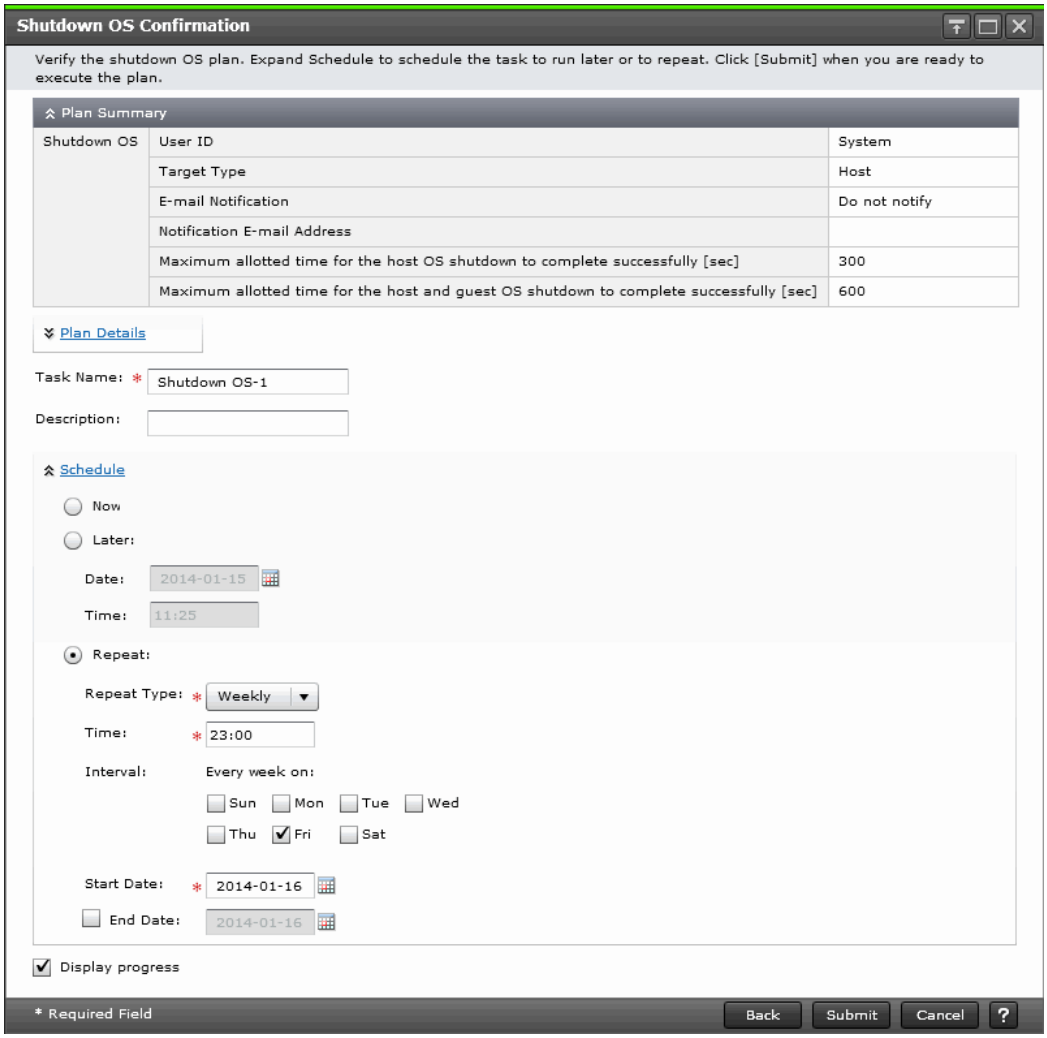
Example host power management schedules

You can set up power management schedules for different scenarios. In most cases, there are various combinations of schedule plans that produce the same result. The following provides simple examples of one power management scheduling method that you can use to achieve a specific result:

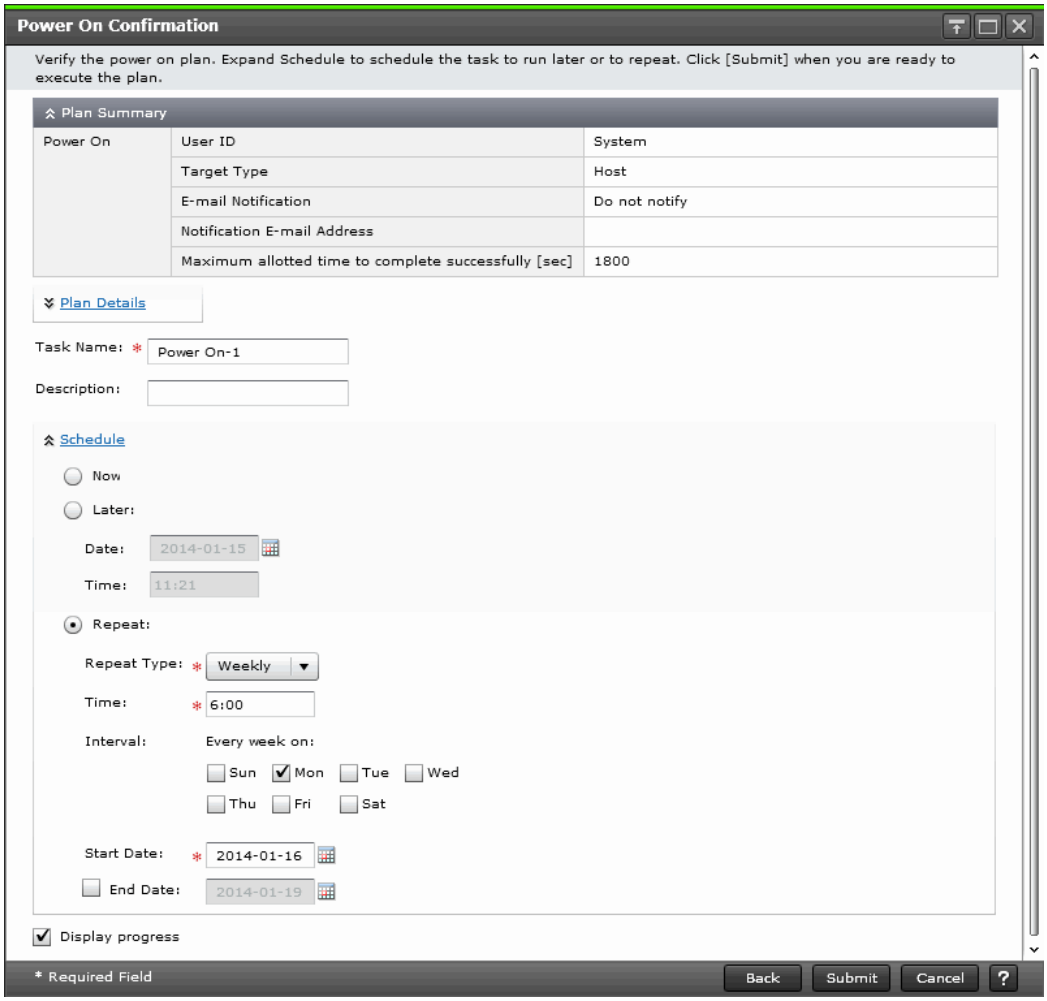
Example 1: Turning off power to a host every weekend

To turn off a host every weekend, create two tasks:

- A task to turn off power to the host at 23:00 every Friday



- A task to turn on the host at 6:00 every Monday



Example 2: Turning off power to a host on Thursday because the following Friday (05/04/2012) is a holiday

When the settings in Example 1 are used, you can turn off power to the host on Thursday night only for the week that includes May 4, 2012 by doing the following:

1. Change the Example 1 task schedule so that the end date is set to 05/03/2012.
2. Create a task to turn off the host at 23:00 on 05/03/2012.
3. Create another task to turn off the host at 23:00 every Friday, and set the task start date to 05/05/2012.

Example 3: Restarting a host on the first Saturday of every month

To restart a host on the first Saturday of every month, create the following task:

- A task to restart the host, scheduled to repeat to at 23:00 on the first Saturday of every month

Example 4: Not rebooting a host for this month only

When the settings in Example 3 are used, you can exclude a month from the regular monthly restart schedule:

- Change the task schedule so that the host is regularly restarted starting from next month

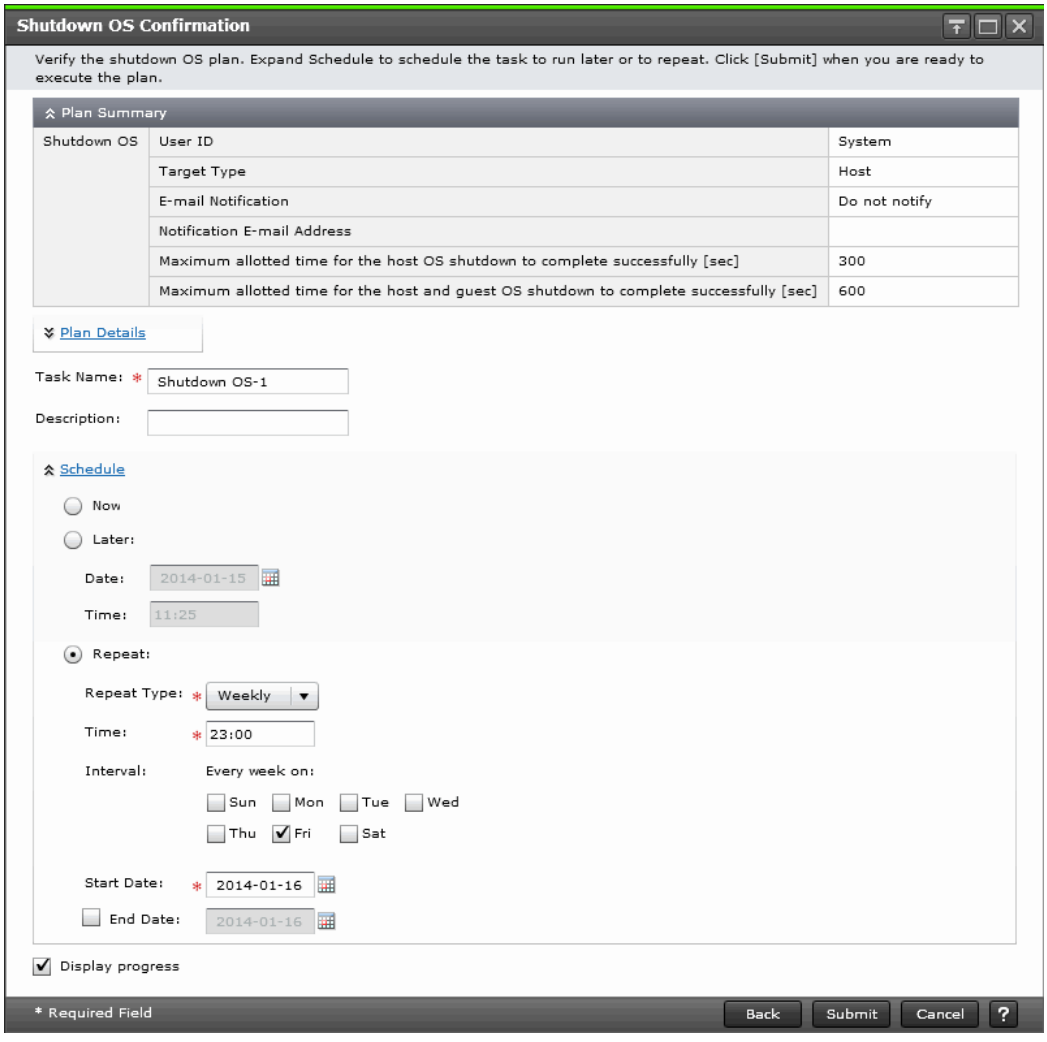
Example server power management schedules

In configurations that include servers with LPARs and servers without logical partitioning, the tasks you must create differ depending on the logical partitioning settings.

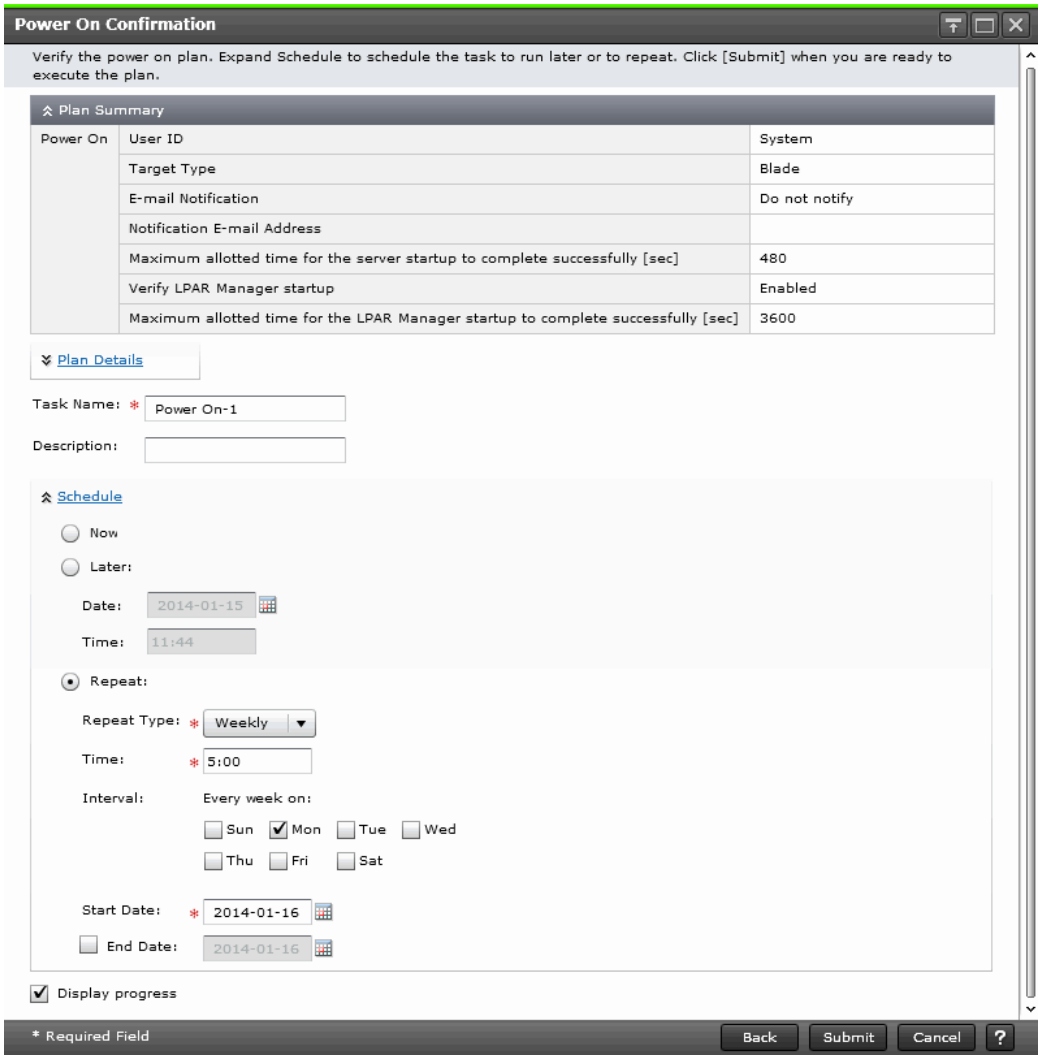
Example 1: Turning off power to a server every weekend

To shut down a server every weekend, create the following two tasks:

- A task that shuts down the hosts on the server that executes every Friday at 23:00.



- A task that turns on the power to the server that executes every Monday at 5:00.

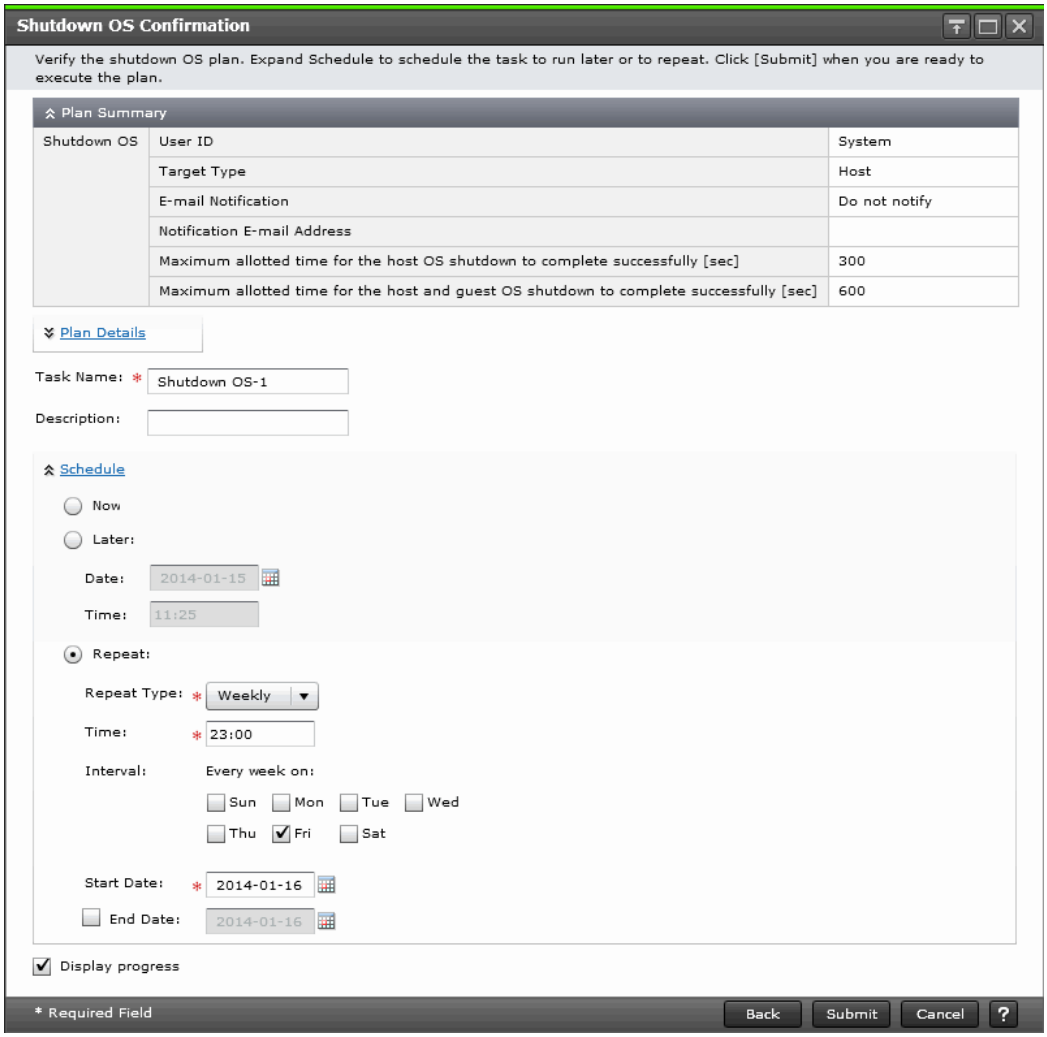


Example 2: Turning off power to a server every weekend, including servers on which LPARs are running

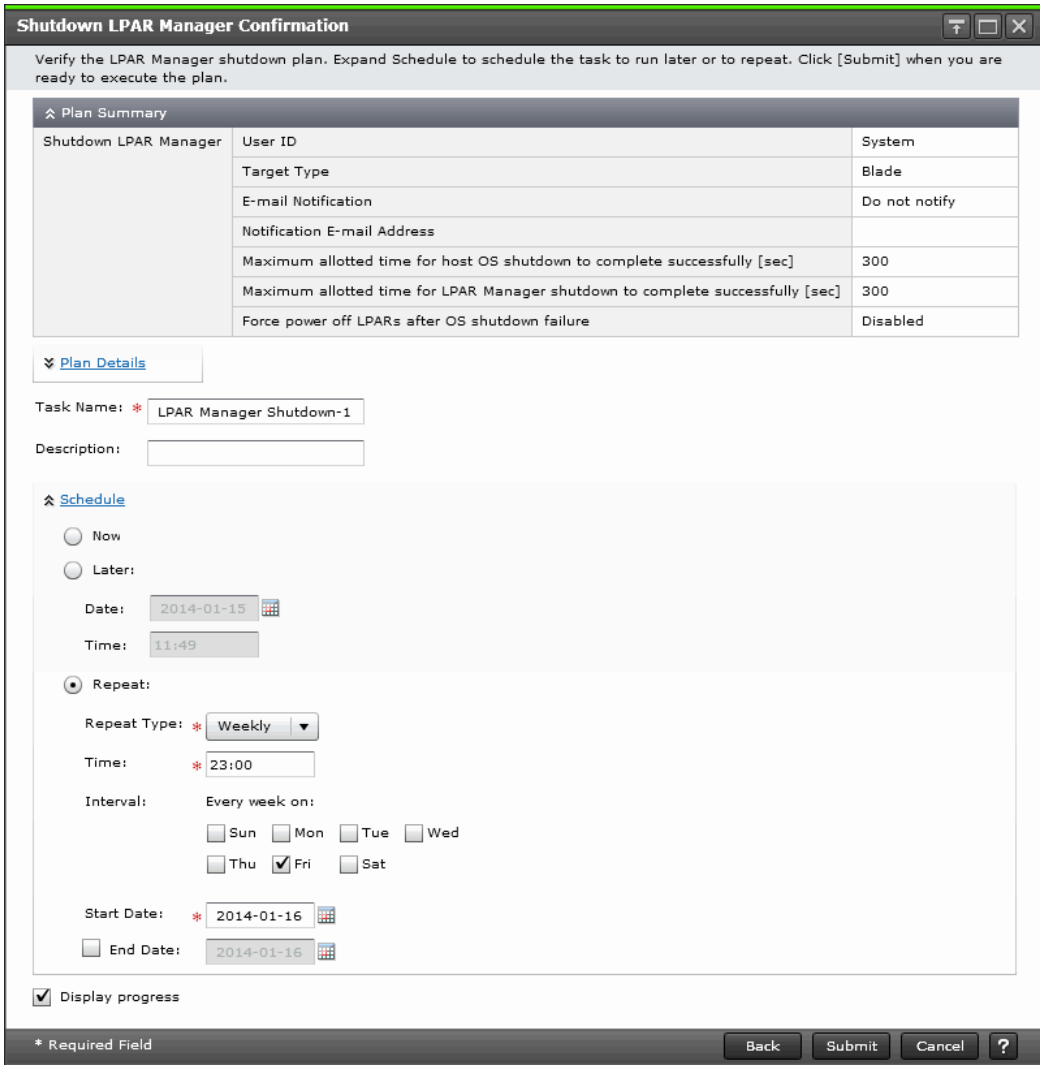
To shut down a server every weekend including servers on which LPARs are running, create the following four tasks:

- A task that shuts down the hosts on the servers on which LPARs are not running that runs every Friday at 23:00.

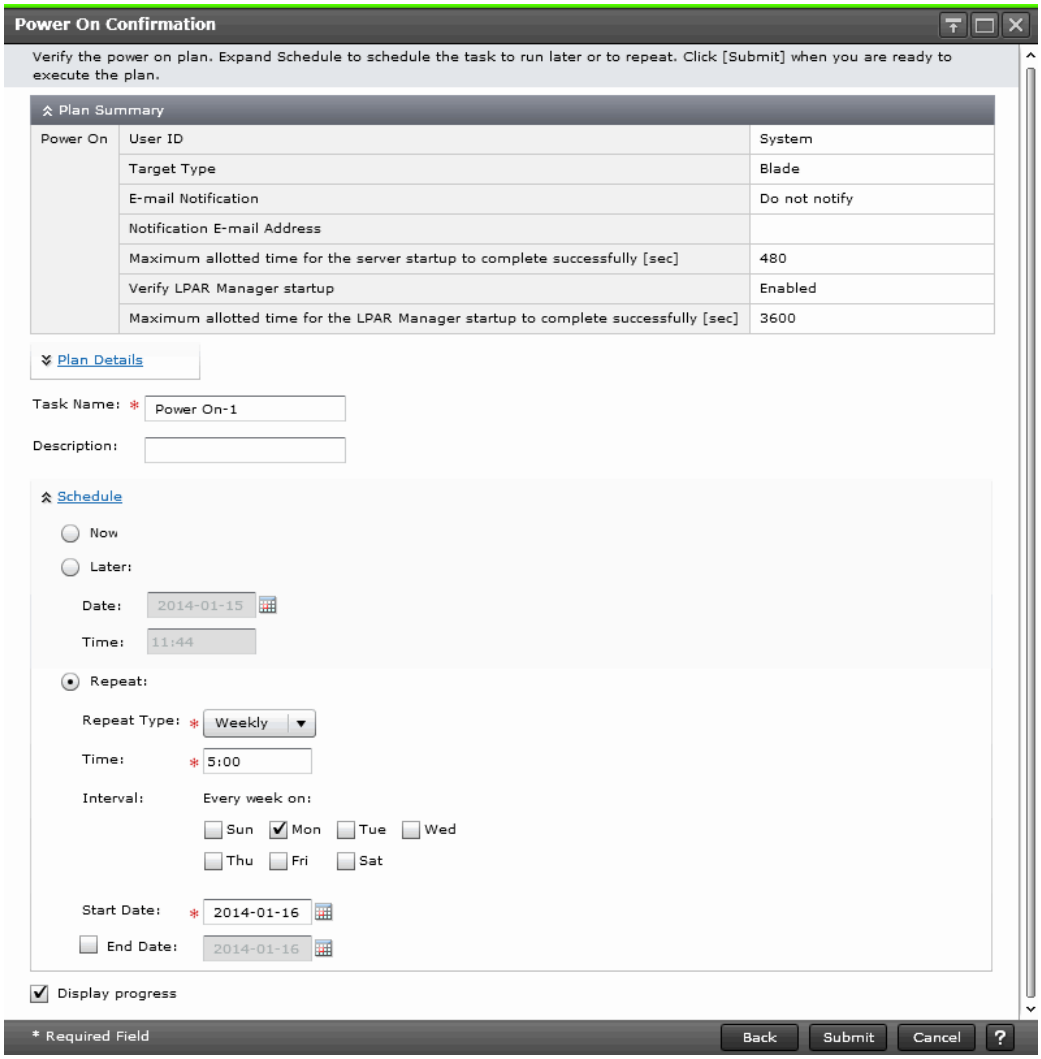
Note: When logical partitioning auto shutdown and LPAR activation order are configured on a server on which LPARs are running, you do not need to create tasks to start the LPAR Managers or the LPARs.



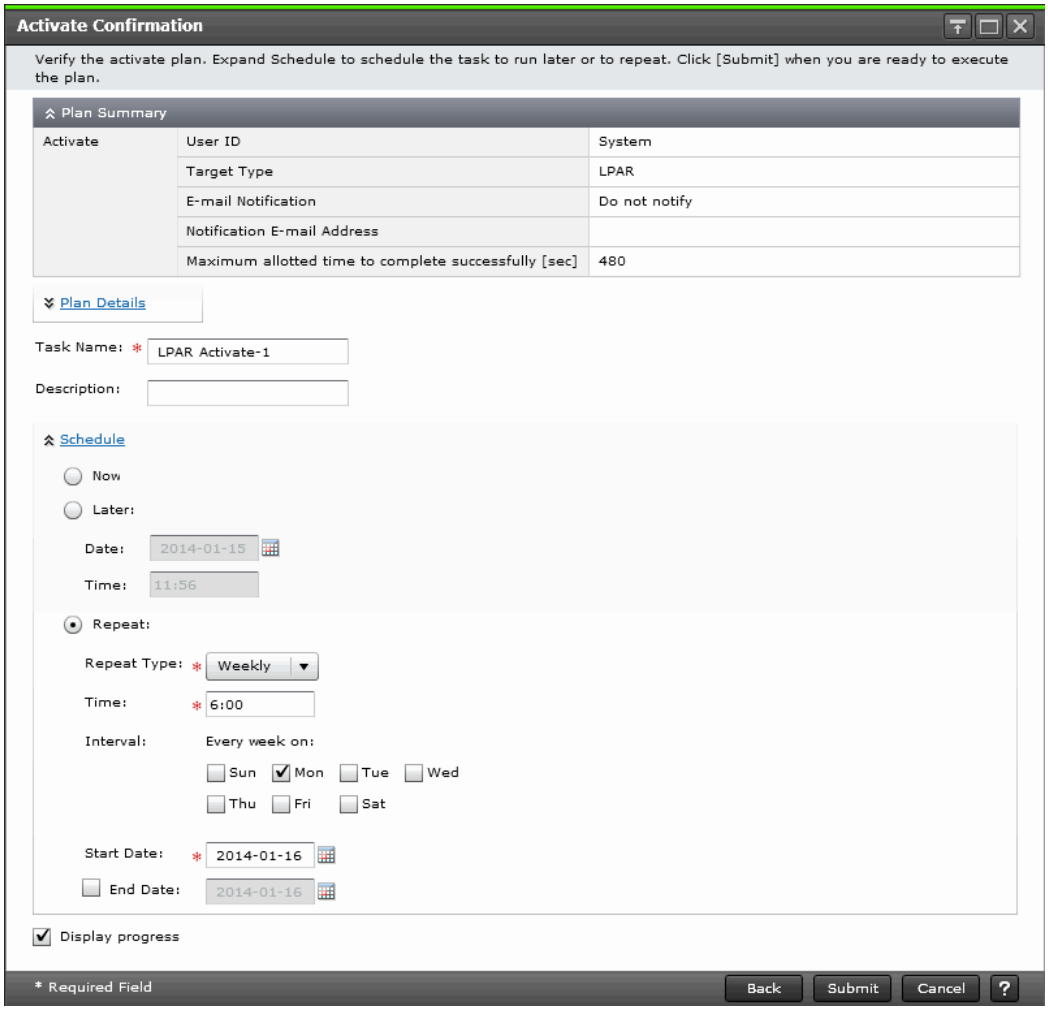
- A task that shuts down the LPAR Manager on which LPARs are running that runs every Friday at 23:00.



- A task that turns on the power of the server that runs every Monday at 5:00.



- A task that starts the LPARs that runs every Monday at 6:00.



Related tasks

- Changing the USB auto assignment setting on page 62
- Creating LPARs on page 64
- Changing LPAR settings on page 65

Related references

- Prerequisites for power management on page 77
- Example host power management schedules on page 91

Using location identifier lamps to locate hardware

You use location identifier (LID) lamps to locate servers and chassis in a network operations center (NOC). Use Hitachi Compute Systems Manager to operate LIDs on a particular server or chassis.

About location identifier lamps

Hitachi Compute Systems Manager allows you to identify the location of servers or chassis by turning the server or chassis lamp on or off from the Compute Systems Manager management client. These lamps are called location identifiers (LIDs).

LIDs in the following locations can be controlled:

- Chassis front-panel
- Individual modules in a chassis
- Blade server
- Rack-mounted server

You can operate the blade server LIDs by selecting a server from the Blade Server list, or by selecting a blade from the Chassis list. If a chassis consists of multiple blades, the LIDs of all blades that make up the chassis are turned on or off when the server is selected and managed from a list of blade servers.

Related tasks

- Using location identifier lamps to locate chassis on page 100
- Using location identifier lamps to locate modules on page 101
- Using location identifier lamps to locate servers on page 101

Using location identifier lamps to locate chassis

You can use location identifier (LID) lamps to locate a chassis in your network operations center. Turn the LID in the chassis front panel on or off to pinpoint that chassis.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Click **All Chassis**.
3. Expand the tree and select the chassis for which you want to turn on or turn off a LID.
4. From that list of chassis, select the chassis for which you want to turn on or turn off a LID.
5. Click **More Actions**, and then select **Turn on LID** or **Turn off LID**.

Result

The chassis LID is turned on or off.

You can verify the progress and execution results on the Resources tab.

Related concepts

- About location identifier lamps on page 100

Using location identifier lamps to locate modules

You can use location identifier (LID) lamps to locate a chassis module in your network operations center. Turn the LID in the chassis module on or off to pinpoint that chassis module.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Click **All Chassis**.
3. Expand the tree and select the link for a chassis name for which you want to turn on or turn off a LID.
4. From that list of chassis names, select the tab of the module for which you want to turn on or turn off a LID.
5. On the **Condition** tab, click **Turn on LID** or **Turn off LID**.

Result

The module LID is turned on or off.

You can verify the progress and execution results on the Resources tab.

Related concepts

- About location identifier lamps on page 100

Using location identifier lamps to locate servers

You can use location identifier (LID) lamps to locate a server in your network operations center. Turn the LID in the server on or off to pinpoint that server.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Click **All Servers**.
3. Expand the tree and select the type of server for which you want to turn on or turn off the LID.
4. From that list of servers, select the server for which you want to turn on or turn off the LID.
5. Click **More Actions**, and then select **Turn on LID** or **Turn off LID**.

Result

The server LID is turned on or off.

You can verify the progress and execution results on the Resources tab.

Related concepts

- About location identifier lamps on page 100

Configuring and using N+M cold standby

If you have purchased a license for N+M cold standby, you can create N+M cold standby groups and perform a failover test to check for errors to verify the N+M cold standby failover plan. You can add active and standby blades. You can check the status of the blades, manually fail over an active blade to a standby blade, fail back to the active blade from the standby blade, and return the blades to their original state.

About N+M cold standby

Hitachi Compute Systems Manager supports N+M cold standby. Cold standby means having a number of active blades (N) and multiple standby blades (M) in a power-off state that are ready to run in place of the active blade if an error occurs.

Before you perform this task, you must register an N+M cold standby license.

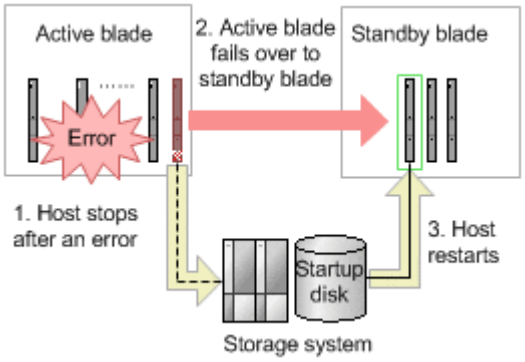
If you are using a Hitachi blade server, you can configure the blade for N+M cold standby. When you configure N+M cold standby in advance and an error occurs on the active blade, the active blade automatically fails over to a standby blade in the same group. After the failover, a host that was executing tasks on the active blade is restarted on the standby blade and resumes operations.

In addition, by checking the health status of the failover-destination blades, you can detect whether there are errors on the standby blade in advance. You can check the health status of the standby blades automatically or manually. If the health check determines that there is an error on the standby blade, the blade is not used as the target of an automatic failover.

N+M cold standby has the following advantages:

- Because only one standby blade is required for multiple active blades, system availability is improved at low cost.
- If you configure multiple standby blades, the failover feature enables operation to continue even if errors occur on multiple active blades.

The following figure shows an overview of N+M cold standby.



After resolving the failure error, you can fail back to the active blade from the standby blade and resume operations on the active blade. Alternatively, you can reassign the standby blade to an active blade and continue operations on the standby blade.

Related tasks

- Configuring N+M cold standby on page 104
- Adding a blade to an N+M cold standby group on page 105
- Removing a blade from an N+M cold standby group on page 106
- Manually checking standby blade health on page 107
- Performing an N+M cold standby test on page 107
- Checking the status of active and standby blades on page 108

Related references

- Prerequisite settings for N+M cold standby on page 103

Prerequisite settings for N+M cold standby

Configuring N+M cold standby requires the following prerequisites:

Licensing

Before you can configure and use N+M cold standby, you must register a valid license.

Blade hardware conditions

N+M cold standby requires that active and standby blades use the same hardware (the same model). In addition, active and standby blades both require specific configuration for using N+M cold standby. For further information, see the blade server documentation.

Blade status

- Standby blades must be managed, powered off, and cannot have experienced any failure errors.
- When failing back to active blades, the active blades must be managed, powered off, and all errors resolved.

After you verify the prerequisites, you must create an N+M cold standby group and run a failover test before you can use the N+M feature.

You can test all combinations of active blades and standby blades or a specific combination of an active blade and a standby blade.

For testing all combinations of active blades and standby blades, the time required for the test depends on the number of assigned standby blades. To reduce the test duration, you can select the All Servers Test check box to perform a minimal test of failover and failback among the active blades and the standby blades.

In addition, specify the allotted time from failover until failback as necessary. If the standby blades have a host or a host on a virtual machine, take into consideration the time required for the host services to start.

Related concepts

- About N+M cold standby on page 102

Related tasks

- Configuring N+M cold standby on page 104
- Adding a blade to an N+M cold standby group on page 105
- Manually checking standby blade health on page 107
- Performing an N+M cold standby test on page 107

Configuring N+M cold standby

You can create an N+M cold standby group (which requires an N+M cold standby license) to which you assign active and standby blades. After you create the group, you can run an N+M cold standby test (failover and failback) between active blades and standby blades.

Prerequisites

Before creating an N+M cold standby group, you must decide whether your environment requires you to modify the default values for automatic failover delay time and time out.

The delay time value enables you to reserve time for the system to generate log files before the failover occurs. In many cases, log files are important when determining the cause of a failure.

The timeout value enables you to specify the time to wait before reporting an error with the failover or failback task. When determining the timeout value, you must consider the time required for startup and shutdown of both systems.

Procedure

1. On the **Resources** tab, select **N+M Cold Standby Groups**.
2. Click **Create Group**.

3. Follow the instructions in the wizard to create an N+M cold standby group and assign active and standby blades.

   Optionally, register the standby blades for which you want to automatically check blade health and set the schedule.
4. In the summary window, verify the N+M cold standby settings.

   Optionally, open **Advanced Settings** and specify the email notification method, the delay time for automatic failover, and the timeout settings.
5. Click **Submit**.

   An N+M cold standby group is created.
6. Run an N+M cold standby failover test between the active blades and standby blades included in the group.
7. Follow the Wizard instructions to select the type of test to perform, and then specify the necessary settings.
8. Optionally, open **Advanced Settings** and specify settings such as the allotted time from failover until failback.
9. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule. The task can be run immediately or at a later time. The default setting is **Now**.
10. Click **Submit**.

    The N+M cold standby test starts.

Result

You can check the test progress and execution results on the Tasks & Alerts tab and display task details to check whether the N+M cold standby finished successfully.

You can also verify the N+M cold standby group on the Resources tab.

Related concepts

- About N+M cold standby on page 102

Related references

- Prerequisite settings for N+M cold standby on page 103
- Troubleshooting examples on page 218

Adding a blade to an N+M cold standby group

If you have an N+M cold standby license, you can add an active or standby blade to an existing N+M cold standby group.

Procedure

1. On the **Resources** tab, select **N+M Cold Standby Groups**.

2. From the list of N+M cold standby groups, click the **Group Name** link for the group to which you want to add the blade.
3. Click the **Active Blades** or **Standby Blades** tab.
4. Click **Edit Active Blades** or **Edit Standby Blades**.
5. In the **Active Blades** or **Standby Blades** dialog box, select the blade to add, and then click **Add**.

   For standby blades, optionally register the blades for which you want to automatically check blade health and set the schedule.
6. Click **OK**.
7. Run an N+M cold standby (failover and failback) test on the new active or standby blade.

Related tasks

- Removing a blade from an N+M cold standby group on page 106
- Performing an N+M cold standby test on page 107

Related references

- Prerequisite settings for N+M cold standby on page 103

Removing a blade from an N+M cold standby group

You can remove an unwanted active or standby blade from an existing N+M cold standby group.

Before removing a blade from an N+M cold standby group, ensure that the target blade is ready for removal and that the failover status in the Active Blades or Standby Blades tab is blank.

Procedure

1. On the **Resources** tab, select **N+M Cold Standby Groups**.
2. From the list of N+M cold standby groups, click the **Group Name** link for the group from which you want to remove the blade.
3. Select the **Active Blades** or **Standby Blades** tab.
4. Click **Edit Active Blades** or **Edit Standby Blades**.
5. In the **Active Blades** or **Standby Blades** dialog box, select the blade to remove, and then click **Remove**.
6. Follow the onscreen instructions and click **OK**.

Related concepts

- About N+M cold standby on page 102

Related tasks

- Adding a blade to an N+M cold standby group on page 105

Manually checking standby blade health

You can manually check the blade health of standby blades.

Before checking a standby blade heath, ensure that the blade is powered off.

Procedure

1. On the **Resources** tab, select **N+M Cold Standby Groups**.
2. From the list of N+M cold standby groups, click the **Group Name** link for the group that contains the standby blades for which you want to check the blade health.
3. Select the **Standby Blades** tab.
4. Select the standby blades to check from the list, and click **Check Blade Health**.
5. Click **Show Plan** and confirm that the information in the plan summary is correct.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run immediately or scheduled for later. The default setting is **Now**.
6. Click **Submit**.

Result

You can view the progress and execution results of the blade health check on the Tasks & Alerts tab. In addition, you can display task details to check whether the blade health check of a standby blade finished successfully.

You can check the result of the blade health check of standby blades on the Standby Blades tab.

Related concepts

- About N+M cold standby on page 102

Related tasks

- Configuring N+M cold standby on page 104
- Adding a blade to an N+M cold standby group on page 105
- Forcing a server to power off on page 87

Performing an N+M cold standby test

You can run an N+M cold standby failover test. If you add an active blade or standby blade to an existing N+M cold standby group, select the existing group and run an N+M cold standby (failover and failback) test.

Procedure

1. On the **Resources** tab, select **N+M Cold Standby Groups**.
2. From the list of N+M cold standby groups, click the **Group Name** link for the group you want to test.
3. On the **Failover Pairs** tab, select the group to test, and then click **Test N+M Cold Standby**.
4. Follow the onscreen instructions to select the type of test to run, and specify the necessary settings.
5. Optionally, open **Advanced Settings** to specify settings such as the allotted time from failover until failback.
6. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule. The task can be run immediately or at a later time. The default setting is **Now**.
7. Click **Submit**.

   The N+M cold standby test starts.

Result

Check the test progress and execution results on the Tasks & Alerts tab. You can display task details to check whether the N+M cold standby finished successfully.

Related references

- Prerequisite settings for N+M cold standby on page 103
- Troubleshooting examples on page 218

Checking the status of active and standby blades

If you have an N+M cold standby license, you can check the status of active and standby blades to verify that, for example, the blades are operating normally and the failover function is performing properly.

Procedure

1. On the **Resources** tab, select **N+M Cold Standby Groups**.
2. In the list of N+M cold standby groups, click the **Group Name** of the groups whose status you want to check.
3. On the **Failover Pairs** tab, check the failover status.
4. Click the **Active Blades** tab to check details for the active blades.
5. Click the **Standby Blades** tab to check details for the standby blades.

Result

If an error occurs on the active blade and the managed host fails over from an active blade to the standby blade, you can check the details of alerts

received from the active blade, the progress of the fail over process, and the results of the execution on the Tasks & Alerts tab.

Postrequisites

Note: When an alert occurs in the chassis or the blade server while Hitachi Compute Systems Manager is stopping, failover is not implemented even if Compute Systems Manager starts and receives an alert. In this case, you must implement manual failovers as necessary.

Related concepts

- About N+M cold standby on page 102

Related tasks

- Performing an N+M cold standby test on page 107

Related references

- Prerequisite settings for N+M cold standby on page 103
- Troubleshooting examples on page 218

Failing back to the active blade from the standby blade

You can fail back to the active blade from the standby blade (which requires an N+M cold standby license) when the errors on the active blade are resolved.

Procedure

1. On the **Resources** tab, select **N+M Cold Standby Groups**.
2. From the list of N+M cold standby groups, click the **Group Name** link for the group that contains the active blade to fail back.
3. Click the **Failover Pairs** tab.
4. Select the failover pair to fail back, and then click **Fail Back to Active Blade**.
5. Optionally, open **Advanced Settings** and specify settings such as the active blade power supply status and the email notification settings.
6. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule. The task can be run immediately or at a later time. The default setting is **Now**.
7. Click **Submit**.

   The failback process starts.

Result

Verify the failback results on the Failover Pairs tab.

Related tasks

- Checking the status of active and standby blades on page 108

Related references

- Prerequisite settings for N+M cold standby on page 103

Reassigning a standby blade to an active blade

You can reassign a standby blade to become an active blade if you have an N +M cold standby license. After Hitachi Compute Systems Manager fails over a blade to a standby blade, you can choose to continue operation on the standby blade by reassigning the blade as an active blade. When you reassign the blade as active, the blade is automatically removed from the N +M cold standby group.

Procedure

1. On the **Resources** tab, select **N+M Cold Standby Groups**.
2. From the list of N+M cold standby groups, click the **Group Name** link for the group that contains the standby blade that you want to reassign.
3. Click the **Failover Pairs** tab.
4. Select the set for which you want to reassign a standby blade as an active blade, and then click **Reassign Standby Blade**.
5. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule. The task can be run immediately or at a later time. The default setting is **Now**.
6. Click **Submit**.

   The reassignment process starts.

Result

Verify the reassignment results on the Failover Pairs tab.

Related concepts

- About N+M cold standby on page 102

Related references

- Prerequisite settings for N+M cold standby on page 103

Manually failing over an active blade to a standby blade

You can manually fail over an active blade to a standby blade (which requires an N+M cold standby license) for migration of a blade server environment or for a routine test.

Procedure

1. On the **Resources** tab, select **N+M Cold Standby Groups**.
2. From the list of N+M cold standby groups, click the **Group Name** link for the group that contains the active blade that you want to manually fail over to a standby blade.
3. On the **Active Blades** tab, select the active blade that you want to fail over to the standby blade, and click **Fail Over To Standby Blade**.
4. From the list of standby blades, select the standby blade to which you want to fail over.
5. Optionally, open **Advanced Settings** and specify settings such as the standby blade power supply status and the email notification setting.
6. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule. The task can be run immediately or at a later time. The default setting is **Now**.
7. Click **Submit**.

   The manual failover process starts.

Result

Verify the manual failover results on the Failover Pairs tab.

Related concepts

- About N+M cold standby on page 102

Related references

- Prerequisite settings for N+M cold standby on page 103

Returning blades to the original status after an unsuccessful failover

If a failover process fails, you can check the cause and take action. You must restore the failover status of the active and standby blades (which requires an N+M cold standby license) to return them to their original statuses.

Procedure

1. On the **Resources** tab, select **N+M Cold Standby Groups**.
2. In the list of N+M cold standby groups, click the **Group Name** for the group that contains the active and standby blades for which the failover did not succeed.
3. On the **Failover Pairs** tab, select the line in which the failover status is **Failed**.
4. Click **Restore Assignment**.
5. Click **Show Plan**, and then verify the active and standby blade pair listed in the summary.

6. Click **Submit**.

Result

The selected line is no longer displayed on the Failover Pairs tab, and the active and standby blades become available for failover again.

Related concepts

- About N+M cold standby on page 102

Related references

- Prerequisite settings for N+M cold standby on page 103
- Troubleshooting examples on page 218

Migrating LPARs

About migrating LPARs

In Hitachi Compute Systems Manager, you can move an LPAR that was created on a blade server to a different blade server. This function is called *LPAR migration*.

By migrating LPARs, you can increase the availability of blade servers, which enables you to use resources more effectively.

You can migrate LPARs using the following methods:

- LPAR cold migration
  Using this method, you migrate an inactive LPAR.
- LPAR migration
  Using this method, you migrate an active LPAR.
  Migrating active LPARs takes more time than migrating inactive LPARs with cold migration.

When migrating LPARs, we recommend that you run an LPAR cold migration task as a test beforehand, and then run LPAR migration.

Related tasks

- Migrating an inactive LPAR on page 114
- Migrating an active LPAR on page 115
- Enabling automatic registration for migration WWPNs on page 114
- Recovering from migration failure for LPARs on page 116
- Changing the allocation time for LPAR migration on page 116

Related references

- Prerequisites for migrating LPARs on page 113

Prerequisites for migrating LPARs

Before migrating LPARs, you must verify the prerequisites on all blade servers specified as migration sources and destinations for LPARs.

You can view all prerequisites in the following windows when creating a migration task in either mode:

- Cold Migrate Plan window
- Migrate Plan window

For details on LPAR migration prerequisites, see the blade server manual.

Before migrating LPARs, you must do the following:

- Ensure the LPAR Manager is running on all blades specified as LPAR migration sources or LPAR destinations.
- Back up the LPAR Manager configuration information on the blade server specified as the migration source and destination for LPARs.
  To prepare for a failure, back up the LPAR Manager configuration information before migrating the LPAR. You must use Element Manager to backup or restore the LPAR Manager configuration information.
- Register the migration source WWPN of the FC that is temporarily used in the migration source LPAR. Register the WWPN in the same host group as the WWPN of the FC used for standard operations by choosing one of the following options:
  - Enable automatic registration for migration WWPNs.
    If you enable automatic registration for migration WWPNs and then run the LPAR migration task, Compute Systems Manager connects with Hitachi Device Manager and WWPNs are registered automatically.
  - Use Hitachi Device Manager to manually register migration WWPNs.
    Use Hitachi Device Manager to add all migration WWPNs in the migration source to the storage system host group in which the corresponding WWPNs are registered.

  For details about using Hitachi Device Manager, see the *Hitachi Command Suite User Guide*.

Related concepts

- About migrating LPARs on page 112

Related tasks

- Migrating an inactive LPAR on page 114
- Migrating an active LPAR on page 115
- Enabling automatic registration for migration WWPNs on page 114

Enabling automatic registration for migration WWPNs

You can automatically register migration WWPNs when migrating an LPAR.

Prerequisites

Before you begin configuring automatic registration of migration WWPNs, set up a connection with Hitachi Device Manager. Ensure that the user name specified for the connection has permission to change the host group to which WWPNs for FC are registered.

Procedure

1. On the **Administration** tab, select **Logical Partitioning > Automatic Registration for Migration WWPNs**.
2. Click **Automatic Registration for Migration WWPNs Setting**.
3. Select the **Enable Automatic Registration for Migration WWPNs** check box.

Related concepts

- About migrating LPARs on page 112

Related tasks

- Migrating an active LPAR on page 115
- Setting up a connection with Hitachi Device Manager on page 43

Related references

- Prerequisites for migrating LPARs on page 113

Migrating an inactive LPAR

You can migrate an inactive LPAR. Before beginning, make sure you have deactivated the LPAR on the migration source.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Logical Partitions > LPAR**.
2. From the list of LPARs, select the LPAR that you want to migrate.
3. Click **LPAR Management** and select **Cold Migrate LPAR**.
4. Read the on-screen instructions and set the information of the LPAR that you are migrating.
5. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule. The task can be run immediately or at a later time. The default setting is **Now**.

6. Click **Submit**.

Result

You can view the progress and execution result of the task on the Tasks & Alerts tab.

You can view the migration status under Migration Status in the list of LPARs.

Related concepts

- About migrating LPARs on page 112

Related tasks

- Migrating an active LPAR on page 115
- Recovering from migration failure for LPARs on page 116
- Deactivating LPARs on page 90

Related references

- Prerequisites for migrating LPARs on page 113

Migrating an active LPAR

You can migrate an active LPAR. Before beginning, ensure that the LPAR is activated on the migration source.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Logical Partitions > LPAR**.
2. From the list of LPARs, select the LPAR that you want to migrate.
3. Click **LPAR Management** and select **Migrate LPAR**.
4. Read the on-screen instructions and set the information for the LPAR you are migrating and the migration network.
5. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule. The task can be run immediately or at a later time. The default setting is **Now**.
6. Click **Submit**.

Result

You can view the progress and execution result of the task on the Tasks & Alerts tab.

You can view the migration status under Migration Status in the list of LPARs.

Related concepts

- About migrating LPARs on page 112

Related tasks

- Enabling automatic registration for migration WWPNs on page 114
- Migrating an inactive LPAR on page 114
- Recovering from migration failure for LPARs on page 116
- Changing the allocation time for LPAR migration on page 116
- Activating LPARs on page 89

Related references

- Prerequisites for migrating LPARs on page 113

Recovering from migration failure for LPARs

You can recover from failure that occur when you are migrating LPARs.

You can view the migration status under Migration Status in the list of LPARs.

- If the migration status is Recovery Failed, you can perform recovery in Hitachi Compute Systems Manager.
- If the migration status is Non-recoverable Failure, you cannot perform recovery in Hitachi Compute Systems Manager. You need to use Element Manager to restore the LPAR Manager configuration information that you backed up before starting the migration.

Before beginning, make sure that LPAR manager is running.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Logical Partitions > LPAR**.
2. From the list of LPARs, select the LPAR that you want to recover.
3. Click **LPAR Management** and select **Recover from Failed Migration**.
4. Click **OK**.

Result

You can view the progress and execution result of the task on the Tasks & Alerts tab.

Related concepts

- About migrating LPARs on page 112

Related tasks

- Migrating an inactive LPAR on page 114
- Migrating an active LPAR on page 115

Changing the allocation time for LPAR migration

You can change the allotted time for migration of an active LPAR.

When setting the allotted time for LPAR migration, consider the time that it will take to complete the LPAR migration.

Procedure

1. On the **Administration** tab, select **Logical Partitioning > Settings**.
2. Click **Edit Settings**.
3. Specify the maximum allotted time for LPAR migration in seconds.
4. Click **OK**.

Related concepts

- About migrating LPARs on page 112

Related tasks

- Migrating an active LPAR on page 115

Capping resource power consumption

You can use Hitachi Compute Systems Manager to control (cap) the power consumption of Hitachi chassis and servers.

About power capping

Hitachi Compute Systems Manager enables you to control power consumption of managed chassis and servers so that the power consumption does not exceed the configured allowable range.

Before you can use power capping, you must have a Power Monitoring license for chassis or rack-mounted servers.

Power capping allows resources to use less power. Note, however, that using power capping might increase the CPU usage of the hosts running on the server as well as the applications running on the hosts. Therefore, before using power capping, ensure that the host performance is flexible enough to manage sudden spikes in CPU usage.

Related tasks

- Enabling chassis power capping on page 118
- Disabling chassis power capping on page 119
- Analyzing host performance data on page 179
- Enabling rack-mounted server power capping on page 120

Related references

- Example power capping schedules on page 121

Enabling chassis power capping

You can enable chassis power capping (which requires a Power Monitoring license) to control the power consumption of a chassis. In addition, you can exclude specific blade servers mounted on that chassis from power capping.

If you use power capping, the chassis voltage and the blade server CPU frequency might decrease, and the applications running on the hosts on the server might be affected. Therefore, before enabling power capping, ensure that the performance of the hosts is flexible.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Chassis > Chassis**.

   The list of managed chassis opens.
2. Click **View Chassis Power Data**.
3. Select the chassis for which you want to enable power capping.
4. Click **Start Power Capping**.
5. Set the upper limit for power consumption.
6. If you want to exclude specific blade servers on the chassis from power capping, open **Target Blades on Chassis** and clear the check box for the blade server for which you do not want to enable power capping.

   Note: You can disable all check boxes by clearing the top check box, or you can clear individual check boxes as needed.
7. Optionally, open **Advanced Settings** and specify email notification settings.
8. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
9. Click **Submit**.

   You can verify the progress and execution results on the **Tasks & Alerts** tab.

Postrequisites

Note: Some chassis types do not apply power capping settings until after restarting the blade servers. To check whether the power capping settings have been applied to the blade servers:

1. On the Resources tab, select Chassis & Servers > All Servers > Blade.

2. Click View Blade Power Data.

You can verify that the system is controlling chassis power consumption correctly by accessing the list of chassis on the Resources tab and selecting View Chassis Power Data.

You can confirm that performance is not affected for a host running on a chassis that is using power capping by accessing the list of hosts on the Resources tab and selecting View Performance Data.

Related concepts

- About power capping on page 117

Related tasks

- Disabling chassis power capping on page 119

Disabling chassis power capping

You can stop controlling the chassis power consumption by disabling power capping. This requires a chassis Power Monitoring license.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Chassis > Chassis**.

   The list of managed chassis opens.
2. Click **View Chassis Power Data**.
3. Select the chassis for which you want to disable power capping.
4. Click **Stop Power Capping**.
5. Optionally, open **Advanced Settings** and specify email notification settings.
6. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
7. Click **Submit**.

   The chassis power capping is disabled.

Result

You can verify the progress and execution results on the Tasks & Alerts tab.

Related concepts

- About power capping on page 117

Related tasks

- Enabling chassis power capping on page 118

Enabling rack-mounted server power capping

You can enable rack-mounted server power capping (which requires a Power Monitoring license) to control the power consumption of a rack-mounted server.

If you use power capping, the server voltage and CPU frequency might decrease, and the applications running on the hosts on the server might be affected. Therefore, before enabling power capping, ensure that the performance of the hosts is flexible.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers > Rack-mounted**.

   The managed rack-mounted server list opens.
2. Click **View Rack-mounted Power Data**.
3. Select the server for which you want to enable power capping.
4. Click **Start Power Capping**.
5. Set the upper limit for power consumption.
6. Optionally, open **Advanced Settings** and specify email notification settings.
7. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
8. Click **Submit**.

   You can verify the progress and execution results on the **Tasks & Alerts** tab.

Postrequisites

You can check the status of whether power consumption is being properly controlled on the rack-mounted server by selecting View Rack-mounted Power Data from a list of rack-mounted servers in the Resources tab.

You can confirm that the performance of the host running on the rack-mounted server for which power capping has been enabled is not affected by selecting View Performance Data from the list of hosts on the Resources tab.

Related tasks

- Disabling rack-mounted server power capping on page 121

Disabling rack-mounted server power capping

You can stop controlling the server power consumption by disabling power capping. This requires a Power Monitoring license.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers > Rack-mounted**.

   The managed rack-mounted servers list opens.
2. Click **View Rack-mounted Power Data**.
3. Select the server for which you want to disable power capping.
4. Click **Stop Power Capping**.
5. Optionally, open **Advanced Settings** and then specify email notification settings.
6. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
7. Click **Submit**.

   Power capping is disabled on the selected servers.

Result

You can verify the progress and execution results on the Tasks & Alerts tab.

Related tasks

- Enabling rack-mounted server power capping on page 120

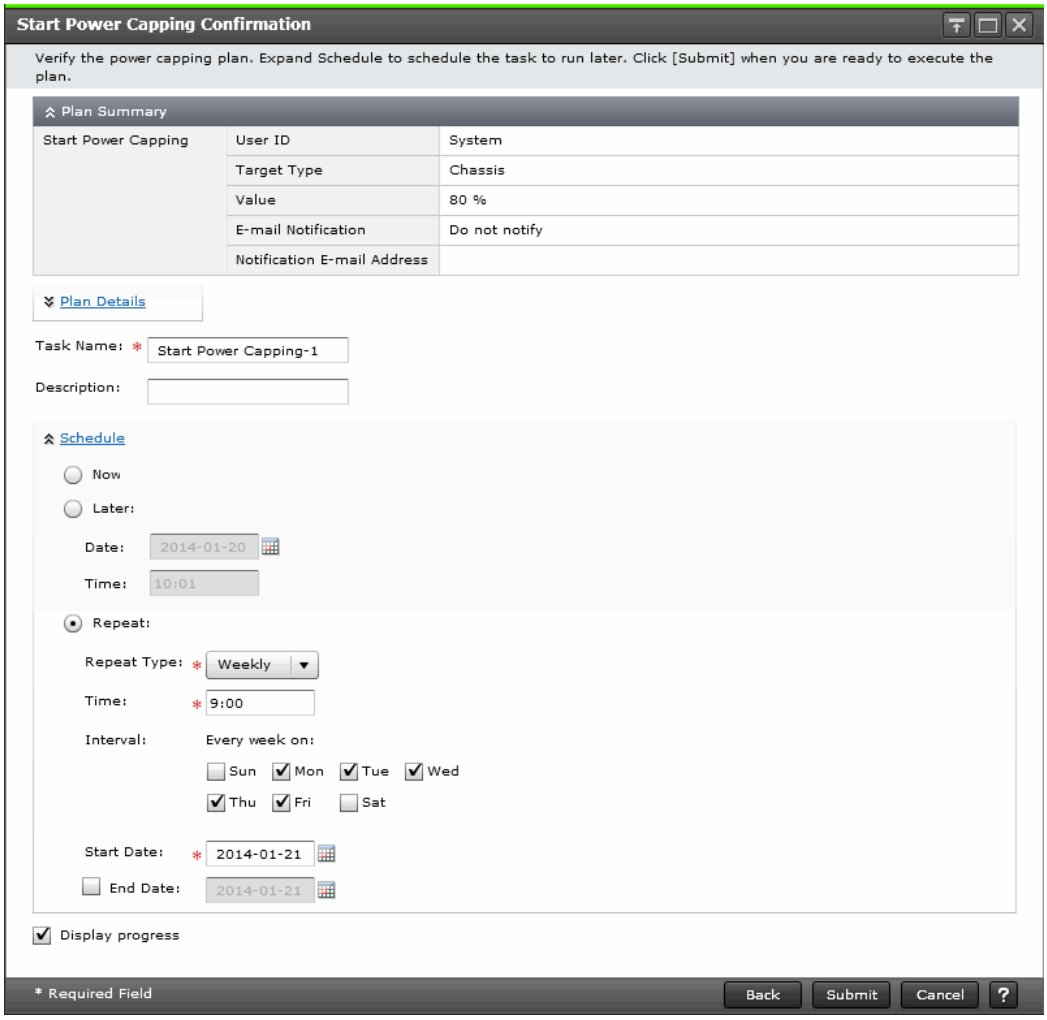
Example power capping schedules

This section provides examples of selecting and scheduling power management options.

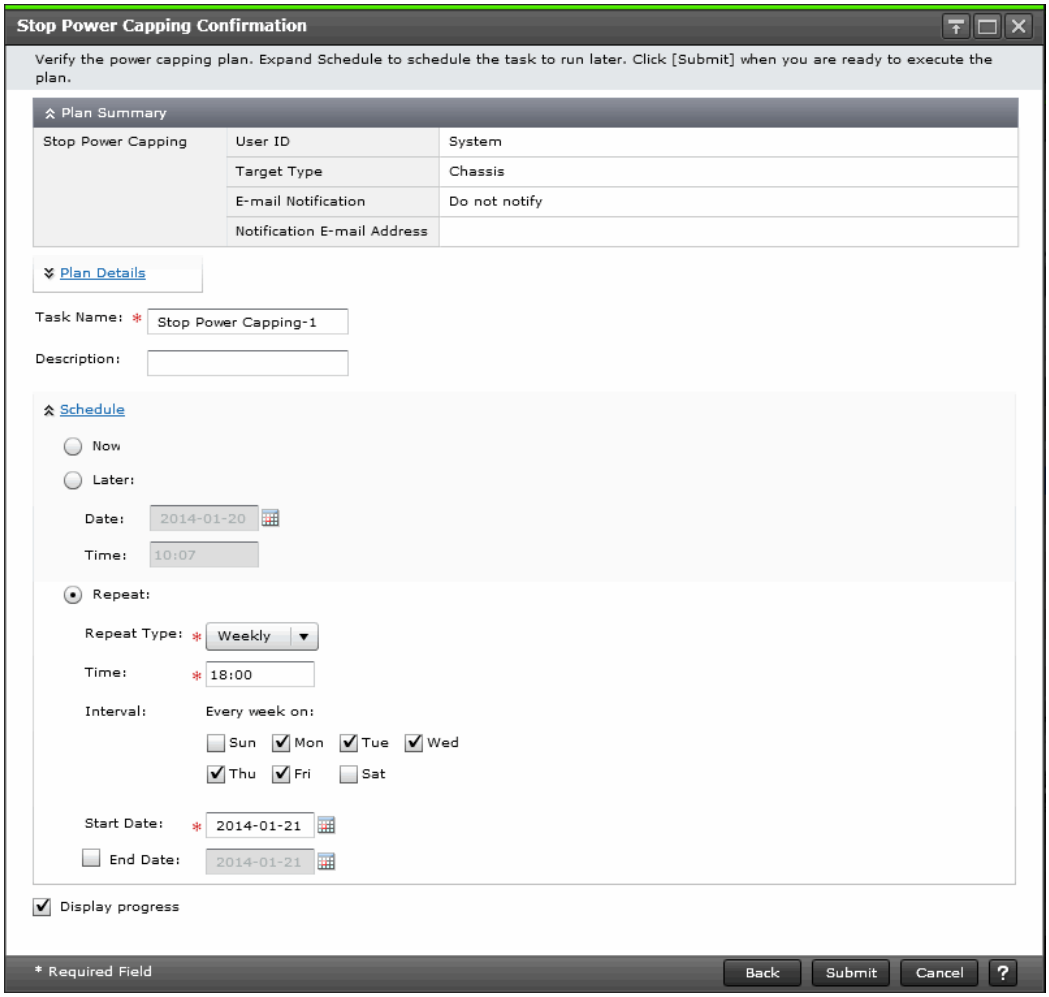
You must have a Power Monitoring license to use this function.

To enable power capping for ten chassis during business hours on weekdays, create two tasks:

- A task to select 10 chassis and enable power capping for them at 9:00 a.m. from Monday to Friday.



- A task to disable power capping at 18:00 for 10 chassis for which power capping is enabled from Monday to Friday.



Related concepts

- About power capping on page 117

Related tasks

- Enabling chassis power capping on page 118
- Disabling chassis power capping on page 119

Managing tasks

This module describes tasks that can you create and manage.

About tasks and task management

When you perform any operation on user resources, Hitachi Compute Systems Manager registers the operation as a task.

If the management server stops before a task starts, the task runs the next time that the management server starts. However, if the management server starts after the time limit elapses, the task will not be executed. In addition, if the management server stops while a task is running, the task fails. Re-register the failed task as necessary.

You can check the progress of current tasks or the result of all previously run tasks on the Tasks & Alerts tab.

On the Tasks & Alerts tab, you can do the following:

- Change the schedule for a task.
- Cancel a task that is running.
- Move a task that ended with an error to the history.
- Delete a task that is no longer needed.

Note: If the total number of registered tasks and tasks moved to the history exceeds 1,000, the system periodically deletes tasks, starting with those having the earliest end date, until the total number decreases to 700. Only tasks moved to the history are deleted.

Related tasks

- Viewing task status on page 124
- Rescheduling tasks on page 125
- Canceling a running task on page 125
- Moving failed tasks to the History tab on page 126
- Deleting tasks on page 126

Viewing task status

Viewing a list of tasks allows you to verify the status of individual tasks.

Procedure

1. On the **Tasks & Alerts** tab, select **All Tasks**.
2. On the **Tasks** tab, verify the task status.

   You can also view the status of a task (**Completed** or **Canceled**) on the **History** tab.

   Tip: All registered tasks, including those registered by other users, are listed in the task list.

3. To display task details and a task summary, click the task name link.

Related concepts

- About tasks and task management on page 123

Related tasks

- Rescheduling tasks on page 125
- Canceling a running task on page 125
- Moving failed tasks to the History tab on page 126
- Deleting tasks on page 126

Rescheduling tasks

You can reschedule any task that is in Waiting status. For example, you may want to skip a scheduled task that runs on a regular schedule.

Procedure

1. On the **Tasks & Alerts** tab, select **All Tasks**.
2. On the **Tasks** tab, select the task that you want to reschedule and click **Reschedule Task**.
3. Change the schedule and click **OK**.

   The task is rescheduled.

Result

You can confirm that the task is rescheduled by viewing the list of tasks on the Tasks & Alerts tab.

Related concepts

- About tasks and task management on page 123

Related tasks

- Canceling a running task on page 125
- Moving failed tasks to the History tab on page 126
- Deleting tasks on page 126

Canceling a running task

You can cancel any tasks that are currently In Progress. For example, you can cancel a task that is taking too long to find a host.

Procedure

1. On the **Tasks & Alerts** tab, select **All Tasks**.
2. On the **Tasks** tab, select the tasks you want to cancel and click **Cancel Tasks**.
3. Confirm that the list of tasks about to be canceled is correct.
4. Click **OK**.

   The tasks are canceled.

Result

You can confirm the task status by viewing the History tab.

Related concepts

- About tasks and task management on page 123

Related tasks

- Rescheduling tasks on page 125
- Moving failed tasks to the History tab on page 126
- Deleting tasks on page 126

Moving failed tasks to the History tab

You can move tasks that have ended with an error to the History tab.

Note: Only tasks that have failed can be manually moved to the History tab.

Procedure

1. On the **Tasks & Alerts** tab, select **All Tasks**.
2. On the **Tasks** tab, select the tasks to move and click **Move to History**.
3. Verify that list of tasks being moved is correct.
4. Click **OK**.

   The selected tasks are moved to the **History** tab.

Related concepts

- About tasks and task management on page 123

Related tasks

- Rescheduling tasks on page 125
- Canceling a running task on page 125
- Deleting tasks on page 126

Deleting tasks

You can delete tasks that are no longer needed. Deleting a task removes it from the task list on the Tasks or History tab. You cannot delete tasks that are in an In Progress state.

Procedure

1. On the **Tasks & Alerts** tab, select **All Tasks**.
2. On the **Tasks** tab or the **History** tab, select the tasks to delete and click **Delete Tasks**.
3. Verify that list of tasks being deleted is correct.
4. Click **OK**.

The selected tasks are deleted.

Related concepts

- About tasks and task management on page 123

Related tasks

- Rescheduling tasks on page 125
- Canceling a running task on page 125
- Moving failed tasks to the History tab on page 126

Using related Hitachi management software

You can access and use Element Manager and remote KVM from within Hitachi Compute Systems Manager.

About using related software for management servers

You can access related software from the management client to operate managed servers and view detailed information about them.

Hitachi Compute Systems Manager can access the following software that comes with the Hitachi server:

- **Element Manager:** View detailed hardware information about chassis and servers, and perform remote operations.
- **Web Remote KVM:** Remotely operate a host or server.

Related tasks

- Using Element Manager to connect to a managed resource on page 127
- Using web remote KVM to connect to managed resources on page 128

Using Element Manager to connect to a managed resource

You can access Element Manager from a management client to remotely operate and view more detailed information about Hitachi managed resources.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Expand the tree and select the managed resource.
3. From the **More Actions** menu, select **Launch Element Manager**.

Result

The Element Manager login window opens.

Related concepts

- About using related software for management servers on page 127

Using web remote KVM to connect to managed resources

You can access KVM from Hitachi Compute Systems Manager to remotely operate and view more detailed information about Compute Systems Manager managed resources.

Note: Before you can view an LPAR or a host on an LPAR, you must first assign a USB to the LPAR.

Procedure

1. On the **Resources** tab, select **Hosts** or **Chassis & Servers**.
2. Expand the tree and select a managed resource.
3. From the **More Actions** menu, select **Access KVM**.

Result

The web remote KVM login window opens.

Related concepts

- About using related software for management servers on page 127

About LPAR USB assignments

To use web remote KVM to perform operations on an LPAR or on a host on the LPAR, or to use USB on an LPAR, you must first assign a USB to the LPAR.

When you create an LPAR, a USB is reserved by default. The USB that is reserved on an LPAR can be changed either when you create the LPAR or later in the LPAR settings. Regardless of whether one USB is reserved by multiple LPARs, you can assign that USB to only one LPAR.

If a USB is assigned to an unintended LPAR, unassign the USB and assign it to the intended LPAR.

Assigning a USB to an LPAR

You can assign a USB to an LPAR manually or you can enable USB auto assignment so that a USB is automatically assigned to the LPAR when the LPAR is activated.

Prerequisites

Before assigning a USB to an LPAR you must:

- Reserve the USB.
- Activate the LPAR.
- Verify that LPAR Manager is running.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Logical Partitions > LPAR**.
2. In the list of LPARs, click the **LPAR Name** link.
3. On the **USB** tab, select the USB you want to assign and click **Assign USB Device**.
4. Click **OK**.

Result

You can view the progress and result of the USB assignment on the Tasks & Alerts tab.

Unassigning a USB from an LPAR

You can unassign a USB from an LPAR assignment.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Logical Partitions > LPAR**.
2. In the list of LPARs, click the **LPAR Name** link.
3. On the **USB** tab, select the USB you want to unassign and click **Unassign USB Device**.
4. Click **OK**.

Result

You can view the progress and result of the USB assignment on the Tasks & Alerts tab.

Setting up Virtual Machine Manager connections for managing virtual resources

This section contains information about setting up connections so that you can launch the VMM interface to manage your virtual resources.

Setting up a connection to a VMM

You can set up connections to a VMM to enable remote operation of virtual resources.

Procedure

1. On the **Administration** tab, select **Virtualization Settings > VMM Web Client Connections**.
2. Click **Create Connection Setting** so that you can create a connection that links and launches the VMM interface.
3. Enter the name and launch path of the VMM Web Client Connection.

4. Select the hypervisor from the **Available Hypervisors** list.
5. Click **Test Connection**.
6. After you verify the connection, click **OK**.

Related tasks

- Operating virtual resources using a VMM on page 130

Operating virtual resources using a VMM

You set up access to a VMM by creating a VMM Web client connection. After you create the connection, you can access your VMM interface from Hitachi Compute Systems Manager so that you can complete tasks and verify detailed information for your virtual resources.

Procedure

1. On the **Resources** tab, select **Virtualization**.
2. Click **All Hypervisors** and then select the hypervisor type.
3. Select the hypervisor that is running the VMM that you want to access, and then select **More Actions > Launch VMM**.
   The VMM window is displayed.

Result

To view the results of any actions completed using the VMM interface, use Compute Systems Manager to refresh the hypervisor information.

Related tasks

- Setting up a connection to a VMM on page 129

Configuring and using Deployment Manager

You can use Deployment Manager to back up the disk data of a managed resource, manage backup image files, restore a backup image to a managed resource, and deploy a new resource by using an existing disk image (snapshot).

About Deployment Manager

Using Deployment Manager, you can build multiple managed resources that have the same environment. You can also restore the disk data of a managed resource if disk failure or damage occurs.

You must have a Deployment Manager license to use this functionality.

Note: To use Deployment Manager, the management server must be running Windows.

Deployment Manager supports the following types of resources:

- Hitachi servers
- Virtual machines on a hypervisor
- LPARs

You can use Deployment Manager to do the following:

- Back up the data on a managed resource as an image file and store it on the management server
- Restore an image file to a managed resource
- Manage image files
- Duplicate the environment of a particular managed resource to a different managed resource

Related concepts

- About duplicating host environments by using Deployment Manager on page 137

Related tasks

- Configuring Deployment Manager on page 132
- Adding managed resources to Deployment Manager on page 133
- Removing managed resources from Deployment Manager on page 133
- Checking managed resource disk configuration on page 134
- Backing up managed resource disk data on page 135
- Restoring disk data to a managed resource on page 136
- Managing image files on page 137

Related references

- Prerequisites for using Deployment Manager on page 131

Prerequisites for using Deployment Manager

Before using Deployment Manager with your managed resources, you must complete the following tasks:

- Verify that the managed resource is configured to give precedence to remote operations by using the PXE protocol. If Hitachi Compute Systems Manager was not running when you changed the boot settings to implement the PXE protocol on your managed resources, you must start Hitachi Compute Systems Manager and then restart the managed resource. For more information, refer to the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.
- Ensure that you do not change the hardware configuration of the managed resource after setting the task plan. You must wait until the task is complete to make any configuration changes.

Note: By default, when you use Deployment Manager to perform the following actions, the power of the target managed resource is automatically

turned off at the beginning of the task, and automatically turned back on at the completion of the task:

- Checking the disk configuration on a managed resource
- Backing up or restoring the data on the disks of a managed resource
- Taking a snapshot of a managed resource
- Deploying a master image

For details about Deployment Manager prerequisites, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

Related concepts

- About Deployment Manager on page 130
- About duplicating host environments by using Deployment Manager on page 137

Related tasks

- Configuring Deployment Manager on page 132
- Adding managed resources to Deployment Manager on page 133
- Removing managed resources from Deployment Manager on page 133
- Checking managed resource disk configuration on page 134
- Backing up managed resource disk data on page 135
- Restoring disk data to a managed resource on page 136
- Managing image files on page 137

Configuring Deployment Manager

Prerequisites

When using Deployment Manager in a cluster environment, ensure that you take the Deployment Manager services offline before changing the configuration.

You can change the default Deployment Manager configuration by using Hitachi Compute Systems Manager. We recommend that you modify the following settings:

- Location of image files
- DHCP server location (local or remote)

Modifying the Deployment Manager default settings is optional.

Procedure

1. On the **Administration** tab, select **Deployment > Settings**.
2. Click **Edit Settings**.
3. Modify the settings information as needed and click **OK**.

Result

When using Deployment Manager in a cluster environment, bring the Deployment Manager services online after changing the configuration.

For details about using the Deployment Manager services in a cluster environment, including how to bring the services online or take them offline, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide* .

Related concepts

- About Deployment Manager on page 130

Related references

- Prerequisites for using Deployment Manager on page 131

Adding managed resources to Deployment Manager

Before you can use managed resources with Deployment Manager, you must add and configure the resources using the Deployment Management feature in Hitachi Compute Systems Manager.

Procedure

1. On the **Administration** tab, select **Deployment > Licensed Resources**.
2. Select the tab of the managed resource that you are adding to Deployment Manager and click **Add Licensed Resource**.
3. Follow the instructions in the wizard to add managed resources for use with Deployment Manager.
4. Click **Submit**.

Related concepts

- About Deployment Manager on page 130

Related tasks

- Configuring Deployment Manager on page 132

Related references

- Prerequisites for using Deployment Manager on page 131

Removing managed resources from Deployment Manager

You can remove the managed resources that you are no longer using with Deployment Manager.

Note: If you replace or move a blade, the managed resources on the related blade server can no longer be referenced as managed resources in

Deployment Manager. To resolve this issue, remove the managed resources from Deployment Manager, and then re-add them.

Procedure

1. On the **Administration** tab, select **Deployment > Licensed Resources**.
2. Select the tab of the managed resource that you are removing from Deployment Manager and click **Remove Licensed Resource**.

Related concepts

- About Deployment Manager on page 130

Related tasks

- Configuring Deployment Manager on page 132
- Adding managed resources to Deployment Manager on page 133

Related references

- Prerequisites for using Deployment Manager on page 131

Checking managed resource disk configuration

We recommend that you check the latest disk configuration for all managed resources on which you plan to run any of the following deployment tasks:

- Backing up a managed resource disk
- Restoring a managed resource image file
- Deploying a managed resource

Procedure

1. On the **Resources** tab, select **General Tasks > Deployment > Check Disk Configuration**.
2. Select a resource for which you want to check disk configuration, and click **Add**.
3. To manually power off the selected resources before the task runs, select the **Manually power off selected resources before running the task** check box.
4. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.
      The task can be run immediately or later. The default setting is **Now**.
5. Click **Submit.**

Result

After the task completes successfully, you can view the disk configuration by accessing the Resources tab and selecting the affected managed resources.

Related concepts

- About Deployment Manager on page 130
- About duplicating host environments by using Deployment Manager on page 137

Related tasks

- Configuring Deployment Manager on page 132
- Adding managed resources to Deployment Manager on page 133
- Backing up managed resource disk data on page 135
- Restoring disk data to a managed resource on page 136

Related references

- Prerequisites for using Deployment Manager on page 131

Backing up managed resource disk data

You can back up the entire drive or individual partitions of a managed resource to the management server. The file created by backing up disk data is called an *image file*. If drive failure or damage occurs, you can restore the managed resource.

Procedure

1. On the **Resources** tab, select **General Tasks > Deployment > Back up System-level Images**.
2. Follow the instructions in the wizard to select a managed resource and disk option.
3. Select a backup profile or click **Edit Backup Profile** to modify an existing profile.
4. Review the power settings and modify them if required. To manually power off the selected resource before the task runs, select the **Manually power off selected resources before running the task** check box.
5. Verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run now, later, or repeated at specified intervals. The default setting is **Now**.
6. Click **Submit**.

Related concepts

- About Deployment Manager on page 130

- About duplicating host environments by using Deployment Manager on page 137

Related tasks

- Configuring Deployment Manager on page 132
- Adding managed resources to Deployment Manager on page 133
- Checking managed resource disk configuration on page 134
- Restoring disk data to a managed resource on page 136
- Managing image files on page 137

Related references

- Prerequisites for using Deployment Manager on page 131

Restoring disk data to a managed resource

You can use an image file stored on the management server to restore the disk data to a managed resource in case of disk failure or disk damage.

Procedure

1. On the **Resources** tab, select **General Tasks > Deployment > Restore System-level Images**.
2. Follow the instructions in the wizard to select a managed resource and an image file.
3. Review the power settings and modify if required. To manually power off the selected resources before the task runs, select the **Manually power off selected resources before running the task** check box.
4. Verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run immediately or at a later time. The default setting is **Now**.
5. Click **Submit**.

Related concepts

- About Deployment Manager on page 130
- About duplicating host environments by using Deployment Manager on page 137

Related tasks

- Configuring Deployment Manager on page 132
- Adding managed resources to Deployment Manager on page 133
- Checking managed resource disk configuration on page 134
- Backing up managed resource disk data on page 135
- Managing image files on page 137

Related references

- Prerequisites for using Deployment Manager on page 131

Managing image files

Backup data files or snapshot data files that are created by Deployment Manager are called *image files*. Using Deployment Manager, you can delete image files, edit image file properties, and add image files back into Deployment Manager from a different storage location.

Caution: Before you delete an image file that you might need later, back it up to another location so that it is available if you need to restore or deploy a resource.

Procedure

1. On the **Administration** tab, select **Deployment > Image File Management**.
2. Select the image file to add or delete, or whose properties you want to edit.
   - To delete the image file, click **Delete Image Files** and confirm the deletion.
   - To edit the image file properties, click **Edit Information**, make the required changes, and then click **OK**.
   - To add an existing image file back into Deployment Manager, copy the image file to the path in which Deployment Manager stores image files, click **Import Image File**, select the image to add, and then click **OK**.

Related concepts

- About Deployment Manager on page 130
- About duplicating host environments by using Deployment Manager on page 137

Related tasks

- Configuring Deployment Manager on page 132
- Restoring disk data to a managed resource on page 136

Related references

- Prerequisites for using Deployment Manager on page 131

About duplicating host environments by using Deployment Manager

You can use Deployment Manager to duplicate a managed host and the associated environment (such as operating system and applications) on another managed resource. This function is referred to as deploying a managed resource.

Deployment consists of several tasks that you complete:

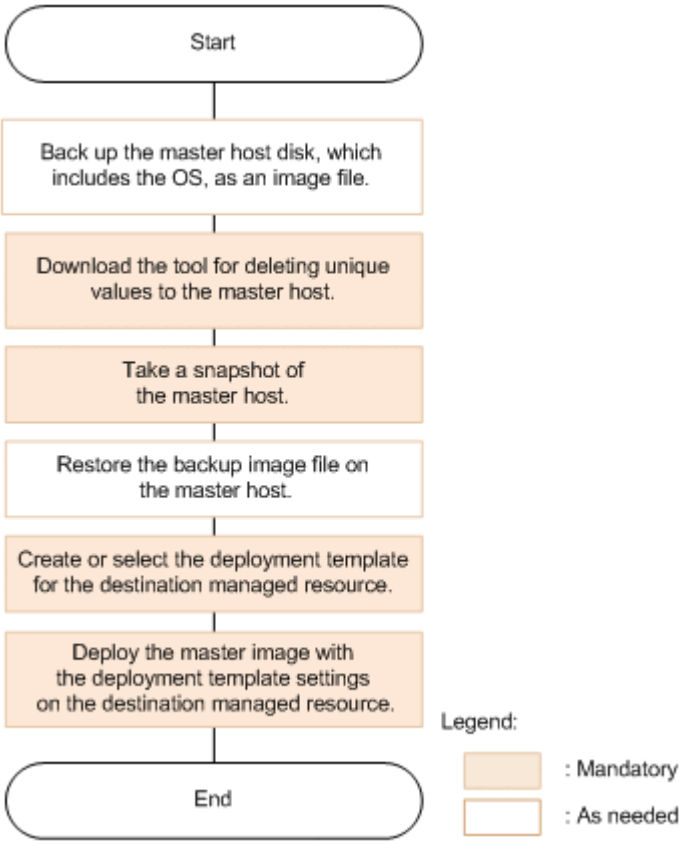
Tasks required to prepare for deploying a master image:

- Select a managed resource to designate as the master host from which to create a master image.
- Configure the master host to reflect the specific operating system and system-level configuration required for deployment.
- Remove any unique information from the master host by using the Sysprep tool, and then take an image snapshot.

Tasks required to deploy a master image:

- Verify that the destination resource uses the same hardware and firmware as the master host.
  For details about hardware requirements, see the hardware documentation. For details about firmware requirements, see the *Compute Systems Manager Release Notes*.
- Configure the deployment template for the destination resource.
- Deploy the master image on the destination managed resource.

The following graphic illustrates the deployment workflow.



Related concepts

- About Deployment Manager on page 130

Related tasks

- Configuring Deployment Manager on page 132
- Adding managed resources to Deployment Manager on page 133
- Removing managed resources from Deployment Manager on page 133
- Checking managed resource disk configuration on page 134
- Backing up managed resource disk data on page 135
- Restoring disk data to a managed resource on page 136
- Managing image files on page 137
- Downloading the tool for deleting unique values from a master host on page 140
- Creating a master host for managed resource deployment on page 139
- Taking a snapshot of a master host disk on page 140
- Setting up deployment templates on page 141
- Deploying a master image on page 142

Related references

- Prerequisites for using Deployment Manager on page 131

Creating a master host for managed resource deployment

Before you create a master image snapshot in order to deploy a managed resource, you must create a master host that includes the operating system you want to deploy and any company-specific system-level applications (antivirus, firewall, and so on). This host is intended to serve as the snapshot source only. It cannot be used for any other purpose.

Note: When you take a snapshot of the master host, the operating system of the server is disabled and you cannot use the server again unless you restore it using a backup image.

Procedure

1. Select a host to use as the master.
2. Configure the host with the operating system and company-specific system-level applications (antivirus, firewall, and so on) that you want reflected in the master image snapshot.

Related concepts

- About duplicating host environments by using Deployment Manager on page 137

Related tasks

- Downloading the tool for deleting unique values from a master host on page 140
- Taking a snapshot of a master host disk on page 140
- Setting up deployment templates on page 141

- Deploying a master image on page 142

Downloading the tool for deleting unique values from a master host

You must delete all unique values from the master host before you take a snapshot. You remove all unique values from a master host by using the Sysprep tool, which you download to the master host.

Procedure

1. From a managed resource on the designated master host, open a browser and log in to Hitachi Compute Systems Manager.
2. From the **Tools** menu, select **Download**.
3. Locate the Sysprep tool in the list of downloads and click **Download** for the operating system that corresponds to the master host.

Result

You can use the downloaded Sysprep tool to delete unique information from the hard disk of the managed resource.

For detailed information on how to use the Sysprep tool to delete unique information from the master host, see the ReadMe file included in the tool download file.

Related concepts

- About duplicating host environments by using Deployment Manager on page 137

Related tasks

- Creating a master host for managed resource deployment on page 139
- Taking a snapshot of a master host disk on page 140
- Setting up deployment templates on page 141
- Deploying a master image on page 142

Taking a snapshot of a master host disk

You can create a disk image from a master host from which all unique information is deleted. This process is called *taking a snapshot*. The snapshot data file is called an image file. You can then use the snapshot as the master image for deployment tasks.

Procedure

1. On the **Resources** tab, select **General Tasks > Deployment > Take a Snapshot**.
2. Follow the instructions in the wizard to select a managed master host.

3. Review the power settings and modify if required. To manually power off the selected resources before the task runs, select the **Manually power off selected resources before running the task** check box.
4. Verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run immediately or at a later time. The default setting is **Now**.
5. Click **Submit**.

Related concepts

- About duplicating host environments by using Deployment Manager on page 137

Related tasks

- Creating a master host for managed resource deployment on page 139
- Downloading the tool for deleting unique values from a master host on page 140
- Setting up deployment templates on page 141
- Deploying a master image on page 142

Setting up deployment templates

You can set up deployment templates for use when deploying master images to destination resources.

Procedure

1. On the **Administration** tab, select **Deployment > Deployment Templates**.
2. Click **Create Template**.
3. Follow the instructions in the wizard to enter the deployment template parameters for the destination managed resource. You can also copy and edit a different deployment template to create a new parameter.
4. Click **Submit**.

Related concepts

- About duplicating host environments by using Deployment Manager on page 137

Related tasks

- Creating a master host for managed resource deployment on page 139
- Downloading the tool for deleting unique values from a master host on page 140
- Taking a snapshot of a master host disk on page 140
- Deploying a master image on page 142

Deploying a master image

By setting a deployment template for a snapshot, you can create a master image, which you can use to deploy the master host environment to a destination managed resource.

Prerequisites

1. Verify that there is an existing image snapshot that you created using the master host.
2. Verify that the hardware specifications of the master host matches that of the destination managed resource.
3. Verify that the deployment template for the destination managed resource is created.

After completing the prerequisite tasks, you are ready to deploy the master image to a managed resource.

Procedure

1. On the **Resources** tab, select **General Tasks > Deployment > Deploy Master Image**.
2. Follow the instructions in the wizard to select a destination managed resource, an image snapshot, and the required deployment templates.
3. To manually power off the selected resource before the task runs, select the **Manually power off selected resources before running the task** check box.
4. Verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule. The task can be run immediately or at a later time. The default setting is **Now**.
5. Click **Submit**.

Related concepts

- About duplicating host environments by using Deployment Manager on page 137

Related tasks

- Creating a master host for managed resource deployment on page 139
- Downloading the tool for deleting unique values from a master host on page 140
- Taking a snapshot of a master host disk on page 140
- Setting up deployment templates on page 141

Updating firmware

You can update the firmware of Hitachi chassis and blade servers using Hitachi Compute Systems Manager.

About updating firmware

You can update the firmware of Hitachi chassis or blade servers using Hitachi Compute Systems Manager.

You can update firmware for the following managed resource types:

- Chassis
  Updates the firmware of a chassis management module.
- Blade servers
  Updates the firmware of the blades that comprise the blade server.

Related tasks

- Updating chassis firmware on page 143
- Updating blade server firmware on page 144

Updating chassis firmware

Using Hitachi Compute Systems Manager, you can update the firmware of a chassis management module. The chassis uses the new firmware when the update processing is complete.

You must obtain the firmware files before you begin this procedure.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Chassis > Chassis**.
   The managed **Chassis** list opens.
2. Select one or more chassis for which you want to update the firmware.
3. Click **More Actions > Update Firmware**.
4. Select a firmware file.
5. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.
      The task can be run immediately or at a later time. The default setting is **Now**.
6. Click **Submit**.

Result

You can check the task results on the Tasks & Alerts tab and verify the updated firmware version in the Chassis list on the Resources tab.

Related concepts

- About updating firmware on page 143

Related tasks

- Updating blade server firmware on page 144

Updating blade server firmware

Using Hitachi Compute Systems Manager, you can update the firmware of the blades that comprise a blade server. The updated firmware is applied after update processing is complete. However, if you update the firmware for a blade server while that blade server is running, you need to restart the blade server after the update is complete.

You must obtain the firmware files before you begin this procedure.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers > Blade**.

   The managed **Server** list opens.
2. Select one or more blade servers for which you want to update the firmware.
3. Click **More Actions > Update Firmware**.
4. Select a firmware file.
5. Click **Show Plan** and verify that the task information is correct in the plan summary.
   a. Optionally, update the task name and provide a description.
   b. Expand **Schedule** to specify the task schedule.

      The task can be run immediately or at a later time. The default setting is **Now**.
6. Click **Submit**. You can check the results of the firmware update from the **Tasks & Alerts** tab.
7. If you updated the firmware while the blade server was running, wait until the tasks complete, and then either reboot the hosts running on the blade server or reset the blade server.

Result

You can check the blade server firmware version from the blade server list or the blade server details on the Resources tab.

Related concepts

- About updating firmware on page 143

Related tasks

- Updating chassis firmware on page 143
- Restarting a host on page 82
- Resetting the power for a server on page 86

5

Monitoring managed resources and resolving alerts

This module describes how to monitor managed resources and manage alerts.

- ☐ Configuring alert settings
- ☐ Monitoring the status of managed resources and tasks
- ☐ Monitoring the performance and power consumption of managed resources
- ☐ Saving resource information output in CSV format
- ☐ Grouping managed resources
- ☐ Alerts and alert resolution

Configuring alert settings

This module describes how to configure alert reception settings, alert notification settings, and automated event handling.

About alert settings

The Hitachi Compute Systems Manager management client enables you to view information (alerts) about failures that occur on a managed resource. Alerts provide the name of the resource on which a failure occurred and the specific location of the failure.

Note: You must set up alerts in advance to enable Compute Systems Manager monitoring of managed resource failure information (alerts).

You can configure the following alert items:

- Configure settings for receiving SNMP traps
  You can receive SNMP traps from a managed host as alerts in Compute Systems Manager.
- Specify an alert-level for email notification
  You can receive email notifications from Compute Systems Manager when an alert occurs. You can define settings to receive notifications when an alert of a certain level occurs. Alert settings notified by email can be changed by individual users.

  Note: Managed chassis or server alerts occurring while Compute Systems Manager is stopped are still received after Compute Systems Manager starts. However, the email notifications set for alerts are not sent.

- Specify scripted commands to run when an alert occurs
  You can register scripted commands to run whenever an alert occurs. Scripted commands can only run from the management server.

  Note: Managed chassis or server alerts occurring while Compute Systems Manager is stopped are still received after Compute Systems Manager starts. However, the scripted commands set for alerts are not run.

- Specify threshold values to trigger alerts
  You can set the threshold values for each type of performance data and for each host so that you can receive an alert before potential performance problems occur on a managed host.
- Specify the number of alerts to store

You can set the number of alerts to store on the system. If the number of alerts exceeds the specified value, the system periodically deletes the oldest alerts. By default, the number of alerts to store is specified by the system-defined values. However, you can specify user-defined custom values to reduce the number of alerts to keep, which decreases the amount of time it takes to display the list of alerts.

Related concepts

- About alerts and alert resolution on page 191

Related tasks

- Enabling SNMP trap reception on page 149
- Associating SNMP traps with alert IDs on page 150
- Specifying an alert level for email notification on page 152
- Specifying scripted commands to run when an alert occurs on page 157
- Specifying threshold values for performance data on page 158
- Specifying the number of alerts to store on page 158

About SNMP trap reception settings

Before Hitachi Compute Systems Manager can receive SNMP traps from managed hosts, you must configure the system to convert the SNMP traps into alerts. You enable SNMP trap reception and conversion to alerts by associating alert IDs reserved for SNMP traps with the SNMP trap object identifier (OID).

If SNMP trap reception is enabled, all SNMP traps output from managed hosts are converted to the following default alerts:

- **Alert ID:** 0x0000
- **Alert Level:** Information
- **Location:** Other
- **Alert Content:** Received SNMP Trap from Host

To manage alerts more carefully, you can associate specific SNMP traps with alerts other than the default 0x0000. Compute Systems Manager provides some default alerts that you can associate with SNMP traps.

You can also define your own alerts to be associated with SNMP traps.

Related tasks

- Associating SNMP traps with alert IDs on page 150
- Enabling SNMP trap reception on page 149

Enabling SNMP trap reception

If SNMP trap reception is enabled, all SNMP traps output from managed resources are converted to alerts.

Procedure

1. On the **Administration** tab, select **System Settings** and then select **SNMP**.
2. Click **Edit Global SNMP Settings**.
3. Select the **SNMP Enabled** check box.
4. Type a community name.
5. Click **OK**.

Result

All SNMP traps output from the managed host are received as alerts (with the default ID: 0x0000).

Related concepts

- About SNMP trap reception settings on page 149

Related tasks

- Associating SNMP traps with alert IDs on page 150

Associating SNMP traps with alert IDs

Associating SNMP traps with alert IDs allows you to refine the information you see when an SNMP trap is received from a managed resource.

Before you configure Hitachi Compute Systems Manager to receive SNMP traps, verify that SNMP trap definition MIB files are registered in the management server. For details about how to register MIB files, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

If an undefined SNMP trap exists in the MIB file, you can use the management client to register it as a user-defined SNMP trap.

Procedure

1. On the **Administration** tab, select **System Settings**.
2. Select **SNMP**.
3. On the **Mappings** tab, click **Create SNMP Setting**.
4. Click **Select Alert ID**, and from the **Alert ID** list, select one of the reserved alert IDs to be associated with the SNMP trap.

   If you want to define a new alert, select an alert ID that does not yet have defined alert content.
5. Optionally, define the **Alert Level**, **Failure Location**, and **Alert Content**.
6. In **SNMP Traps**, select an SNMP trap to be associated with the alert.
   a. If there is no SNMP trap available that you want to associate with in the table, click **Add SNMP Trap** and choose an SNMP trap from the list.

b. If you want to define a new SNMP trap, click **Add SNMP Trap**, expand **Add User SNMP Trap**, add the required information to create an SNMP trap to be associated with the alert ID you specified, and click **Add to SNMP Traps List** to add the new SNMP trap to the list. The new SNMP trap is selected.

7. Click **OK**.

   Your settings are saved.

Result

To verify the settings, select the Administration tab, click System Settings, then click SNMP. Click the alert ID link to view the SNMP setting summary.

Related concepts

- About SNMP trap reception settings on page 149

Related tasks

- Registering SNMP trap definitions that are not defined in MIB files on page 151
- Verifying MIB-defined SNMP traps definitions on page 151

Verifying MIB-defined SNMP traps definitions

Before you can enable the SNMP trap definitions provided in MIB files, verify that you have registered the SNMP trap MIB files to the management server. For details about how to register MIB files, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

You cannot edit or delete MIB-defined SNMP traps by using the Hitachi Compute Systems Manager user interface. To change or delete MIB-defined SNMP traps, edit the MIB file on the management server.

Procedure

1. On the **Administration** tab, select **System Settings**.
2. Select **SNMP**.
3. Select the **MIB SNMP Traps** tab.

Related concepts

- About alert settings on page 148

Registering SNMP trap definitions that are not defined in MIB files

Usually, SNMP trap definitions are registered by using MIB files. However, you can use the management client to register custom SNMP traps.

Procedure

1. On the **Administration** tab, select **System Settings**.

2. Select **SNMP**.
3. On the **User SNMP Traps** tab, click **Add User SNMP Trap**.
4. Type the required values and click **OK**.

Related concepts

- About alert settings on page 148
- About SNMP trap reception settings on page 149

Specifying an alert level for email notification

Hitachi Compute Systems Manager can send email notifications for alerts based on alert levels that you specify. Users can individualize the alert level for which email notifications are sent to them. Preferred alert-level settings are stored for each user.

Prerequisites

Before you can receive alert level email notification, you must verify the following:

- Compute Systems Manager email notification setup is complete.
- User account profile has been updated to register the email address.

Procedure

1. On the **Administration** tab, select **Automated Event Handling**.
2. Select **E-mail Notifications**.
3. Click **Edit Setting**.
4. Select the alert level for which you would like to be notified and click **OK**.

Result

The user now receives email notifications for alerts that match the specified alert level.

Related concepts

- About alert settings on page 148

Related tasks

- Editing a user account profile on page 201
- Editing your own profile on page 201
- Setting up email notification on page 40

About automated event handling

To automate event handling, create and register scripted commands to run when an alert occurs.

When using scripted commands, be aware of the following:

- Scripted commands can be run only from the management server.

- Managed chassis or server alerts occurring while Compute Systems Manager is stopped are still received after Compute Systems Manager starts. However, the scripted commands set for alerts are not run. Check the alerts, and then run the scripted commands manually as necessary.

Related concepts

- About alerts and alert resolution on page 191

Related tasks

- Specifying scripted commands to run when an alert occurs on page 157

Related references

- Scripted command prerequisites and conditions (Windows) on page 153
- Scripted command prerequisites and conditions (Linux) on page 155

Scripted command prerequisites and conditions (Windows)

Scripted commands that run when an alert occurs must adhere to the following conditions:

- Commands must be in `.exe` or `.bat` format.
- Commands cannot exceed 260 bytes.
  Specify variables so that the expanded character string for variables does not exceed the operating system limit value.
- Use full paths (excluding paths set in the `PATH` environment variable). You cannot specify a network directory.
- All resources affected by commands must allow Windows System account access.
- You cannot run Internal Windows commands at the time an alert occurs. To run an internal Windows command, you must include the command in the batch file or use the `cmd /c` command.
- The current directory is *`HCS-Common-Component-install-directory`*`\uCPSB\CC\web\containers\ComputeSystemsManagerWebService`.
- The only environment variables that are enabled when the system runs a command are the system environment variables enabled when the Hitachi Compute Systems Manager program service starts.
  No environment variables are read when the system runs a command.
- Command paths or arguments that contain spaces must be enclosed in double quotation marks (").

You cannot run the following:

- Commands that display windows or dialog boxes.
- Commands that require interaction.
  When specifying the `csm login` command of the Compute Systems Manager CLI, you can avoid interaction by specifying a user name and password in the parameters. For details about the `csm login` command,

see the *Hitachi Command Suite Compute Systems Manager CLI Reference Guide.*

- Windows 16-bit applications.
- Programs that use Windows Dynamic Data Exchange (DDE).
- Resident programs.
- Programs on removable disks that are not active.

The following table lists variables that you can specify for arguments in a scripted command.

Variable	Description
%D	Outputs the date of the alert in *YYYY-MM-DD* format.
%T	Outputs the time of the alert in *HH-MM-SS* format.
%M[1]	Outputs the name of the resource on which the alert originated. For hosts: *host-name* For chassis or blade servers: *chassis-name* For rack-mounted servers: *server-name* For LPARs: *blade-server-name*
%A	Outputs the IP address of the resource on which the alert originated.
%L	Outputs the alert level character string. For information: INFO For warnings: WARNING For errors: ERROR
%I	Outputs the alert ID character string in 0x*XXXX* format.
%S[1]	Outputs the alert content.
%P[1]	Outputs the failure location for the alert. For hosts: The failure locations set in the SNMP settings For chassis or blade servers: *module-type-name*-Slot*slot-number* For rack-mounted servers: *module-type-name* For LPARs: Server blade-Slot*slot-number*-LPAR*LPAR-number* *slot-number* might not be output depending on the module type, or it might be output with multiple slot numbers linked.
%H[1]	Outputs the ID of the LPAR Manager on which the alert originated. This might be output as an empty string.
%V[1]	Outputs the name of the LPAR on which the alert originated. This might be output as an empty string.
%U[1]	Outputs the number of the LPAR on which the alert originated. This might be output as an empty string.

1. This variable must be enclosed in double quotation marks (").

The following list shows command examples:

- Specifying "arg1" and "arg2"as the arguments of a command:
  `"c:\program files\a\a.exe" arg1 arg2`
- Redirecting the command results to a file named d:\work.txt:
  `cmd /c "c:\program files\x\x.bat" > d:\work.txt`
- Specifying a variable as a command argument:
  `"c:\program files\a\a.exe" %A "%S"`

Related tasks

- Specifying scripted commands to run when an alert occurs on page 157

Scripted command prerequisites and conditions (Linux)

Scripted commands that run when an alert occurs must adhere to the following conditions:

- Commands must be run using the correct format or reside in a shell script.
- Commands cannot exceed 260 bytes.
  Specify variables so that the expanded character string for variables does not exceed the operating system limit.
- Use full paths (excluding the paths set in the `PATH` environment variable).
  When specifying an NFS mount directory, set the directory permissions to grant root user access.
- All resources affected by commands must allow root user account access.
- Internal Linux commands cannot run at the time an alert occurs. To run an internal Linux command, you must write the command in a shell script file.
- The current directory is *HCS-Common-Component-install-directory*`/uCPSB/CC/web/containers/ComputeSystemsManagerWebService`.
- The only environment variables that are enabled when the system runs a command are the system environment variables enabled when the Hitachi Compute Systems Manager program service starts.
  No environment variables are read when the system runs a command.
- Command paths or arguments that contain spaces must be enclosed in double quotation marks (").

You cannot run the following:

- Commands that require interaction
  When specifying the `csm login` command of the Compute Systems Manager CLI, you can avoid interaction by specifying a user name and password in the parameters. For details about the `csm login` command, see the *Hitachi Command Suite Compute Systems Manager CLI Reference Guide.*
- Resident programs
- Programs on removable disks that are not active

The following table lists variables that you can specify for arguments in a scripted command.

Variable	Description
%D	Outputs the date of the alert in *YYYY-MM-DD* format.
%T	Outputs the time of the alert in *HH-MM-SS* format.
%M[1]	Outputs the name of the resource on which the alert originated. For hosts: *host-name* For chassis or blade servers: *chassis-name* For rack-mounted servers: *server-name* For LPARs: *blade-server-name*
%A	Outputs the IP address of the resource on which the alert originated.
%L	Outputs the alert level character string. For information: INFO For warnings: WARNING For errors: ERROR
%I	Outputs the alert ID character string in 0x*XXXX* format.
%S[1]	Outputs the alert content.
%P[1]	Outputs the failure location for the alert. For hosts: The failure locations set in the SNMP settings For chassis or blade servers: *module-type-name*-Slot*slot-number* For rack-mounted servers: *module-type-name* For LPARs: Server blade-Slot*slot-number*-LPAR*LPAR-number* *slot-number* might not be output depending on the module type, or it might be output with multiple slot numbers linked.
%H[1]	Outputs the ID of the LPAR Manager on which the alert originated. This might be output as an empty string.
%V[1]	Outputs the name of the LPAR on which the alert originated. This might be output as an empty string.
%U[1]	Outputs the number of the LPAR on which the alert originated. This might be output as an empty string.

1. This variable must be enclosed in double quotation marks (").

The following shows an example command in which a variable is specified as a command argument:

```
/test/test.sh %A "%S"
```

Related concepts

- About automated event handling on page 152

- About alert settings on page 148

Related tasks

- Specifying scripted commands to run when an alert occurs on page 157

Specifying scripted commands to run when an alert occurs

You can specify scripted commands to run when an alert occurs. You must configure SNMP trap reception if you are setting the commands to run when an alert occurs on a host. You must also configure threshold values for performance data if you are setting the commands to run when a performance alert occurs.

Procedure

1. On the **Administration** tab, select **Automated Event Handling**.
2. Click **Scripted Commands**.
3. Click **Create Scripted Command**.
4. Type a name for the command in the **Scripted Command Name** field.
5. In the **Command Path** field, type the full path of the scripted command that you want to run when the specified alert occurs.

   You can specify arguments for the command after the full path.
6. For **Resource Type**, select the type of resource to which the command applies.
7. For **Resources**, click **Add Resources** to select the resource for which to apply the command settings.
8. For the **Alert ID**, click **Add Alert IDs** and then select one or more alert IDs from the list.
9. Specify any other required items, and then close the dialog box.

   The scripted command is saved.

Result

To verify the settings, click the Administration tab, and then select Automated Event Handling > Scripted Commands. To view details, click the name of the scripted command.

Related concepts

- About automated event handling on page 152
- About alert settings on page 148

Related references

- Scripted command prerequisites and conditions (Windows) on page 153
- Scripted command prerequisites and conditions (Linux) on page 155

Specifying threshold values for performance data

You can set a threshold value for each performance metric that Hitachi Compute Systems Manager collects so that an alert is triggered when that value is exceeded.

Prerequisites

You can analyze the performance of hosts only if they are managed by Compute Systems Manager.

Procedure

1. On the **Administration** tab, click **Performance and Power Monitoring > Performance > Create Performance Profile**.
2. In the window that opens, set the threshold values for triggering performance alerts.

Result

You will receive alerts related to performance metrics of managed hosts when performance metric threshold values are exceeded.

Related concepts

- About alert settings on page 148

Related tasks

- Registering hosts and selecting performance data types on page 177

Specifying the number of alerts to store

You can set the number of alerts to store on the system. If the number of alerts exceeds the specified value, the system periodically deletes the oldest alerts. By default, the number of alerts to store is specified by the system-defined values. However, you can specify user-defined custom settings to reduce the number of alerts to keep, which decreases the amount of time it takes to display the list of alerts.

If you want to change the number of alerts to store from the system-defined value, you can specify a custom value.

Procedure

1. On the **Administration** tab, select **System Settings > Alert > Edit Settings**.
2. Select **Use custom settings**.
3. Specify the custom settings as follows:
   a. Specify the maximum number of alerts to store in the system.

b. Specify the number of alerts to keep after the system reaches the maximum and deletes the oldest alerts.
c. To delete alerts immediately instead of waiting until the next system maintenance cycle, select the **Delete alerts immediately** check box.

4. Click **OK** to save your settings.

Tip: You can return to the system-defined settings at any time by returning to this screen and selecting **Use the system settings**.

Related concepts

- About alerts and alert resolution on page 191
- About alert settings on page 148

Monitoring the status of managed resources and tasks

Hitachi Compute Systems Manager provides multiple methods and displays for viewing information, including:

- a dashboard for viewing summary information about managed resources and their statuses.
- a global monitoring bar for viewing task status.
- tabs that provide access to lists with more detailed information about resources, tasks, and alerts.

About viewing information summaries

Hitachi Compute Systems Manager provides information summaries in various areas of the web client. The dashboard displays summary information for the status of managed resources, and other summary information, such as unresolved alerts. Task status summaries are available in the global monitoring bar.

When you log in to Compute Systems Manager, the dashboard appears. You can access the dashboard at any time by using the Dashboard tab. You can customize the dashboard to select which reports to display and the layout of the reports on the page. If you create logical groups, you can display reports for each logical group. When using the drop-down menu for selecting a logical group, a forward slash (/) appears at the beginning of a public logical group path, and a tilde (~) appears at the beginning of a private logical group path.

The dashboard includes the following reports:

- Resource Status
  Displays the operating status for all managed resource types.
  - Host Status

Displays the number of hosts in a pie graph as Running (green), Stopped (red), and Unknown (gray).
    - Hypervisor Status
      Displays the number of hypervisors in a pie graph as Running (green), Stopped (red), and Unknown (gray).
    - Virtual Machine Status
      Displays the number of virtual machines in a pie graph as Running (green), Stopped (red), and Unknown (gray).
    - Chassis Power Status
      Displays the number of chassis in a pie graph as On (green), or Unconnected (gray).
    - Server Power Status
      Displays the number of servers in a pie graph, as On (green), Off (red), and Unconnected (gray).
- Alert Status
  Displays the number of resources on which an unresolved alert has occurred and a bar graph showing the top three resources by number of unresolved alerts.
  The alerts are separated in the bar graph by Errors (red) and Warnings (yellow).
- Information
  Displays a To Do list specific to the logged-in user and shows events (tasks and alerts) that have occurred.
  The To Do list shows things you have to respond to, such as unresolved alerts and failed tasks. The Event list shows both alerts and tasks, and is configurable to show new, current day, or the previous week's system events.
- Unresolved Alerts
  Displays a list of alerts that have not yet been resolved and provides access for you to resolve each alert.
  To view alert details, select an alert, and then click Respond to Alert for more detailed alert information. From the Detailed Alert Information dialog box, you can assign the alert to another user, change the status, or share the alert via email.

If you have licenses to use Performance Monitoring and Power Monitoring, you can also see the Performance Monitor and Power Monitor reports on the dashboard.

- Performance Monitor
  Displays host performance data for the last 24 hours. You can select up to five hosts to be displayed.
- Power Monitor
  Displays total power consumption for all supported Hitachi servers, unless a logical group is selected. You can choose the term (day, week, month) and filter by logical group.

You can also view summary information for managed resources on the Resources tab.

The global monitoring bar provides task status and is always available at the bottom of the main window, regardless of which tab you are viewing. You can click the links for each status type to view a list of tasks with that status and to view more details about the status of each task.

Note: Only tasks that you created are included in the task summaries in the global monitoring bar.

Related concepts

- About logical groups on page 188

Related tasks

- Monitoring the status of managed resources from the dashboard on page 161
- Customizing the dashboard on page 162
- Resolving alerts on page 193
- Viewing task status from the global monitoring bar on page 163

Monitoring the status of managed resources from the dashboard

The Hitachi Compute Systems Manager dashboard displays real-time reports for managed resources, including at-a-glance resource operating status, events, and unresolved alerts.

If you have licenses to use the Performance Monitoring and Power Monitoring, you will also see the Performance Monitor and Power Monitor reports on the dashboard.

When you log in to Compute Systems Manager, the dashboard appears. If another tab is active, the dashboard can be viewed at any time by clicking the Dashboard tab.

Procedure

1. Click the **Dashboard** tab, if another tab is active.
2. Use the dashboard reports to review resource status, alert status, including the top 3 resources with active error alerts, events, and a list of unresolved alerts. If you have licenses for the performance monitoring and power monitoring, then these reports are displayed in the dashboard as well.
3. To view details of a specific report, click the  icon to view the related tab for more specific information about a managed resource.

Related concepts

- About viewing information summaries on page 159

Related tasks

- Resolving alerts on page 193
- Viewing detailed host information on page 165
- Customizing the dashboard on page 162

Customizing the dashboard

You can customize the dashboard to change the layout or to display only the reports that you want to view. Hitachi Compute Systems Manager retains the changes that you make so that the dashboard displays your customized settings the next time you log in.

Procedure

1. On the **Dashboard** tab, click **Dashboard Settings**.
2. Make the desired changes and then close the dialog box.

   You can change the number of columns displayed on the dashboard and increase or reduce the number of reports to display.
3. To change the layout of the reports on the dashboard, drag the title bar of each report to the desired location.

Related concepts

- About viewing information summaries on page 159

Related tasks

- Monitoring the status of managed resources from the dashboard on page 161

Customizing performance reports displayed on the dashboard

You can specify up to five hosts or a type of graph for performance reports displayed in the dashboard and choose the metrics and report type you want. Hitachi Compute Systems Manager retains the changes you make so that the dashboard displays your customized settings the next time you log in.

Procedure

1. On the **Dashboard**, open the **Performance Monitor** report.
2. Open the **Dashboard Performance Monitoring Settings** dialog box by clicking the tool  icon.
3. Select the type of performance report you want to display in the dashboard.

   a. Choose a report type, either **Display by Host** or **Display by Metric**.
   b. Under **Threshold**, select an alert level displayed by a sub-line.
   c. Select up to five hosts for that you want to display metric data.

d. If you chose to **Display by Metric**, select metrics from the available metrics list.

4. Click **OK**.

Related concepts

- About viewing information summaries on page 159

Related tasks

- Monitoring the status of managed resources from the dashboard on page 161

Viewing task status from the global monitoring bar

Hitachi Compute Systems Manager displays task summary information at the bottom of the main window for tasks that you have created. You can click the link for each status type to display a list of tasks for each status.

The global monitoring bar is available at the bottom of the main window regardless of which tab is active.

Procedure

1. In the global monitoring bar, click the link next to the task status for which you want to display a list of tasks.
2. Review the task list.
3. Click **Close** to close the task list.

Related concepts

- About viewing information summaries on page 159
- About tasks and task management on page 123

Related tasks

- Setting the display duration for task status indicators on page 163

Related references

- Navigating the Hitachi Compute Systems Manager main window on page 28

Setting the display duration for task status indicators

You can specify how long to accumulate the tasks displayed in the global monitoring bar for Completed and Failed tasks. Each user can specify the aggregation period.

Procedure

1. Click the **Completed** or **Failed** task link.
2. Click **Edit Duration**.

3. Specify a date for which you want to start accumulating completed and failed tasks.

Result

A list of tasks that were completed or failed since the chosen start date is displayed.

Related concepts

- About viewing information summaries on page 159

Related tasks

- Viewing task status from the global monitoring bar on page 163

Viewing the configuration and relationships of resources managed by a hypervisor

You can view the configuration and relationships of the resources managed by a hypervisor using the topology view.

Procedure

1. On the **Resources** tab, select **Virtualization > All Hypervisors**.
2. From the list of hypervisors, select the hypervisor type.
3. Select the hypervisor for which you want to view information related to resources and click **View Topology**.

Result

The topology view of the specified hypervisor is displayed.

Related concepts

- About viewing information summaries on page 159

Related tasks

- Refreshing hypervisor information on page 171
- Viewing the configuration and relationships of a virtual machine on page 164
- Viewing detailed virtual machine information on page 166

Related references

- Navigating the Hitachi Compute Systems Manager main window on page 28

Viewing the configuration and relationships of a virtual machine

You can view the configuration and relationships between a virtual machine and the resources it is managing as well as the host or server running the virtual machine.

Procedure

1. On the **Resources** tab, select **Virtualization > All Virtual Machines**.
2. Select the virtual machine type.
3. Select the virtual machine for which you want to view information related to resources and click **View Topology**.

Result

The topology view of the specified virtual machine is displayed.

Viewing the configuration of LPARs in LPAR Manager

You can view LPAR configuration information using LPAR Manager.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers > Blade**.
2. In the server list window, click **Server Name**.
3. Select **Logical Partitioning** and then **LPAR**.

Viewing the configuration and relationships of an LPAR

You can view the host configuration for a managed LPAR or blade server configuration.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Logical Partitions > LPAR**.
2. From the list of LPARs, select the LPAR hosting the configuration or topology you want to view, and then click **View Topology**.

Viewing detailed host information

You can view detailed host information on the Resources tab.

Procedure

1. On the **Resources** tab, click **Hosts** to expand the tree.
2. Select the operating system of the hosts you want to view.

   You can use the filtering attributes to filter the displayed items.
3. To view information about a specific host, click the link for the host in the list of hosts.
4. View the **Host Summary**, or click the tabs to access specific host information. Use the filtering attributes under each tab to refine the host details.

Related concepts

- About viewing information summaries on page 159

Related tasks

- Refreshing host information on page 170

Related references

- Navigating the Hitachi Compute Systems Manager main window on page 28

Viewing detailed hypervisor information

View configuration information for hypervisors.

Procedure

1. On the **Resources** tab, select **Virtualization**.
2. From **All Hypervisors**, select the hypervisor type.
3. From the list of hypervisors, click the **Hypervisor Name** link for which you want to view information.
   - To view a summary of the hypervisor, click **Text View**.
   - To view diagrams related to the hypervisor, click **Topology View**.
   - To view information about a virtual machine that runs on the hypervisor, click the **VM Name** link on the **VMs** tab.

Result

The configuration information of a managed hypervisor is displayed.

Related concepts

- About viewing information summaries on page 159

Viewing detailed virtual machine information

View configuration information for virtual machines.

Procedure

1. On the **Resources** tab, select **Virtualization**.
2. From **All Virtual Machines**, select the virtual machine type.
3. From the list of virtual machines, click the **VM Name** link for which you want to view information.
   - To view a summary of the virtual machine, click **Text View**.
   - To view diagrams related to the virtual machine, click **Topology View**.

Result

The configuration information of a managed virtual machine is displayed.

Related references

- Navigating the Hitachi Compute Systems Manager main window on page 28

Viewing detailed chassis information

You can view configuration information for managed chassis and the blade servers on which they are mounted.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Choose **All Chassis**.
3. Expand the tree and select the chassis whose information you want to verify.
4. From the list of chassis, click the **Chassis Name** link for which you want to view information. The configuration information for the managed chassis is displayed.

   To view information about a blade server mounted on the chassis, click the **Server Name** link of the **Server Blades** tab.
5. To view detailed hardware information about a chassis, select **View Additional Chassis Information**, from the **More Actions** menu.

Related concepts

- About viewing information summaries on page 159

Related tasks

- Refreshing chassis information on page 172

Related references

- Navigating the Hitachi Compute Systems Manager main window on page 28

Viewing detailed server information

You can view configuration information for managed servers including the following:

- Information for hosts attached to the server
- Information for the chassis on which a blade server is mounted
- Information for LPARs on the blade server
- Information for volumes allocated to the server (requires that you enable the Obtain Storage Volume information option for the Device Manager connection)

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.

2. Select **All Servers**.
3. Expand the tree and select the type of server for which you want to view information.
4. From the list of servers, click the **Server Name** for which you want to view information.
   - To verify information about a host mounted on a server, click **Host Name**.
   - To verify information about the chassis on which the blade server is mounted, click **Chassis Name** in the **Summary** field.
   - To verify LPAR information, select **Logical Partitioning > LPAR**, and then click the **LPAR Name** link.
   - To view volume information for the storage system that is allocated to the server, select the **Storage Volumes** tab.
5. To view detailed hardware information about a blade server, from the **More Actions** menu, select **View Additional Blade Information**.

Related concepts

- About viewing information summaries on page 159

Related tasks

- Refreshing server information on page 173
- Specifying user-defined asset tags for servers on page 168
- Setting up a connection with Hitachi Device Manager on page 43

Related references

- Navigating the Hitachi Compute Systems Manager main window on page 28

Specifying user-defined asset tags for servers

You can specify a user-defined asset tag for server managed resources using Element Manager. After you define the asset tag, you can view it along with the other server information in the server list.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Select **All Servers**.
3. Expand the tree and select the type of server for which you want to specify a user-defined asset tag.
4. From the list of servers, locate the server for which you want to specify an asset tag and click the associated **Chassis Name** link.

   The chassis summary screen opens.
5. From the **More Actions** menu, select **Launch Element Manager**.

   The Element Manager application opens.

6. Using Element Manager, enter or modify the unique asset tag for the server.
   When you return to the Hitachi Compute Systems Manager screen, the new asset tag now appears as the server name in the Server list.

Related tasks

- Viewing detailed server information on page 167

Viewing detailed LPAR information

You can view configuration information for managed LPARs, including:

- Information for hosts on the LPAR
- Information for the chassis on which a blade server is mounted
- Information for LPARs on the blade server
- Information for volumes allocated to the LPAR (requires that you enable the Obtain Storage Volume information option for the Device Manager connection)

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Logical Partitions > LPAR**.
2. From the list of LPARs, select the **LPAR Name** link of the LPAR you want to view.
   The configuration information for the managed LPAR is displayed.
3. To view LPAR configuration, do one of the following:
   - To view host information for the LPAR, click the **Host Name** link of the host in the summary column.
   - To view information about the blade server on which the LPAR resides, click the **Server Name** link of the server in the summary column.
   - To view chassis information, click the **Chassis Name** link of the chassis in the summary column.
   - To view volume information for the storage system that is allocated to the LPAR, select the **Storage Volumes** tab.

Related concepts

- About viewing information summaries on page 159

Related tasks

- Creating LPARs on page 64
- Creating an LPAR host on page 68
- Setting up a connection with Hitachi Device Manager on page 43

Viewing a list of storage systems

You can view a list of storage systems by using Hitachi Compute Systems Manager.

Prerequisites

Before you can view a list of storage systems, you must verify the following:

- Compute Systems Manager and Hitachi Device Manager are installed on the same management server.
- The connection with Hitachi Device Manager is enabled.
- Users who are viewing the storage system list are registered in a Hitachi Device Manager user group and are assigned the required resource group and role.
- The properties file specifies the settings required to display the storage system list. For details about properties, see the Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide.

Procedure

1. On the **Resources** tab, select **Storage Systems > All Storage Systems**.
2. Select **Storage Systems**.
3. From the list of storage systems, click the **Storage System Name** for which you want to view information.

Related tasks

- Setting up a connection with Hitachi Device Manager on page 43

Refreshing information about managed resources

If current information includes an unusual status or an unknown alert, it may not match information previously collected and displayed about a managed resource. To obtain the most current status information, you can refresh the information about managed resources at any time.

Information can be refreshed automatically by configuring the automatic refresh interval, or you can disable automatic refreshing altogether.

Related tasks

- Refreshing host information on page 170
- Refreshing chassis information on page 172
- Refreshing server information on page 173
- Refreshing virtual machine information on page 171
- Refreshing LPAR information on page 173
- Setting automatic refresh options on page 174

Refreshing host information

You can refresh host status when you want to see the most recent host information.

Procedure

1. On the **Resources** tab, select **Hosts**.
2. Select **All Hosts**.
3. Expand the tree, and select the host type for which you want to refresh information.
4. From the list of hosts, select one or more hosts for which you want to refresh information.
5. Click **Refresh Hosts**.

Result

You can view the status of a host on the Resources tab.

Related concepts

- Refreshing information about managed resources on page 170

Related tasks

- Setting automatic refresh options on page 174

Refreshing hypervisor information

You can refresh hypervisor status to view the most current hypervisor information.

Procedure

1. On the **Resources** tab, select **Virtualization**.
2. Select **All Hypervisors**.
3. Expand the tree, and select the hypervisor type for which you want to refresh information.
4. From the list of hypervisors, select one or more hypervisors for which you want to refresh information.
5. Click **Refresh Hypervisors**.

Result

On the Resources tab, you can check the refreshed hypervisor information. Information for virtual machines mounted on a hypervisor is also refreshed.

Related concepts

- Refreshing information about managed resources on page 170

Related tasks

- Setting automatic refresh options on page 174

Refreshing virtual machine information

You can refresh virtual machine status when you want to see the most recent virtual machine information.

When you refresh virtual machine information, the status of the hypervisor on which the virtual machine is running is also refreshed.

Procedure

1. On the **Resources** tab, select **Virtualization**.
2. Select **All Virtual Machines**.
3. Expand the tree and select the virtual machine type for which you want to refresh information.
4. From the list of virtual machines, select one or more virtual machines for which you want to refresh information.
5. Click **Refresh VMs**.

Result

You can view the status of a virtual machine on the Resources tab.

Related concepts

- Refreshing information about managed resources on page 170

Related tasks

- Setting automatic refresh options on page 174

Refreshing chassis information

You can refresh chassis status when you want to see the most recent chassis information.

When you refresh the chassis status, the status of each blade server mounted on the chassis and each LPAR on the blade server is also refreshed.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Select **All Chassis**.
3. Expand the tree and select the chassis type for which you want to refresh information.
4. From the list of chassis, select one or more chassis for which you want to refresh information.
5. Click **Refresh Chassis**.

Result

You can view the status of a chassis on the Resources tab.

Related concepts

- Refreshing information about managed resources on page 170

Related tasks

- Setting automatic refresh options on page 174

Refreshing server information

You can refresh server status when you want to see the most recent server information.

The status of the LPARs on blade servers is also refreshed.

Note: If you add, replace, move or remove a blade server from a managed chassis, you must refresh the chassis information.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Select **All Servers**.
3. Expand the tree and select the server type for which you want to refresh information.
4. From the list of servers, select one or more servers for which you want to refresh information.
5. Click **Refresh Servers**.

Result

You can view the status of a server on the Resources tab.

Related concepts

- Refreshing information about managed resources on page 170

Related tasks

- Refreshing host information on page 170
- Setting automatic refresh options on page 174

Refreshing LPAR information

You can refresh LPAR status when you want to see the most recent LPAR information.

When you refresh the LPAR status, the status of the blade server on which the LPAR is running is also refreshed.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Select **All Logical Partitions**.
3. Expand the tree, and select **LPAR**.
4. From the list of LPARs, select one or more LPARs for which you want to refresh information.

You can select multiple LPARs.

5. From the **More Actions** menu, select **Refresh LPARs**.

Result

You can view the status of a LPAR on the Resources tab.

Related concepts

- Refreshing information about managed resources on page 170

Related tasks

- Setting automatic refresh options on page 174

Setting automatic refresh options

You can customize the automatic refresh interval settings.

Procedure

1. On the **Administration** tab, select **System Settings**.
2. Select **Refresh Intervals**.
3. Click **Edit Refresh Intervals**.
4. Specify the desired settings and click **OK**.
   - Schedule the **Configuration Refresh Interval** in minutes.
   - Schedule the **Status Refresh Interval** in minutes.
   - Disable automatic refresh.
   - Restore the default settings.

Result

When information about a managed resource is automatically refreshed, information about all resources managed by Hitachi Compute Systems Manager is refreshed.

To verify the automatic refresh interval settings, on the Administration tab, select System Settings, and then select Refresh Intervals.

Postrequisites

Note: Managed resource performance data and power data are not refreshed using the interval set using this procedure. For details on setting the schedule that Compute Systems Manager uses to collect performance data and power data, see the topics about performance data and power data.

Related concepts

- Refreshing information about managed resources on page 170

Related tasks

- Refreshing host information on page 170

- Registering hosts and selecting performance data types on page 177
- Refreshing virtual machine information on page 171
- Refreshing LPAR information on page 173

Monitoring the performance and power consumption of managed resources

Performance and Power Monitoring enable you to collect performance metrics and power consumption information for specified resources. You can set threshold values for performance metrics to trigger performance-related alerts. Performance and power monitoring requires a separate license.

Collecting data allows you analyze performance metrics and plan capacity expansion. When performance-related alerts are triggered, you can verify relevant performance index metrics and make the necessary changes to resolve performance-related problems.

About performance and power data analyses

Hitachi Compute Systems Manager collects performance index information from managed hosts and power data from managed chassis and servers. By analyzing the collected information, you can understand system load and performance requirements and power consumption, and plan future system configuration optimization.

Before you can collect information about host performance, you must register a Performance Monitoring license.

Before you can collect information about chassis or server power, you must register a chassis or rack-mounted server Power Monitoring license.

Compute Systems Manager can collect the following types of performance and power data:

Resource Type	Type of information collected
Host	Performance data: • CPU load percentage • Memory usage percentage • Disk usage percentage • Disk load • Disk queue length • Network packets
Chassis	Power data: • Input power (AC) • Power consumption (DC) • Intake temperature • Air flow
Blade server	Power data:

Resource Type	Type of information collected
	• Power consumption (DC) • CPU frequency
Rack-mounted server	Power data: • Input power (AC) • Intake temperature

Compute Systems Manager collects performance and power data based on Performance and Power Monitoring profile settings that define performance and power data to be collected from specified resources. This collected information is used to monitor host performance and chassis and server power consumption. The performance and power metrics of different resources can be compared on a time-series graph. Collected performance data can also be exported to a CSV file.

For performance data, you can specify threshold values for each type of performance data collected or for each host. When threshold values are exceeded, an alert is triggered.

You can enable power capping when, based on the power data, you decide that you want to minimize the power consumption of chassis and servers.

Related tasks

- Specifying threshold values for performance data on page 158
- Analyzing host performance data on page 179
- Enabling data collection for performance monitoring on page 176
- Enabling data collection for power monitoring on page 177

Enabling data collection for performance monitoring

If you have a registered Performance Monitoring license, you can collect host performance data. Before you can collect host performance data, you must enable data collection.

Procedure

1. On the **Administration** tab, select **Performance and Power Monitoring**, and then **Performance**.
2. Click **Edit Performance Monitoring Settings**.
3. Select the **Enable Data Collection** check box.
4. Select the **Enable Thresholds** check box if you want to set the threshold value for receiving an alert related to performance.
5. Optionally, open **Advanced Settings** and change the maximum threshold value and maximum graph value to the desired settings.
6. Click **OK**.

Result

Host performance data collection is now enabled.

Related concepts

- About performance and power data analyses on page 175

Related tasks

- Analyzing host performance data on page 179
- Registering hosts and selecting performance data types on page 177

Enabling data collection for power monitoring

If you have a chassis or rack-mounted server Power Monitoring license, you can collect chassis or server power data. Before you can collect chassis or server power data, you must enable data collection.

Procedure

1. On the **Administration** tab, select **Performance and Power Monitoring**, and then **Power**.
2. Select the type of managed resource for which you want to enable data collection for power monitoring.
3. Click **Edit Power Monitoring Settings**.
4. Select the **Enable Data Collection** check box.
5. Optionally, open **Advanced Settings** and change the maximum value to be displayed in the graph for the power data.
6. Click **OK**.

Result

Power data collection for the chassis or servers is now enabled.

Related concepts

- About performance and power data analyses on page 175

Related tasks

- Registering chassis and servers and selecting power data types on page 179
- Analyzing chassis power-consumption data on page 180
- Analyzing blade server power-consumption data on page 181
- Analyzing rack-mounted server power data on page 182

Registering hosts and selecting performance data types

Before you can analyze host performance data, register the types of performance data to collect and the hosts from which to collect the information. Register this information by creating a performance profile. The frequency of performance data collection and the threshold values for

triggering alerts can be customized for each host, but using the preset system defaults makes registration easier.

Before starting this task, you must register a valid Performance Monitoring license.

Before you can collect performance data, you must ensure that the host is managed by Hitachi Compute Systems Manager and then enable data collection.

Procedure

1. On the **Administration** tab, select **Performance and Power Monitoring**, and then **Performance**.
2. Click **Create Performance Profile**.
3. Type a **Profile Name**.
4. Under **Schedule**, set the interval at which performance data for the host is to be collected.
5. Under **Data Collection Settings**, verify the default settings for each metric, including threshold values, occurrences, and enabled or disabled state.

   If you do not want to change the default settings, skip this step and select target hosts. If you want to change the default settings, perform the following steps.

   a. Select the row for the metric you would like to change.
   b. Click **Edit Data Collection Settings**.
   c. Specify custom settings, and then click **OK**.
   d. To save custom settings, click **Save as User Default** under **Data Collection Settings**. The user settings are saved, and are displayed as the default instead of the system default settings. Click **Load System Default** to display the system default settings.
6. Under **Target Hosts**, click **Add Hosts**.
7. Select a host from the list of available hosts and click **Add** to add the host to the list of selected hosts.
8. Click **OK** when you are finished adding hosts.
9. Click **OK** to complete the performance profile.

   The new performance profile is listed in the **Performance Settings** list.

Result

You can now analyze performance data for the specified host.

Related concepts

- About performance and power data analyses on page 175

Related tasks

- Analyzing host performance data on page 179

- Enabling data collection for performance monitoring on page 176
- Analyzing rack-mounted server power data on page 182

Registering chassis and servers and selecting power data types

Before you can analyze chassis or server power data, you must register the types of power data to collect and the resources from which to collect the power data. The types of power data collected for a blade server can be specified for each chassis on which the blade server is mounted.

Before you perform this task, you must register a chassis or rack-mounted server Power Monitoring license.

Before you can collect power data, you must ensure that the resource is managed by Hitachi Compute Systems Manager and then enable power data collection.

Procedure

1. On the **Administration** tab, select **Performance and Power Monitoring**, and then **Power**.
2. Select the type of managed resource for which you want to analyze power data.
3. Click **Create Power Profile**.
4. Type a **Profile Name**.
5. Under **Data Collection**, select the interval at which to save data.
6. Select the type of power data and the managed resource for which you want to collect power data.
7. Click **OK** to complete the power monitor profile.

   The new power monitor profile is listed in the **Power Settings** list.

Result

You can now analyze power data for the specific chassis or servers.

Related concepts

- About performance and power data analyses on page 175

Related tasks

- Analyzing host performance data on page 179
- Analyzing blade server power-consumption data on page 181
- Analyzing chassis power-consumption data on page 180
- Enabling data collection for power monitoring on page 177

Analyzing host performance data

If you have a registered Performance Monitoring license, you can view the current performance data of specified hosts in list format or view metric trends in a time-series graph. From the CPU and disk usage rates or the

correlations between metrics that are displayed, you can analyze host performance, including which hosts have a heavy load and which are less used, and use this data to plan reallocation or increase resources.

Procedure

1. On the **Resources** tab, select **Hosts** and then select an operating system.
2. Click **View Performance Data**.
3. To view a listing of the current performance data for the hosts, click the **Summary** tab.
   - To update the list of performance data, select the host you want to update and click **Refresh Performance Data**.
   - To export the performance data to a CSV file, select the host from which you want to export and click **Export to CSV**.
4. To view performance data trends, click the **Host Data by Metric** tab.
5. Click **Select Hosts** and add target hosts from the **Available Hosts - Select up to 5** list. Select up to five hosts and click **OK**.

   You can view the performance data under each metric tab.
6. To view the correlation between metrics, select the **Metrics by Host** tab.
7. Click **Select Hosts** and add target hosts from the **Available Hosts - Select up to 5** list. Select up to five hosts and click **OK**.

   All performance data metrics for the selected host are displayed in the graph.

Related concepts

- About performance and power data analyses on page 175

Related tasks

- Registering hosts and selecting performance data types on page 177
- Enabling data collection for performance monitoring on page 176

Analyzing chassis power-consumption data

If you have a registered chassis Power Monitoring license, you can view a listing of the current power data about chassis or check the trends of a specific metric in a time series graph. By analyzing chassis power consumption information in these ways, you can understand power consumption trends based on the correlation between metrics, such as chassis power consumption and fan airflow. If the power consumption is not within acceptable limits, you can plan power capping.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Chassis > Chassis**.
2. Click **View Chassis Power Data**.

3. Click the **Summary** tab to view a listing of the current, total, and average power data for the chassis.
   - To display the latest information when viewing the list of current power data, click **Refresh Chassis Power Data**.
   - To enable power capping, select the chassis and click **Start Power Capping**.
   - To export power data to a CSV file, select the chassis for which you want to export information and click **Export to CSV**.
4. To view power data metric trends, click the **Chassis Data by Metric** tab.
5. Click **Select Chassis** and add target chassis from the **Available Chassis - Select up to 5** list.

   Select up to five chassis and click **OK**.

   Each metric for the selected chassis is displayed on a separate tab.
6. To check the correlation between metrics, select **Metrics by Chassis**.
7. Click **Select Chassis** and add target chassis from the **Available Chassis - Select up to 5** list.

   Select up to five chassis and click **OK**.

   All power data metrics for the chassis are displayed in a graph.

Related concepts

- About performance and power data analyses on page 175

Related tasks

- Analyzing host performance data on page 179
- Analyzing blade server power-consumption data on page 181
- Enabling data collection for power monitoring on page 177
- Analyzing rack-mounted server power data on page 182

Analyzing blade server power-consumption data

If you have a registered blade server Power Monitoring license, you can view a listing of the current power data about blade servers or check the trends of a specific metric in a time series graph. By analyzing server power consumption information, you can understand trends based on the correlation between metrics, such as blade server power consumption and CPU frequency. If the power consumption is not within acceptable limits, you can plan power capping on the chassis on which the blade server is mounted.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers > Blade**.
2. Click **View Blade Power Data**.
3. Click the **Summary** tab to view a listing of the current, total, and average power data for the blade server.

To display the latest information when viewing the list of power data, select a server and click **Refresh Servers Power Data**.

To export information to a CSV file, select the blade server for which you want to export information and click **Export to CSV.**

4. To view power data metric trends, click the **Server Data by Metric** tab.
5. Click **Select Server** and add target servers from the **Available Blades - Select up to 5** list. Select up to five servers and click **OK**.

   Each metric for the selected blade server is displayed on a separate tab.
6. To view the correlation between metrics, select **Metrics by Server**.
7. Click **Select Server** and add target servers from the **Available Blades - Select up to 5** list.

   Select up to five servers and click **OK**.

   All power data metrics for the blade server are displayed in a graph.

Result

You can determine the correlation between metrics, such and power consumption and CPU frequency, and check which blade servers are consuming a large amount of power, or have energy available.

Related concepts

- About performance and power data analyses on page 175

Related tasks

- Analyzing host performance data on page 179
- Analyzing chassis power-consumption data on page 180
- Enabling data collection for power monitoring on page 177
- Analyzing rack-mounted server power data on page 182

Analyzing rack-mounted server power data

If you have a registered rack-mounted server Power Monitoring license, you can view a listing of the current power data about rack-mounted servers or check the trends of a specific metric in a time-series graph. By analyzing information about rack-mounted server power consumption in these ways, you can understand power consumption trends based on the correlation between server power consumption and intake temperature. If the power consumption is not within acceptable limits, you can create a plan to cap power consumption.

Procedure

1. On the **Resources** tab, select **Chassis & Servers > All Servers > Rack-mounted**.
2. Click **View Rack-mounted Power Data**.

3. Click the **Summary** tab to view a listing of the current, total, and average power data for the rack-mounted server.
   - To display the latest information when viewing the list of power data, select a server and click **Refresh Servers Power Data**.
   - To export information to a CSV file, select the rack-mounted server for which you want to export information and click **Export to CSV.**
4. To view power data metric trends, click the **Server Data by Metric** tab.
5. Click **Select Server** and add target servers from the rack-mounted server list.

   Each metric for the selected rack-mounted server is displayed on a separate tab.
6. To view the correlation between metrics, select **Metrics by Server**.
7. Click **Select Server** and add target servers from the rack-mounted server list.

   All power data metrics for the rack-mounted server are displayed in a graph.

Result

You can determine the correlation between metrics, and check which rack-mounted servers are consuming a large amount of power, or have energy available.

Related concepts

- About performance and power data analyses on page 175

Related tasks

- Analyzing host performance data on page 179
- Analyzing chassis power-consumption data on page 180
- Enabling data collection for power monitoring on page 177
- Analyzing blade server power-consumption data on page 181

Deleting performance data

If you registered a Performance Monitoring license and have collected performance data, you can periodically delete data to maintain free space in the database. You can purge collected performance data manually by specifying a cutoff date.

Procedure

1. On the **Administration** tab, select **Performance and Power Monitoring > Performance**.
2. Click **Manual Performance Data Purge**.
3. Verify the current file size of the collected performance data before purging.
4. Specify a cutoff date.

5. Verify the file size after the data purge, and click **OK** to delete the data.

Result

Collected data stored before the specified cutoff date is deleted. As a result, the amount of space that can be used to store performance data increases.

Related concepts

- About performance and power data analyses on page 175

Related tasks

- Analyzing host performance data on page 179
- Deleting power data on page 184

Deleting power data

If you have registered a Power Monitoring license and have collected power data, you can delete data to maintain free space in the database. You can purge collected power data manually by specifying a cutoff date.

Procedure

1. On the **Administration** tab, select **Performance and Power Monitoring > Power**.
2. Select the type of managed resource for which you want to delete power data.
3. Click **Manual Power Data Purge**.
4. Verify the current file size of the collected power data before purging.
5. Specify a cutoff date for the data. The power data after the cutoff date will be retained.
6. Verify the file size after the data purge, and click **OK** to delete the data.

Result

Collected data stored before the specified cutoff date is deleted. As a result, the amount of space that can be used to store power data increases.

Related concepts

- About performance and power data analyses on page 175

Related tasks

- Analyzing chassis power-consumption data on page 180
- Analyzing blade server power-consumption data on page 181
- Deleting performance data on page 183
- Analyzing host performance data on page 179

Saving resource information output in CSV format

You can save output information from managed resources to a CSV file.

Exporting information about managed resources in CSV format

You can export data about managed resources to a CSV file using Hitachi Compute Systems Manager.

Before you can export performance or power data to a CSV file, you must have a license registered for the power monitoring or performance monitoring.

You can export the following types of information to a CSV file using Compute Systems Manager:

- Managed resource inventory information
- Host performance data
- Chassis power data
- Server power data

Related tasks

- Exporting managed resource inventory information in CSV format on page 185
- Exporting host performance data in CSV format on page 186
- Exporting chassis power data in CSV format on page 186
- Exporting server power data in CSV format on page 187

Exporting managed resource inventory information in CSV format

You can export inventory information to a CSV file, and then analyze the collected metrics beyond the capabilities of the displayed graphs.

Procedure

1. Click the **Resources** tab.
2. Open the managed resource tree, and select the resource for which you want to export inventory information.
3. Select the export option:
   - For virtual machines, click the **Export to CSV**.
   - For all other resources, select **More Action > Export to CSV**.
4. Click **Save**, and specify the destination.

Result

The managed resource configuration is exported to a CSV file in the specified location. You can now use external tools to analyze the exported resource inventory data.

Related concepts

- About performance and power data analyses on page 175

Related tasks

- Exporting host performance data in CSV format on page 186
- Exporting chassis power data in CSV format on page 186
- Exporting server power data in CSV format on page 187

Exporting host performance data in CSV format

If you registered a Performance Monitoring license, you can export performance data to a CSV file, and then analyze the collected metrics beyond the capabilities of the displayed graphs.

Procedure

1. On the **Resources** tab, under **Hosts**, select an operating system.
2. Click **View Performance Data**.
3. In the list of hosts on the **Summary** tab, select the host from which you want to export information and then click **Export to CSV**.
4. Check the metrics that you want to export and specify the start and end dates of the period for which you want to export the data.

   When exporting information about a single host, you can select multiple metrics at the same time. When you export information about multiple hosts, only one metric can be selected.
5. Click **OK**.
6. Click **Save**, and specify the destination.

Result

The host performance data is exported to a CSV file in the location you specified. You can now use external tools to analyze the exported host performance data.

Related tasks

- Exporting managed resource inventory information in CSV format on page 185
- Exporting chassis power data in CSV format on page 186
- Exporting server power data in CSV format on page 187

Exporting chassis power data in CSV format

If you have registered a Power Monitoring license, you can export collected power monitoring metrics data to a CSV file, and then analyze the collected metrics beyond the capabilities of the displayed graphs.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Select **All Chassis**.
3. Click **View Chassis Power Data**.
4. In the list of chassis on the **Summary** tab, select the chassis for which you want to export information, and then click **Export to CSV**.
5. In the window that opens, specify the types of information that you want to export and the start and end dates of the period for which you want to export the information.

   When exporting information about a chassis, you can select multiple items at the same time. When exporting information about multiple chassis, only one item can be selected.
6. Click **OK**.
7. Click **Save** and specify the destination.

Result

The chassis power data is exported to a CSV file in the location you specified. You can now use external tools to analyze exported chassis information.

Related tasks

- Exporting managed resource inventory information in CSV format on page 185
- Exporting host performance data in CSV format on page 186
- Exporting server power data in CSV format on page 187

Exporting server power data in CSV format

If you registered a chassis or rack-mounted server Power Monitoring license, you can export collected power monitoring metrics data to a CSV file, and then analyze the collected metrics beyond the capabilities of the displayed graphs.

Procedure

1. On the **Resources** tab, select **Chassis & Servers**.
2. Select **All Servers**.
3. Expand the tree and select the type of server for which you want to export information.
4. For blade servers, click **View Blade Power Data**. For rack-mounted servers, click **View Rack-mounted Power Data**.
5. In the list of servers on the **Summary** tab, select the server for which you want to export information, and then click **Export to CSV**.
6. In the window that opens, specify the types of information that you want to export and the start and end dates of the period for which you want to export the information.

When exporting information about a server, you can select multiple items at the same time. To export information about multiple servers, only one item can be selected.

7. Click **OK**.
8. Click **Save**, and specify the destination.

Result

The server power data is exported to a CSV file in the location you specified. You can now use external tools to analyze exported server information.

Related tasks

- Exporting managed resource inventory information in CSV format on page 185
- Exporting host performance data in CSV format on page 186
- Exporting chassis power data in CSV format on page 186

Grouping managed resources

Hitachi Compute Systems Manager allows administrators to group managed resources into folders and logical groups.

About logical groups

A logical group is a collection of managed resources grouped together by installation location, organization, or use.

When using logical groups, you can verify the operational status and configuration information of management resources and the management resources within a logical group.

There are two types of logical groups:

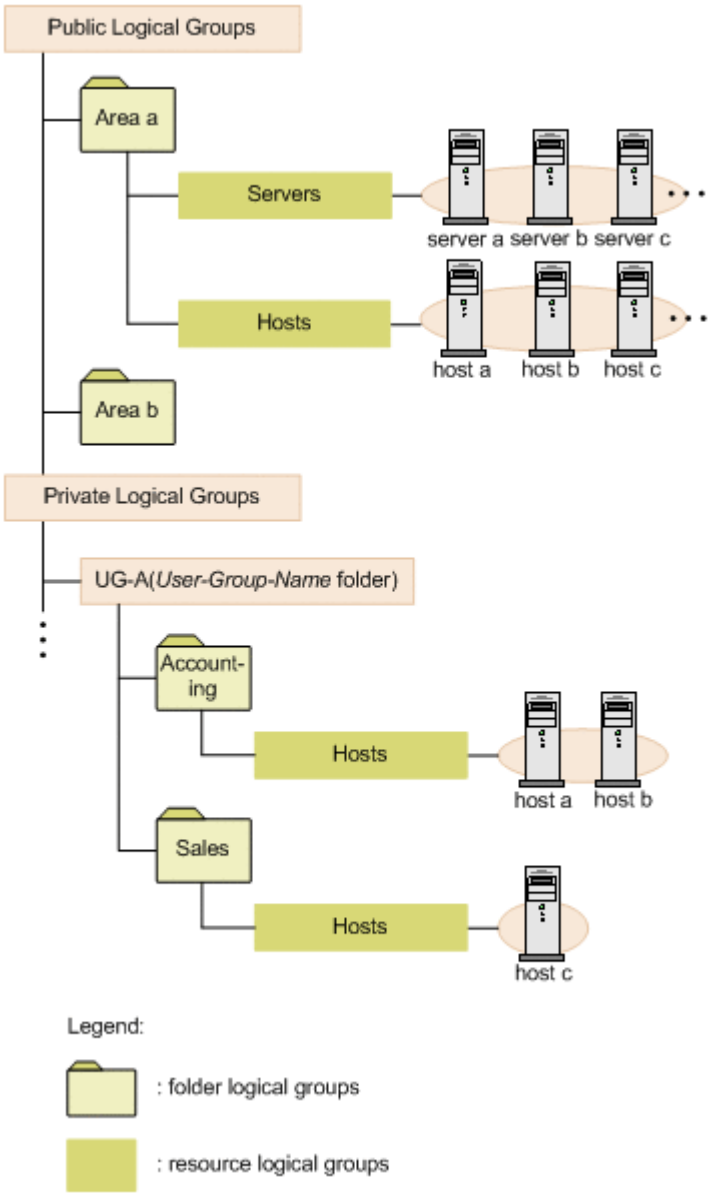
- Folder logical groups
  Register folders and resource groups to folders.
- Resource logical groups
  Register resources to resource logical groups. Resource logical groups are the lowest-level of logical groups.

There are two methods for managing logical groups:

- Public logical groups
  Hitachi Compute Systems Manager users can view, create, edit, or delete logical groups according to the roles assigned to the user groups to which they belong.
  You create logical groups in the Public Logical Groups folder. When the logical group level is displayed, a forward slash (/) appears at the beginning of the path.
- Private logical groups

Only users from the same user group can view, create, edit, or delete logical groups.
You create logical groups in the folders (default: *user-group-name*) of each user group that are located immediately under the Private Logical Groups folder. When the logical group level is displayed, a tilde (~) appears at the beginning of the path.

The following figure shows a hierarchy of folders and logical groups.



You can change the hierarchy of logical groups or add and remove resources from existing logical groups. You can also add a resource to multiple logical groups.

Related tasks

- Creating logical groups on page 190

- Editing logical groups on page 190
- Viewing logical group information on page 191

Related references

- Required roles and resource groups by function on page 210

Creating logical groups

Before creating a logical group, verify that all resources that you want to include in the logical groups have been previously discovered by Hitachi Compute Systems Manager and are available in the list of managed resources.

Procedure

1. On the **Resources** tab, select **Logical Groups**.
2. Select a method for managing logical groups.

   To create a private logical group, select a user group under **Private Logical Groups**.
3. Click **Create Logical Group** and then specify the required items .

Result

You can verify the hierarchy of the logical groups and folders that you have created by viewing them on the Resources tab under Logical Groups.

Related concepts

- About logical groups on page 188

Related tasks

- Editing logical groups on page 190
- Viewing logical group information on page 191

Editing logical groups

After creating a logical group, you can move to another logical group, or edit a logical group to add or remove resources.

Procedure

1. On the **Resources** tab, click **Logical Groups**.
2. From the list of logical groups, select the logical group that you want to edit.
3. Click **Edit Logical Group** and specify the required items.

Result

When you change the location of a logical group, you can expand the Logical Groups tree to confirm the change in the configuration. When a resource in

the logical group changes, you can confirm the changes from the list of resources.

Related concepts

- About logical groups on page 188

Related tasks

- Creating logical groups on page 190
- Viewing logical group information on page 191

Viewing logical group information

You can view configuration information for each logical group, including the number of resources and the status for each resource in the logical group.

Procedure

1. On the **Resources** tab, click **Logical Groups**.
2. Expand the tree and select the logical group for which you want to view information.

Related concepts

- About logical groups on page 188

Related tasks

- Creating logical groups on page 190
- Editing logical groups on page 190

Alerts and alert resolution

Hitachi Compute Systems Manager provides alert details to help you troubleshoot errors or failures that occur on managed resources.

About alerts and alert resolution

Hitachi Compute Systems Manager provides alert notification for errors or failures that occur on a managed resource.

Alert details provide information about the resource on which a failure occurred and the specific location of the failure.

Users are notified about alerts by email.

Alerts display one of the following status indicators:

- Unconfirmed
- In Progress
- Resolved

To ensure that no alerts go unattended, you can assign unconfirmed or unresolved alerts to another user and, optionally, notify the user by email.

All users can view a history of generated alerts, including the status of those alerts. Specific users can delete alerts from the list of alerts.

By default, the system settings specify deleting the oldest alerts at regular intervals when the number of alerts exceeds 1,000,000. The number of stored alerts after the deletion is approximately 900,000. If you want to change the number of alerts to store on the system (maximum number of stored alerts), you can specify user-defined custom settings.

Related tasks

- Resolving alerts on page 193
- Assigning an alert to a user on page 193
- Requesting alert resolution by another user on page 194
- Viewing a list of alerts on page 195
- Deleting alerts on page 195
- Specifying the number of alerts to store on page 158

Prerequisites for alert resolution

Before Hitachi Compute Systems Manager can receive alerts, you must complete the following tasks:

- Specify settings on managed hosts so that SNMP traps are sent to the management server.
- Configure SNMP trap reception in Compute Systems Manager if you want to receive alerts about hosts.
- Set up threshold values for performance data if you want to receive performance alerts.

If you are using email notification to send alerts, you must also complete these additional tasks:

- In Compute Systems Manager, configure the SMTP server to send email notifications.
- Register the email address of each user who sends and receives email notifications.

Related tasks

- Associating SNMP traps with alert IDs on page 150
- Setting up email notification on page 40
- Specifying an alert level for email notification on page 152
- Resolving alerts on page 193
- Requesting alert resolution by another user on page 194

Resolving alerts

You, or another user to whom you assign an alert, can resolve unresolved alerts. When an alert has been resolved, you can notify other users that the alert has been resolved.

Procedure

1. On the **Dashboard**, select an alert from the **Unresolved Alerts** list, and then click **Respond to Alert**.
2. Review the alert details and take appropriate action to resolve the issue that caused the alert.
   - To view alert information, select the **Go to Related Screen** check box, select the related Screen from the drop-down menu, and then **OK**.
   - After you resolve the issue, return to the **Detailed Alert Information** window and, in the **Update Status** area, change **Status** to **Mark as resolved**.
3. To send an email to another user, in the **Share Alert** area, click **Compose Message**.
4. Add the message content and choose a recipient from the list.
5. Click **Send**.
6. Optionally, expand **Update Multiple Alerts** to select other alerts to mark as resolved.
7. Click **OK** to close the **Detailed Alert Information** dialog box.

Result

The alert status for the selected alerts changes to Resolved. If you specified to send an email notification to another user, the email is sent.

Related concepts

- About alerts and alert resolution on page 191

Related tasks

- Requesting alert resolution by another user on page 194

Related references

- Prerequisites for alert resolution on page 192

Assigning an alert to a user

You can assign alerts to specified users for resolution. Alerts that are assigned can still be resolved by you or other unassigned users.

Procedure

1. On the **Dashboard**, select an alert from the **Unresolved Alerts** list, and then click **Respond to Alert**.
2. In the **Update Status** area, change **Status** to **Proceed with troubleshooting**.
3. Change the user assigned to the alert.
4. To send an email to another user, in the **Share Alert** area, click **Compose Message**.
5. Add the message content and choose a recipient from the list, or add a recipient's email address.
6. Click **Send**.
7. Optionally, expand **Update Multiple Alerts** to select other alerts to assign to the user.
8. Click **OK** to close the **Detailed Alert Information** dialog box.

Result

The alert status for the selected alerts changes to In Progress.

Related concepts

- About alerts and alert resolution on page 191

Related tasks

- Resolving alerts on page 193

Related references

- Prerequisites for alert resolution on page 192

Requesting alert resolution by another user

If you cannot resolve an alert, you can delegate the alert by assigning it to another user for resolution.

If your assigned role does not allow you to reassign alerts, you can send an email to another user to request that they assign themselves to the alert.

Procedure

1. On the **Dashboard**, select an alert from the list of **Unresolved Alerts**, and then click **Respond to Alert**.

   Optionally, maximize the **Unresolved Alerts** report to show the complete list of alerts and all columns.
2. In the **Share Alert** area, click **Compose Message**.
3. Choose a user from the list and, optionally, modify the **Subject** and **Comments** fields to specify more information about your request.
4. Click **Send**.
5. Click **OK** to close the **Detailed Alert Information** dialog box.

Result

An email is sent to the specified user.

Related tasks

- Resolving alerts on page 193
- Assigning an alert to a user on page 193

Viewing a list of alerts

You can check the alerts and alert statuses generated by the managed resources.

Procedure

1. On the **Tasks & Alerts** tab, select **All Alerts**.
2. Expand the tree and select the time period for which to display the list.

Result

The screen shows a list of alerts generated by all managed resources, including the status for each.

Related concepts

- About alerts and alert resolution on page 191

Related tasks

- Resolving alerts on page 193
- Deleting alerts on page 195

Deleting alerts

You can delete any alert regardless of whether it has been resolved.

Procedure

1. On the **Tasks & Alerts** tab, select **All Alerts**.
2. Expand the tree and select the time period for which to display the list.
3. From the list, select the alerts that you want to delete.
4. Click **Delete Alerts** and verify that the list of alerts to delete is correct.
5. Click **OK**.

Result

The selected alerts are deleted.

Related concepts

- About alerts and alert resolution on page 191

Related tasks

- Viewing a list of alerts on page 195

6

Managing users and controlling resource access

This module describes how to add users and manage user permissions, profiles, and user authentication.

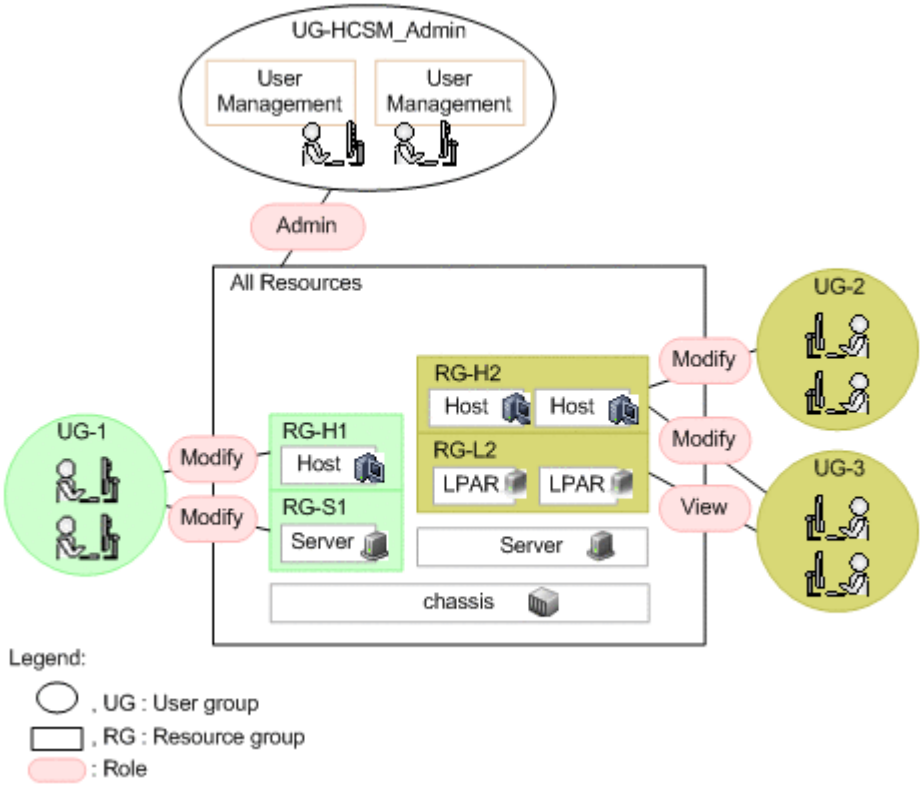
About access control of managed resources by groups

You can control access to managed resources by assigning resource groups and roles (permissions for specific tasks) to user groups. In a multi-tenancy environment, you can use managed resources by grouping them according to different companies and divisions.

System administrators who have both User Management permissions and the Admin role for the built-in resource group All Resources control access to managed resources.

System administrators create a resource group for each type of managed resource, and create a user group for users who are assigned the same role and use the same resources.

The following figure shows an example of setting up access control:



You can view and use only the resources of the assigned resource groups according to the permissions of the assigned roles. In the previous example, the UG-1 users can view and use only the resources included in the assigned resource groups (RG-H1 and RG-S1). They cannot view the resources in the unassigned resource groups (such as RG-H2 and RG-L2).

Note: If you use control the power or refresh information for a managed resource, other resources running on the target managed resource might be affected. This means that users must have access to determine how specific

actions affect these other resources. Therefore, in addition to providing the user group with permission to access the resource group containing the target resource, the system administrator must also provide the user group with permission to access any resource groups that contain resources running on the target managed resource.

Related concepts

- About user management on page 199
- About resource groups on page 207
- About user groups on page 208

Related references

- User group roles on page 210
- Required roles and resource groups by function on page 210

User management

This module describes user management.

About user management

When you create a Hitachi Compute Systems Manager user account, you set the permissions and role for the user based on the scope of the tasks that you want the user to manage.

When Compute Systems Manager is installed, the `system` account (default password: `manager`) is set by default. You use this account to run all Hitachi Command Suite products and to manage users. You cannot delete this account or change the account ID.

After creating a user account, if necessary, assign the User Management permission to manage other users. Also, you must register the user account to a user group and assign a resource group to that user group. Users who do not have an assigned resource group cannot log in to Hitachi Compute Systems Manager.

Hitachi Command Suite products share user accounts and user groups. You can add user accounts that you created in other Hitachi Command Suite products to user groups that you created in Compute Systems Manager.

You can also manage user accounts by linking to an external authentication server, such as an LDAP directory server. However, the built-in account (`system`) cannot be authenticated on an external authentication server.

The Compute Systems Manager user account used to connect to external authentication servers and external authorization servers is managed as a Windows Active Directory (authorization) group.

Related concepts

- About access control of managed resources by groups on page 198

Related tasks

- Creating a user account on page 200
- Setting user management permissions on page 200
- Editing a user account profile on page 201
- Editing your own profile on page 201
- Changing the password for a user account on page 202
- Changing your password on page 202
- Locking user accounts on page 203
- Changing the user authentication method on page 204

Related references

- User group roles on page 210
- Required roles and resource groups by function on page 210

Creating a user account

User accounts are required for accessing Hitachi Compute Systems Manager.

Procedure

1. On the **Administration** tab, click **Users and Permissions** and then click **Users**.
2. Click **Add User**, and then specify a user ID and password for the user.
3. Click **OK**.

Note:

- If accounts are managed by an external authentication server, use the external authentication password to set the password.
- If you delete a user, all tasks registered by that user fail.

Related concepts

- About user management on page 199
- About user groups on page 208

Related tasks

- Setting user management permissions on page 200

Setting user management permissions

After you create a user account, you specify the permissions for the user. If you want a user to manage other users, you must set the User Management permission.

Procedure

1. On the **Administration** tab, click **Users and Permissions** and then click **Users**.
2. From the list, select the user for which you want to change permissions and click **Change Permission**.
3. Specify the permissions for the user and click **OK**.
4. Verify that the correct permissions for the user are selected in the **Granted Permission** table.

Related concepts

- About user management on page 199
- About user groups on page 208

Related references

- Required roles and resource groups by function on page 210

Editing a user account profile

Editing user profiles allows you to modify the name, email address, and description for a user account.

Procedure

1. On the **Administration** tab, click **Users and Permissions** and then **Users**.
2. From the list, select the user for which you want to edit the profile and click **Edit Profile**.
3. Edit the profile information for the user and click **OK**.
4. Confirm that the updated user profile information appears in the **Users** area.

Related concepts

- About user management on page 199

Editing your own profile

As your user settings change, you need to update your user profile.

Procedure

1. On the **Administration** tab, click **User Profile**.
2. Click **Edit Profile**.
3. Edit the profile information.
4. Click **OK**.
5. Confirm that the updated user profile information appears in the **Users** area.

Related concepts

- About user management on page 199

Changing the password for a user account

As user passwords expire or are compromised, they need to be changed.

Procedure

1. On the **Administration** tab, click **Users and Permissions** and then **Users**.
2. From the list, select the user for which you want to change the password and click **Change Password**.
3. Type and verify the new password.
4. Click **OK**.
5. Confirm that the user can log in with the new password.

Postrequisites

Note: When the user account is being managed by the external authentication server, set the password from the external authentication server.

Related concepts

- About user management on page 199

Related tasks

- Changing your password on page 202

Changing your password

As your password expires or is compromised, it needs to be changed.

Procedure

1. On the **Administration** tab, click **User Profile**.
2. Click **Change Password**.
3. Type and verify the new password.
4. Click **OK**.

Postrequisites

Note: When the user account is being managed by the external authentication server, set the password from the external authentication server.

Related concepts

- About user management on page 199

Related tasks

- Changing the password for a user account on page 202

Locking user accounts

You can lock any Hitachi Compute Systems Manager user account, including accounts of users that are currently logged in.

If you lock the account of a user who is currently logged in, that user cannot log in during the next attempt. If that user attempts to perform any function other than logging out or displaying Help, an invalid session message displays.

Accounts that are locked cannot be used to log in to Compute Systems Manager or any other Hitachi Command Suite product.

Procedure

1. On the **Administration** tab, select **Users and Permissions**.
2. Select **Users**.

   A list of users appears.
3. Select the check box of each user you want to lock, and then click **Lock Users**.

Postrequisites

Note: To lock the System account, you must use the properties file to specify the settings. For more information, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

Related concepts

- About user management on page 199

Related tasks

- Unlocking user accounts on page 203
- Setting automatic account locking on page 206

Unlocking user accounts

You can unlock user accounts that were manually locked or automatically locked by the automatic account lock function.

Procedure

1. On the **Administration** tab, select **Users and Permissions**.

2. Select **Users**.

   A list of users appears.
3. Select the check box of each user you want to unlock, and then click **Unlock Users**.

Related concepts

- About user management on page 199

Related tasks

- Locking user accounts on page 203
- Setting automatic account locking on page 206

Changing the user authentication method

For Hitachi Compute Systems Manager authentication, you can use either the default authentication method common to all Hitachi Command Suite products, or you can change the default authentication method for a user to use an external authentication server. For details about how to configure the management server, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

Before you can change the user authentication method for a user, verify the following:

- A connection to an external authentication server is configured on the management server.
- The user ID and password must be registered both in Compute Systems Manager and on the external authentication server.

Procedure

1. On the **Administration** tab, select **Users and Permissions**.
2. Select **Users** in the tree, and then select the check box for each user whose authentication method you want to specify.
3. Click **Change Auth**.
4. Specify an authentication method and refresh the settings.
5. Verify that the authentication method is correct by viewing the **Authentication** column in the **Users** list.

Related concepts

- About user management on page 199

Related tasks

- Enabling connections to an external authorization server on page 205

Enabling connections to an external authorization server

To use external authentication, you must enable a connection to the external authentication server.

Before you can enable a connection to an external authentication server, the external authentication server and the connection to the external authorization server must be set up on the management server. You must also register the user ID and password in the authenticated group.

Procedure

1. On the **Administration** tab, select **Users and Permissions**.
2. Click **Groups**, select the **Domain-Name**, and click **Add Groups**.
3. Specify the necessary items.

   For **Distinguished Name**, register the distinguished name of the authorized group. Click **Check DN** to confirm that the distinguished name has been registered on the external authorized server.
4. From **Domain-Name**, select the group that was just added and then click **Change Permission**.
5. Set the permissions and then close the dialog box.

Postrequisites

Tip: To delete registered authorization groups, select the check boxes of the groups to be deleted, and then click Delete Groups.

Related concepts

- About user management on page 199

Related tasks

- Changing the user authentication method on page 204

Setting a password policy

You can increase user security by setting a password policy.

If an external authentication server is used to authenticate users, passwords are checked by using a combination of character types specified on the external authentication server.

The password policy that you set are applied when a user account is added or when an existing user password is changed. As a result, even if an existing password does not satisfy the password policy, a user can continue to use the password to log in to the system.

Procedure

1. On the **Administration** tab, select **Security**.
2. Select **Password**.
3. Click **Edit Settings** and enter the conditions for the new password policy.
4. Click **OK**.
5. Confirm the changes by selecting **Password** again to view the updated password policy.

Related concepts

- About user management on page 199

Setting automatic account locking

A user account can be automatically locked after a specified number of failed login attempts. You can specify the number of failed attempts before a user account is locked by configuring an account lock policy.

Procedure

1. On the **Administration** tab, select **Security**.
2. Select **Account Lock**.
3. Click **Edit Settings** and specify a number of failed login attempts before a user account is locked.
4. Click **OK**.
5. Confirm that the changes by selecting **Account Lock** again to view the updated password policy.

Postrequisites

Note: To lock the System account, you must use the properties file to specify the settings. For details, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.

- If Hitachi Command Suite products other than Hitachi Compute Systems Manager are also being used, the login failure counter does not use a separate counter for each Hitachi Command Suite product.
- If an authentication server is used to authenticate users, the settings on the external authentication server are used to control automatic locking.

Related concepts

- About user management on page 199

Managing resource groups

This module describes how to manage resource groups.

About resource groups

A resource group is a group of resources that are managed by Hitachi Compute Systems Manager.

There are two types of resource groups:

- All Resources— A built-in resource group that contains all resources that are managed by Compute Systems Manager. The installation program creates this group automatically.
- User-defined resource groups—A resource group for grouping Compute Systems Manager managed resource types. The system administrator creates resource groups based on the system environment.

Note: You cannot register a single managed resource to more than one user-defined resource group.

Related concepts

- About access control of managed resources by groups on page 198
- About user management on page 199
- About user groups on page 208

Related tasks

- Creating resource groups on page 207
- Editing resource groups on page 208

Creating resource groups

You can create resource groups to control access to a specific set of managed resources. You must register your resources before you can add them to a resource group.

Procedure

1. On the **Administration** tab, click **Resource Groups**.
2. Click **Create Resource Group**, and then specify the resource type and the resources to add to the group.
3. Click **OK**.
   The new resource group appears in the list of resource groups.

Related concepts

- About resource groups on page 207

Related tasks

- Editing resource groups on page 208

Editing resource groups

You can edit resource groups to add or delete managed resources.

Procedure

1. On the **Administration** tab, click **Resource Groups**.
2. Select the resource group that you want to edit and click **Edit Resource Group**.
3. Add and delete managed resources as needed and click **OK**.
   The changes are reflected in the updated resource group.

Related concepts

- About resource groups on page 207

Related tasks

- Creating resource groups on page 207

Managing user groups

This module describes how to manage user groups.

About user groups

A user group consists of one or more users having the same permissions (role) for the same resources. There are built-in resource and user groups for administrative convenience. In addition to displaying Hitachi Compute Systems Manager user groups, the user interface displays user groups registered in other Hitachi Command Suite products.

Compute Systems Manager includes the following types of user groups:

- Built-in user groups for Compute Systems Manager— Built-in user groups to which the Compute Systems Manager resource group "All Resources" is assigned. The installation program creates the following groups automatically based on user role:
  - HCSM_AdminGroup
  - HCSM_ModifyGroup
  - HCSM_ViewGroup

  The system administrator adds users and assigns them to these groups or user-defined groups to specify user permissions for Compute Systems Manager. When you upgrade Compute Systems Manager from versions earlier than 8.0.1, the upgrade automatically adds users to the following user groups according the user's existing permissions.
- Built-in user groups common to Hitachi Command Suite products— Built-in user groups to which the "All Resources" from each Hitachi Command

Suite product is assigned. The product installation programs create the following groups automatically based on user role:
  - AdminGroup
  - ModifyGroup
  - ViewGroup

  The system administrator adds users and assigns them to these groups when necessary. You cannot delete or edit these groups. You cannot modify or delete these user groups in any way. You cannot change the names or descriptions, or change the resource groups or role assignments.

  Note: Additional built-in user groups might display in the Compute Systems Manager GUI, but these groups are not used in Compute Systems Manager.

- User-defined user groups— User groups used to group users that need access to specific resource groups and roles. The system administrator creates user groups as required and assigns Compute Systems Manager resource groups and roles as needed.

Note: You can assign resource groups from other Hitachi Command Suite products to user groups created in Compute Systems Manager. However, resource groups of other Hitachi Command Suite products are not displayed in the Compute Systems Manager GUI.

Also, you cannot delete user groups that include other Hitachi Command Suite product resource groups from the Compute Systems Manager GUI. Before you can delete a user group, you must remove the resource group assignment from the GUI of the other Hitachi Command Suite product.

Related concepts

- About access control of managed resources by groups on page 198
- About user management on page 199
- About resource groups on page 207

Related tasks

- Creating user groups on page 213
- Editing user groups on page 214
- Assigning resource groups and roles to a user group on page 214
- Changing a user's user group on page 215
- Exporting user or user group information in CSV format on page 216

Related references

- User group roles on page 210
- Required roles and resource groups by function on page 210

User group roles

There are three different user group roles. The following table lists the user group roles and describes the types of tasks that users belonging to the group can complete.

Roles	User tasks associated with the assigned role
Admin	Users with this role can complete tasks such as use resources, view resource information, and view system settings. Also, if All Resources is assigned, the user can register the resources to manage and change the system settings.
Modify	Users with this role can manage resources and view information about managed resources.
View	User with this role can view resource information.

Related concepts

- About user management on page 199
- About resource groups on page 207
- About user groups on page 208

Related tasks

- Assigning resource groups and roles to a user group on page 214

Related references

- Required roles and resource groups by function on page 210

Required roles and resource groups by function

The resource groups, roles, and permissions that are required for using Hitachi Compute Systems Manager functionality differ depending on the function. Functions that can be executed by any role are not included.

- Users who belong to a user group with an All Resources assignment can complete tasks such as registering resources and configuring Deployment Manager settings.
- Users who belong to a user group with an assignment of a user definition resource group can manage power supplies and update information.
- Users who manage other users and user groups require the User Management permission.

Function	Resource Group	Role or permission
Prepare before use		
Set up email notification	All Resources	Admin
View email notification settings	All Resources or user-defined resource groups	Admin

Function	Resource Group	Role or permission
Set a warning banner message	Using this function does not depend on the resource group.	User Management
Set up SSL communication with a managed server	All Resources	Admin
View communication settings between managed server and SSL	All Resources or user-defined resource groups	Admin
Set up SNMP trap reception	All Resources	Admin
Configure commands to run when an alert occurs	All Resources	Admin
Specify threshold values for performance data	All Resources	Admin
Set up a connection with Hitachi Device Manager	All Resources	Admin
Discover and register management targets		
Discover and register management targets	All Resources	Admin
Manage or unmanage resources	All Resources	Admin
Add or remove a blade server as a target of a logical partitioning plug-in license	All Resources	Admin
Remove resource information	All Resources	Admin
Set logical partitioning	All Resources	Admin, Modify
Create or change the settings of an LPAR	All Resources	Admin, Modify
Register resource credentials	All Resources	Admin
Set access controls for management targets		
Manage users	Using this function does not depend on the resource group.	User Management
Manage resource groups	All Resources	Admin
Manage user groups	This function is not dependent on the resource group.	User Management
Assign resource groups and roles to a user group	All Resources	Admin and User Management
Use managed resources		
Configure LOM settings for hosts	All Resources	Admin, Modify
Manage power settings for managed resources	All Resources or user-defined resource groups	Admin, Modify
Set a timeout period for power management	All Resources	Admin
Configure an N+M cold standby group	All Resources	Admin
Edit or remove an N+M cold standby group	All Resources	Admin
Run N+M cold standby	All Resources	Admin, Modify
Reschedule a task A user who belongs to a user group in which the Admin role is assigned for All Resources	All Resources or user-defined resource groups	Admin, Modify

Function	Resource Group	Role or permission
can complete all tasks. Other users can only do so for tasks that they created.		
Cancel a task, move a task to the History tab, or delete a task A user who belongs to a user group in which the Admin role is assigned for All Resources can complete all tasks. Other users can only do so for tasks that they created.	All Resources or user-defined resource groups	Admin, Modify
View a task A user who belongs to a user group in which All Resources is assigned can reference task details. Other users can reference only the details of tasks that they created.	All Resources or user-defined resource groups	Admin, Modify
Use Element Manager or web remote KVM to connect to managed resources	All Resources or user-defined resource groups	Admin, Modify
Assign a USB to an LPAR	All Resources	Admin, Modify
Unassign a USB from an LPAR	All Resources	Admin, Modify
Change the USB auto assignment setting	All Resources	Admin, Modify
Set up a connection to a VMM	All Resources	Admin, Modify
Use virtual resources using a VMM	All Resources or user-defined resource groups	Admin, Modify
Add or remove a managed resource from Deployment Manager	All Resources	Admin, Modify
Manage image files	All Resources	Admin
Set up deployment templates	All Resources	Admin
Use Deployment Manager to access the disk on the managed resource	All Resources	Admin, Modify
Deploy a master image	All Resources	Admin, Modify
Monitor managed resources		
Set power capping	All Resources	Admin, Modify
Refresh information about managed resources	All Resources or user-defined resource groups	Admin, Modify
Set automatic refresh interval for resource information	All Resources	Admin
Register the target host and select the performance data type	All Resources	Admin
Register the target chassis or servers and select the performance data type	All Resources	Admin
Refresh host performance data	All Resources or user-defined resource groups	Admin, Modify
Refresh chassis or server power data	All Resources or user-defined resource groups	Admin, Modify
Create, edit, or delete a logical group	All Resources or user-defined resource groups	Admin, Modify, View

Function	Resource Group	Role or permission
		A user who belongs to a user group in which the View role is assigned can create, add, and delete logical groups only.
On the Alert Details window, change the status of an alert or send a message	All Resources or user-defined resource groups	Admin
Assign an alert to another user	All Resources or user-defined resource groups	Admin
Delete alerts	All Resources or user-defined resource groups	Admin
Specify the number of alerts to store on the system	All Resources	Admin
View the number of alerts to store on the system	All Resources or user-defined resource groups	Admin
Maintenance on the management client		
Operate LIDs	All Resources	Admin, Modify
Enable automatic registration for migration WWPN	All Resources	Admin
Migrate an LPAR	All Resources	Admin, Modify
Recover from migration failure	All Resources	Admin, Modify
Change the allotted time for LPAR migration	All Resources	Admin
Update the firmware	All Resources	Admin

Related concepts

- About user management on page 199
- About resource groups on page 207
- About user groups on page 208

Related tasks

- Assigning resource groups and roles to a user group on page 214

Related references

- User group roles on page 210

Creating user groups

You can create user groups as needed to meet the needs of the customer environment.

In most cases, you create users before you create user groups.

Procedure

1. On the **Administration** tab, select **User Groups**.
2. On the **User Groups** tab, click **Create User Group**.

3. Click **Add Users** to select the user group members.
4. Click **OK**.
   You can click the user group name to verify group membership (list of users) on the **User Groups** tab.

   After you create user groups, you can assign resource groups to the user groups to provide access to specific managed resources.

Related concepts

- About user groups on page 208

Related tasks

- Creating a user account on page 200
- Assigning resource groups and roles to a user group on page 214

Related references

- User group roles on page 210
- Required roles and resource groups by function on page 210

Editing user groups

As user information and membership in user groups change, you can update this information.

Procedure

1. On the **Administration** tab, select **User Groups**.
2. Select the user group that you want to update and click **Edit User Group**.
3. Change name of the user group or any other information and add or delete user as required.

   On the **User Groups** tab, select the modified user group to confirm the changes.

Related concepts

- About user groups on page 208

Related tasks

- Assigning resource groups and roles to a user group on page 214
- Creating user groups on page 213

Related references

- Required roles and resource groups by function on page 210

Assigning resource groups and roles to a user group

You can assign resource groups and roles to a user group.

Before making any assignments, you must create a resource and user group.

Procedure

1. On the **Administration** tab, select **User Groups**.
2. On the **User Groups** tab, click the link for the target user group.
3. On the **User Group** tab, click the link for the target user group.
4. Select the **Resource Group** tab and click **Add Resource Groups**.
5. Select the resource group to assign to the user group and ensure you set the required user group roles.

   From the **Resource Groups** tab resource group list, you can confirm the updated settings.

Note:

- If a user is logged in to the system when you make a change, the user role remains the same until the user logs out the system and then logs in again.
- After you change a user role, tasks registered by that user might not run because of insufficient permissions.

Related concepts

- About resource groups on page 207
- About user groups on page 208

Related tasks

- Creating user groups on page 213

Related references

- User group roles on page 210
- Required roles and resource groups by function on page 210

Changing a user's user group

To change user permissions or the set of resources that a user can access, you can change the user group to which the user belongs.

Procedure

1. On the **Administration** tab, select **User Groups**.
2. On the **Users** tab, select a target user and then click **Assign User Groups**.
3. Change the user groups to which a user belongs as required.

   From the **User** tab user list, you can confirm the changes.

Related concepts

- About user groups on page 208

Related tasks

- Creating user groups on page 213

Exporting user or user group information in CSV format

You can export user or user group-related information, such as access control information, to a CSV file.

Procedure

1. On the **Administration** tab, select **User Groups**.
2. On the **User Groups** or **Users** tab, click **Export to CSV**.
3. Click **Save** and specify the storage location.

   The information is saved to a CSV file in the location you specified.

Related concepts

- About user groups on page 208

Related tasks

- Creating a user account on page 200
- Creating user groups on page 213

7

Troubleshooting

This module describes troubleshooting management client issues.

- Troubleshooting a management client

Troubleshooting a management client

This section describes issues that might occur and how to troubleshoot them.

About troubleshooting

If problems occur during the operation of Hitachi Compute Systems Manager, follow the displayed instructions.

If no message is displayed, or the problem is not resolved when the displayed instructions are followed, contact the system administrator.

For more information about displayed messages, see the *Hitachi Command Suite Compute Systems Manager Messages*.

Related references

- Troubleshooting examples on page 218

Troubleshooting examples

The following table describes problems that may occur with a management client and possible causes and solutions.

Problem	Possible cause	Solution
No login window displays.	Hitachi Compute Systems Manager is not running or is now being started on the management server.	Wait a while and then retry. If the login window still does not appear, contact your system administrator.
You cannot log in even after providing the correct user ID and password.	The user account is locked.	Ask a user with User Management permission to unlock the account. A user can unlock his or her own account by using the management server. For details about how to unlock an account on a management server, see the *Hitachi Command Suite Compute Systems Manager Installation and Configuration Guide*.
A task ends in an error that cannot be handled by using the management client.	The management server database is blocked.	Contact the system administrator to restore the database. After the database is restored, try to run the task again.
Host Refresh or Power Operation fails	• The managed host's motherboard was replaced, and Compute Systems Manager does not recognize the host. • An IP address is allocated to a different host, and	Rediscover the hosts. Using Advanced Settings of the Discover Resources window, change Discovery Type Criteria to All and then discover the hosts.

Problem	Possible cause	Solution
	Compute Systems Manager does not recognize the host to which the IP address is allocated.	
Blade server is not updated	The blade was added, replaced, moved, or discarded while Compute Systems Manager was stopped and the blade server has not been recognized by Compute Systems Manager.	Update the information for the chassis that contains the blade that was added, replaced, moved, or discarded. If the blade is replaced or moved, scheduled task settings are canceled. If you want to continue execution of scheduled tasks, register them again.
Failover fails in the N +M cold standby configuration	• Communication error • The blade does not satisfy the failover requirements.	Perform the following procedure: **1.** Correct the cause for the failure. If you cannot correct the cause, contact the system administrator. **2.** Return the active blade and standby blade that could not fail over to their original state. When the active blade and standby blade are returned to their original state, they become available for fail over again. **3.** Manually fail over from the active blade to the standby blade. A host that was running on the active blade on which an error occurred resumes operation on the standby blade.
Hyper-V is not being managed	The host on which the Hyper-V is installed has been already discovered as a Windows host.	In the Discover Resources window, specify All for Discovery Type Criteria, and then perform discovery again.
An LPAR cannot be referenced as a Deployment Manager managed resource	• The LPAR was deleted by using a product other than Compute Systems Manager • The LPAR was migrated by using a product other than Compute Systems Manager • Logical partitioning on the blade server that contains the unreferenceable LPAR is disabled.	Because the unreferenceable LPAR has been deleted or migrated, remove it as a managed resource from Deployment Manager. If you want to continuing using the LPAR with Deployment Manager, re-add the resource to Deployment Manager. If logical partitioning is disabled, re-enable it.

Related concepts

- About user management on page 199

Related tasks

- Configuring N+M cold standby on page 104
- Refreshing chassis information on page 172

Glossary

A

active blade server

A server that is actively running your applications. When using the N+M cold standby feature for redundancy, the *running* server is referred to as an active server and the failover server is referred to as the *standby* server.

alert

A notification that a certain event has occurred. Alerts are triggered when errors or failures occur on a component of a managed resource, or when thresholds are exceeded.

B

base DN

The starting point in the active directory hierarchy at which your searches begin.

C

certificate

Refers to a digital certificate used with SSL. The browser examines the certificate and determines whether it is authentic before allowing communication.

certificate signing request

A message that is sent from an applicant to a certification authority to apply for a digital identity certificate.

chassis

A housing in which blades and other various shared electronic components are mounted.

CLI

command line interface

CSV

comma-separated values

D

daemon

A Linux program that runs in the background.

device (dev or DEV)

A physical or logical unit with a specific function.

discovery

A process that finds and identifies network objects. For example, discovery may find and identify all hosts within a specified IP address range.

Distributed Component Object Model (DCOM)

A Microsoft Windows interface in which client programs can request services from other network computers.

Domain Name System (DNS)

A hierarchical distributed naming system for computers.

F

FC

Fibre Channel

Fibre Channel Information Tool (fcinfo)

A tool used on Microsoft Windows servers that enables remote gathering of Fibre Channel information for servers connected to SAN storage.

G

GUI

graphical user interface

H

HBA

See host bus adapter.

host bus adapter (HBA)

One or more dedicated adapter cards that are installed in a host, have unique WWN addresses, and provide Fibre Channel I/O connectivity to storage systems, typically through Fibre Channel switches. Unlike general-purpose Ethernet adapters, which handle a multitude of network protocols, host bus adapters are dedicated to high-speed block transfers for optimized I/O performance.

hypervisor

Software that enables multiple guest operating systems (virtual machines) to run concurrently on a single physical host computer. Each operating system runs independently, but the hypervisor controls the host processor and resources.

I

inventory

Information about managed resources, such as operating system version, hardware status, and IP address.

IPMI

Intelligent Platform Management Interface

J

Java heap dump

A record of all live Java objects and classes that is used for troubleshooting diagnostics.

Java thread

A Java program's path of execution.

JDK

Java Development Kit

K

key password

Unlocks the private keys stored in the keystore.

keystore

A keystore contains private keys and certificates with corresponding public keys that are used for secure SSL communications.

L

lights-out management (LOM)

Provides remote management of discovered hosts by connecting to a host's management interface from the Hitachi Compute Systems Manager management client.

Lightweight Directory Access Protocol (LDAP) server

A server that provides distributed directory service such as user account information.

logical group

A user-defined collection of managed resources, grouped together by installation location, organization, or use.

M

managed resource

Any system, such as a host, chassis, or server, managed by Hitachi Compute Systems Manager.

management client

A computer used to operate a graphical user interface client or a command-line interface client.

management information base (MIB)

A virtual database of objects that can be monitored by a network management system. SNMP uses standardized MIBs that allow any SNMP-based tool to monitor any device defined by a MIB file.

management module

A component installed in a chassis that controls the blades and other various shared electronic components.

management target

Any system, such as hosts, servers, or chassis, within an IP address range that is targeted to be managed by a software application.

N

N+M cold standby

A failover mechanism for servers that increases availability. With N+M cold standby, "N" servers are active and running your applications, and "M" servers are on standby, powered off, and not consuming data center resources. If a failure occurs on a running blade server, the software detects the failure and automatically replaces the failed blade with a standby blade.

O

object identifier (OID)

OIDs uniquely identify managed objects. SNMP traps can be distinguished from each other because they have unique OIDs.

P

performance profile

A user-defined set of performance metrics and data collection interval settings used to collect and analyze managed host performance data.

power profile

A user-defined set of performance metrics and data collection interval settings used to collect and analyze chassis power consumption data.

private key

An encryption/decryption key known only to the party or parties that exchange secure communication.

properties file

A file that defines aspects of the operating environment. The operating environment can be modified by changing the appropriate properties file.

R

remote method invocation (RMI) request

A request to invoke a program on a remote computer.

resource group

A collection of resources that are grouped by one or more system resource types.

role

Permissions that are assigned to users in a user group to control access to resources in a resource group. Resource groups can be assigned to different user groups with different roles.

root

A Linux user account that has access to all commands and files.

S

SAN

See storage area network.

Secure Sockets Layer (SSL)

A common protocol for managing the security of message transmission over the Internet.

Two SSL-enabled peers use their private and public keys to establish a secure communication session, with each peer encrypting transmitted data with a randomly generated and agreed-upon symmetric key.

self-signed certificate

A digital identity certificate signed by the person who created it, rather than a trusted certificate authority.

SNMP

Simple Network Management Protocol

SNMP trap

An event generated by an SNMP agent from the managed resource that communicates an event, such as an error or failure.

SRV (service) record

A specification of data in DNS for defining the location (host name and port number) of servers or services.

SSH (secure shell)

A network protocol for secure data communication.

standby blade server

A server that remains powered-off until it is required to replace another server on which a failure occurs. When using the N+M cold-standby feature for redundancy, the running server is referred to as an *active* server, and the failover server is referred to as the *standby* server.

su command

The su command changes user credentials on a Linux system to those of the root user or to the user specified by the Name parameter, and then initiates a new session.

sudo command

The sudo (superuser do) command allows a system administrator to change user credentials on a Linux system to those of the root user or to the user specified by the Name parameter, and then initiates a new session. The session is usually limited and all actions are recorded in a log.

T

threshold

A user-defined limit that triggers an alert when reached or exceeded.

transport layer security (TLS)

Transport layer security (TLS) and its predecessor, secure sockets layer (SSL), are cryptographic protocols that provide communication security over the Internet.

truststore

A truststore contains public keys in the form of trusted third-party certificates, such as those from a certificate authority (CA) or from another party with which you must set up secure SSL communication.

truststore file

A key database file that contains public keys for a trusted entity.

U

User Access Control (UAC)

Management of user accounts in Windows Server 2008.

user group

A collection of users who have access to the same resources and have the same permissions for those resources. Permissions for users are determined by the user groups to which they belong. Users and resource groups can be assigned to multiple user groups.

V

virtual machine

One instance of an operating system along with one or more applications running in an isolated partition within the computer. A VM enables different operating systems to run in the same computer at the same time as well as prevents applications from interfering with each other. All virtual machines run simultaneously.

virtual machine manager (VMM)

Software that manages hypervisors and the associated virtual machines (for the fundamental concept, see *virtual machine*). VMMs can manage multiple hypervisors and all virtual machines running on the hypervisor. VMMs can create virtual machines, change virtual machine configuration, and migrate virtual machines to a different hypervisor.

W

wake-on-LAN (WOL)

An ethernet computer networking standard that allows a computer or server to be turned on or *awakened* from a remote location by a network message.

Windows Management Instrumentation (WMI)

A method for managing Windows devices, for example, to connect to Windows hosts.

Index

S

T

U

V

W

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0) 1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-91HC194-14